```
No.     Time        Source                Destination           Protocol Info
      1 0.000000    192.168.1.106         192.168.1.255         CUPS
ipp://192.168.1.106:631/printers/Bluetooth_Modem (idle)

Frame 1 (145 bytes on wire, 145 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:51.997652000
    Time delta from previous packet: 0.000000000 seconds
    Time since reference or first frame: 0.000000000 seconds
    Frame Number: 1
    Packet Length: 145 bytes
    Capture Length: 145 bytes
    Protocols in frame: eth:ip:udp:cups
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.255
(192.168.1.255)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 131
    Identification: 0x5954 (22868)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (0x11)
    Header checksum: 0x9c5c [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.255 (192.168.1.255)
User Datagram Protocol, Src Port: ipp (631), Dst Port: ipp (631)
Common Unix Printing System (CUPS) Browsing Protocol

No.     Time        Source                Destination           Protocol Info
      2 1.000315    192.168.1.106         192.168.1.255         CUPS
ipp://192.168.1.106:631/printers/Bluetooth_Modem-1 (idle)

Frame 2 (136 bytes on wire, 136 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:52.997967000
    Time delta from previous packet: 1.000315000 seconds
    Time since reference or first frame: 1.000315000 seconds
```

```
    Frame Number: 2
    Packet Length: 136 bytes
    Capture Length: 136 bytes
    Protocols in frame: eth:ip:udp:cups
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.255
(192.168.1.255)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 122
    Identification: 0x5955 (22869)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (0x11)
    Header checksum: 0x9c64 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.255 (192.168.1.255)
User Datagram Protocol, Src Port: ipp (631), Dst Port: ipp (631)
Common Unix Printing System (CUPS) Browsing Protocol

No.     Time        Source                Destination           Protocol Info
      3 2.000560    192.168.1.106         192.168.1.255         CUPS
ipp://192.168.1.106:631/printers/Bluetooth_PDA_Sync (idle)

Frame 3 (149 bytes on wire, 149 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:53.998212000
    Time delta from previous packet: 2.000560000 seconds
    Time since reference or first frame: 2.000560000 seconds
    Frame Number: 3
    Packet Length: 149 bytes
    Capture Length: 149 bytes
    Protocols in frame: eth:ip:udp:cups
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
```

```
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.255
(192.168.1.255)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 135
    Identification: 0x5956 (22870)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (0x11)
    Header checksum: 0x9c56 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.255 (192.168.1.255)
User Datagram Protocol, Src Port: ipp (631), Dst Port: ipp (631)
Common Unix Printing System (CUPS) Browsing Protocol

No.     Time        Source                Destination           Protocol Info
      4 3.000831    192.168.1.106         192.168.1.255         CUPS
ipp://192.168.1.106:631/printers/itlprinter_sclab_clarkson_edu (idle)

Frame 4 (166 bytes on wire, 166 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:54.998483000
    Time delta from previous packet: 3.000831000 seconds
    Time since reference or first frame: 3.000831000 seconds
    Frame Number: 4
    Packet Length: 166 bytes
    Capture Length: 166 bytes
    Protocols in frame: eth:ip:udp:cups
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.255
(192.168.1.255)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
```

```
        .... ...0 = ECN-CE: 0
    Total Length: 152
    Identification: 0x5957 (22871)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (0x11)
    Header checksum: 0x9c44 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.255 (192.168.1.255)
User Datagram Protocol, Src Port: ipp (631), Dst Port: ipp (631)
Common Unix Printing System (CUPS) Browsing Protocol

No.     Time        Source                Destination           Protocol Info
      5 4.001086    192.168.1.106         192.168.1.255         CUPS
ipp://192.168.1.106:631/printers/Stylus_CX6400-1 (idle)

Frame 5 (145 bytes on wire, 145 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:55.998738000
    Time delta from previous packet: 4.001086000 seconds
    Time since reference or first frame: 4.001086000 seconds
    Frame Number: 5
    Packet Length: 145 bytes
    Capture Length: 145 bytes
    Protocols in frame: eth:ip:udp:cups
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.255
(192.168.1.255)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 131
    Identification: 0x5958 (22872)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
```

```
    Time to live: 64
    Protocol: UDP (0x11)
    Header checksum: 0x9c58 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.255 (192.168.1.255)
User Datagram Protocol, Src Port: ipp (631), Dst Port: ipp (631)
Common Unix Printing System (CUPS) Browsing Protocol

No.     Time        Source                Destination           Protocol Info
      6 5.024906    192.168.1.106         224.0.0.251           MDNS
Standard query SRV nuuanu._ftp._tcp.local

Frame 6 (82 bytes on wire, 82 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.022558000
    Time delta from previous packet: 5.024906000 seconds
    Time since reference or first frame: 5.024906000 seconds
    Frame Number: 6
    Packet Length: 82 bytes
    Capture Length: 82 bytes
    Protocols in frame: eth:ip:udp:dns
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: 01:00:5e:00:00:fb
(01:00:5e:00:00:fb)
    Destination: 01:00:5e:00:00:fb (01:00:5e:00:00:fb)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 224.0.0.251
(224.0.0.251)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x18 (DSCP 0x06: Unknown DSCP; ECN: 0x00)
        0001 10.. = Differentiated Services Codepoint: Unknown (0x06)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 68
    Identification: 0x5959 (22873)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (0x11)
    Header checksum: 0xbf29 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 224.0.0.251 (224.0.0.251)
User Datagram Protocol, Src Port: mdns (5353), Dst Port: mdns (5353)
Domain Name System (query)
```

```
No.     Time        Source                Destination           Protocol Info
      7 5.158733    192.168.1.108         224.0.0.251           MDNS
Standard query response SRV 0 0 21 nuuanu.local

Frame 7 (147 bytes on wire, 147 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.156385000
    Time delta from previous packet: 5.158733000 seconds
    Time since reference or first frame: 5.158733000 seconds
    Frame Number: 7
    Packet Length: 147 bytes
    Capture Length: 147 bytes
    Protocols in frame: eth:ip:udp:dns
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 01:00:5e:00:00:fb
(01:00:5e:00:00:fb)
    Destination: 01:00:5e:00:00:fb (01:00:5e:00:00:fb)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 224.0.0.251
(224.0.0.251)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x18 (DSCP 0x06: Unknown DSCP; ECN: 0x00)
        0001 10.. = Differentiated Services Codepoint: Unknown (0x06)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 133
    Identification: 0x9c98 (40088)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (0x11)
    Header checksum: 0x7ba7 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 224.0.0.251 (224.0.0.251)
User Datagram Protocol, Src Port: mdns (5353), Dst Port: mdns (5353)
Domain Name System (response)

No.     Time        Source                Destination           Protocol Info
      8 5.595281    192.168.1.106         192.168.1.108         SMB      Trans2
Request, QUERY_PATH_INFO, Query File Basic Info, Path: \

Frame 8 (148 bytes on wire, 148 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.592933000
    Time delta from previous packet: 5.595281000 seconds
    Time since reference or first frame: 5.595281000 seconds
```

```
    Frame Number: 8
    Packet Length: 148 bytes
    Capture Length: 148 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 134
    Identification: 0x595a (22874)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cf1 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 0, Ack: 0, Len: 82
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 0    (relative sequence number)
    Next sequence number: 82    (relative sequence number)
    Acknowledgement number: 0    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x623e [correct]
```

```
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526492
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 78
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 10
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 123
```

```
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 10
        Total Data Count: 0
        Max Parameter Count: 2
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: QUERY_PATH_INFO (0x0005)
        Byte Count (BCC): 13
        Padding: 000000
        QUERY_PATH_INFO Parameters
            Level of Interest: Query File Basic Info (257)
            Reserved: 00000000
            File Name: \

No.     Time        Source                Destination           Protocol Info
      9 5.598739    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=0 Ack=82 Win=64158 Len=0 TSV=1545526513
TSER=636883955

Frame 9 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.596391000
    Time delta from previous packet: 0.003458000 seconds
    Time since reference or first frame: 5.598739000 seconds
    Frame Number: 9
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
```

```
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9c99 (40089)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1a04 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 0, Ack: 82, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 0    (relative sequence number)
    Acknowledgement number: 82    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64158
    Checksum: 0x76b2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     10 5.601067    192.168.1.108         192.168.1.106         SMB      Trans2
Response, QUERY_PATH_INFO

Frame 10 (166 bytes on wire, 166 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.598719000
    Time delta from previous packet: 0.005786000 seconds
```

```
    Time since reference or first frame: 5.601067000 seconds
    Frame Number: 10
    Packet Length: 166 bytes
    Capture Length: 166 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 152
    Identification: 0x9c9a (40090)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x199f [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 0, Ack: 82, Len: 100
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 0    (relative sequence number)
    Next sequence number: 100    (relative sequence number)
    Acknowledgement number: 82    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
```

```
    Checksum: 0x954e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 96
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 8
        Time from request: 0.005786000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
```

```
        Process ID: 1
        User ID: 100
        Multiplex ID: 123
    Trans2 Response (0x32)
        Subcommand: QUERY_PATH_INFO (0x0005)
        Word Count (WCT): 10
        Total Parameter Count: 2
        Total Data Count: 36
        Reserved: 0000
        Parameter Count: 2
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 36
        Data Offset: 60
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 41
        Padding: 00
        QUERY_PATH_INFO Parameters
            EA Error offset: 0
        Padding: 0000
        QUERY_PATH_INFO Data

No.     Time        Source                Destination           Protocol Info
     11 5.601109    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=82 Ack=100 Win=65535 Len=0 TSV=636883955 TSER=1545526513

Frame 11 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.598761000
    Time delta from previous packet: 0.000042000 seconds
    Time since reference or first frame: 5.601109000 seconds
    Frame Number: 11
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
```

```
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x595b (22875)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d42 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 82, Ack: 100, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 82    (relative sequence number)
    Acknowledgement number: 100    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x70ed [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     12 5.601614    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.bash_history

Frame 12 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.599266000
    Time delta from previous packet: 0.000547000 seconds
    Time since reference or first frame: 5.601614000 seconds
    Frame Number: 12
    Packet Length: 180 bytes
    Capture Length: 180 bytes
```

```
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x595c (22876)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5ccf [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 82, Ack: 100, Len: 114
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 82    (relative sequence number)
    Next sequence number: 196    (relative sequence number)
    Acknowledgement number: 100    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xfec9 [correct]
    Options: (12 bytes)
        NOP
        NOP
```

```
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 14
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 124
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 42
```

```
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 42
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 45
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.bash_history

No.     Time        Source                Destination           Protocol Info
     13 5.606021    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=100 Ack=196 Win=64126 Len=0 TSV=1545526513
TSER=636883955

Frame 13 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.603673000
    Time delta from previous packet: 0.004407000 seconds
    Time since reference or first frame: 5.606021000 seconds
    Frame Number: 13
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
```

```
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9c9b (40091)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1a02 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 100, Ack: 196, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 100    (relative sequence number)
    Acknowledgement number: 196    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64126
    Checksum: 0x75fc [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     14 5.608512    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: .bash_history

Frame 14 (258 bytes on wire, 258 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.606164000
    Time delta from previous packet: 0.006898000 seconds
```

```
    Time since reference or first frame: 5.608512000 seconds
    Frame Number: 14
    Packet Length: 258 bytes
    Capture Length: 258 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 244
    Identification: 0x9c9c (40092)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1941 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 100, Ack: 196, Len: 192
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 100    (relative sequence number)
    Next sequence number: 292    (relative sequence number)
    Acknowledgement number: 196    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
```

```
    Checksum: 0xefb2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 188
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 12
        Time from request: 0.006898000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
```

```
        Process ID: 1
        User ID: 100
        Multiplex ID: 124
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 120
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 120
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 133
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
     15 5.608561    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=196 Ack=292 Win=65535 Len=0 TSV=636883955 TSER=1545526513

Frame 15 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.606213000
    Time delta from previous packet: 0.000049000 seconds
    Time since reference or first frame: 5.608561000 seconds
    Frame Number: 15
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
```

```
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x595d (22877)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d40 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 196, Ack: 292, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 196    (relative sequence number)
    Acknowledgement number: 292    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x6fbb [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     16 5.608942    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.CFUserTextEncoding

Frame 16 (192 bytes on wire, 192 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.606594000
```

```
    Time delta from previous packet: 0.000430000 seconds
    Time since reference or first frame: 5.608942000 seconds
    Frame Number: 16
    Packet Length: 192 bytes
    Capture Length: 192 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 178
    Identification: 0x595e (22878)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cc1 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 196, Ack: 292, Len: 126
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 196    (relative sequence number)
    Next sequence number: 322    (relative sequence number)
    Acknowledgement number: 292    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
```

```
    Window size: 65535
    Checksum: 0x175a [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 122
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 18
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
```

```
        User ID: 100
        Multiplex ID: 125
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 54
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 54
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 57
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.CFUserTextEncoding

No.     Time        Source                Destination           Protocol Info
     17 5.613174    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=292 Ack=322 Win=64114 Len=0 TSV=1545526513
TSER=636883955

Frame 17 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.610826000
    Time delta from previous packet: 0.004232000 seconds
    Time since reference or first frame: 5.613174000 seconds
    Frame Number: 17
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
```

```
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9c9d (40093)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1a00 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 292, Ack: 322, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 292    (relative sequence number)
    Acknowledgement number: 322    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64114
    Checksum: 0x74ca [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
```

```
     18 5.615872    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: .CFUserTextEncoding

Frame 18 (270 bytes on wire, 270 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.613524000
    Time delta from previous packet: 0.006930000 seconds
    Time since reference or first frame: 5.615872000 seconds
    Frame Number: 18
    Packet Length: 270 bytes
    Capture Length: 270 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 256
    Identification: 0x9c9e (40094)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1933 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 292, Ack: 322, Len: 204
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 292    (relative sequence number)
    Next sequence number: 496    (relative sequence number)
    Acknowledgement number: 322    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x9de7 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 200
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 16
        Time from request: 0.006930000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
```

```
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 125
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 132
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 132
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 145
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
     19 5.615964    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=322 Ack=496 Win=65535 Len=0 TSV=636883955 TSER=1545526513

Frame 19 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.613616000
    Time delta from previous packet: 0.000092000 seconds
    Time since reference or first frame: 5.615964000 seconds
    Frame Number: 19
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
```

```
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x595f (22879)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d3e [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 322, Ack: 496, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 322    (relative sequence number)
    Acknowledgement number: 496    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x6e71 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis
```

```
No.     Time        Source                Destination           Protocol Info
     20 5.616287    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.DS_Store

Frame 20 (172 bytes on wire, 172 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.613939000
    Time delta from previous packet: 0.000415000 seconds
    Time since reference or first frame: 5.616287000 seconds
    Frame Number: 20
    Packet Length: 172 bytes
    Capture Length: 172 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 158
    Identification: 0x5960 (22880)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cd3 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 322, Ack: 496, Len: 106
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 322    (relative sequence number)
    Next sequence number: 428    (relative sequence number)
    Acknowledgement number: 496    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
```

```
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x0678 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 102
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 22
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
```

```
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 126
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 34
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 34
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 37
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.DS_Store

No.     Time        Source                Destination           Protocol Info
     21 5.620751    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=496 Ack=428 Win=64134 Len=0 TSV=1545526513
TSER=636883955

Frame 21 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.618403000
    Time delta from previous packet: 0.004464000 seconds
    Time since reference or first frame: 5.620751000 seconds
```

```
    Frame Number: 21
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9c9f (40095)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19fe [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 496, Ack: 428, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 496    (relative sequence number)
    Acknowledgement number: 428    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64134
    Checksum: 0x7380 [correct]
    Options: (12 bytes)
```

```
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     22 5.622926    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: .DS_Store

Frame 22 (250 bytes on wire, 250 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.620578000
    Time delta from previous packet: 0.006639000 seconds
    Time since reference or first frame: 5.622926000 seconds
    Frame Number: 22
    Packet Length: 250 bytes
    Capture Length: 250 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 236
    Identification: 0x9ca0 (40096)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1945 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 496, Ack: 428, Len: 184
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 496    (relative sequence number)
    Next sequence number: 680    (relative sequence number)
```

```
    Acknowledgement number: 428    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x5e3a [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 180
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 20
        Time from request: 0.006639000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
```

```
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 126
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 112
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 112
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 125
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
     23 5.622994    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=428 Ack=680 Win=65535 Len=0 TSV=636883955 TSER=1545526513

Frame 23 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.620646000
    Time delta from previous packet: 0.000068000 seconds
```

```
    Time since reference or first frame: 5.622994000 seconds
    Frame Number: 23
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5961 (22881)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d3c [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 428, Ack: 680, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 428    (relative sequence number)
    Acknowledgement number: 680    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x6d4f [correct]
```

```
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     24 5.623288    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.emacs.d

Frame 24 (170 bytes on wire, 170 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.620940000
    Time delta from previous packet: 0.000362000 seconds
    Time since reference or first frame: 5.623288000 seconds
    Frame Number: 24
    Packet Length: 170 bytes
    Capture Length: 170 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 156
    Identification: 0x5962 (22882)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cd3 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 428, Ack: 680, Len: 104
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 428    (relative sequence number)
```

```
    Next sequence number: 532    (relative sequence number)
    Acknowledgement number: 680    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x6c60 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 100
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 26
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
```

```
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 127
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 32
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 32
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 35
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.emacs.d

No.     Time        Source                Destination           Protocol Info
```

```
     25 5.627090    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=680 Ack=532 Win=64136 Len=0 TSV=1545526513
TSER=636883955

Frame 25 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.624742000
    Time delta from previous packet: 0.003802000 seconds
    Time since reference or first frame: 5.627090000 seconds
    Frame Number: 25
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9ca1 (40097)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19fc [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 680, Ack: 532, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 680    (relative sequence number)
    Acknowledgement number: 532    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64136
    Checksum: 0x725e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     26 5.629514    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: .emacs.d

Frame 26 (250 bytes on wire, 250 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.627166000
    Time delta from previous packet: 0.006226000 seconds
    Time since reference or first frame: 5.629514000 seconds
    Frame Number: 26
    Packet Length: 250 bytes
    Capture Length: 250 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 236
    Identification: 0x9ca2 (40098)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1943 [correct]
```

```
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 680, Ack: 532, Len: 184
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 680    (relative sequence number)
    Next sequence number: 864    (relative sequence number)
    Acknowledgement number: 532    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x4cf9 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 180
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 24
        Time from request: 0.006226000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
```

```
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 127
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 112
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 112
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 125
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data
```

```
No.     Time        Source                Destination           Protocol Info
     27 5.629583    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=532 Ack=864 Win=65535 Len=0 TSV=636883955 TSER=1545526513

Frame 27 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.627235000
    Time delta from previous packet: 0.000069000 seconds
    Time since reference or first frame: 5.629583000 seconds
    Frame Number: 27
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5963 (22883)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d3a [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 532, Ack: 864, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 532    (relative sequence number)
    Acknowledgement number: 864    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
```

```
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x6c2f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     28 5.629980    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.lpoptions

Frame 28 (174 bytes on wire, 174 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.627632000
    Time delta from previous packet: 0.000466000 seconds
    Time since reference or first frame: 5.629980000 seconds
    Frame Number: 28
    Packet Length: 174 bytes
    Capture Length: 174 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 160
    Identification: 0x5964 (22884)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
```

```
    Header checksum: 0x5ccd [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 532, Ack: 864, Len: 108
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 532    (relative sequence number)
    Next sequence number: 640    (relative sequence number)
    Acknowledgement number: 864    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1d2b [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 104
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 30
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
```

```
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 128
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 36
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 36
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 39
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
```

```
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.lpoptions

No.     Time        Source                Destination           Protocol Info
     29 5.634406    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=864 Ack=640 Win=64132 Len=0 TSV=1545526513
TSER=636883955

Frame 29 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.632058000
    Time delta from previous packet: 0.004426000 seconds
    Time since reference or first frame: 5.634406000 seconds
    Frame Number: 29
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9ca3 (40099)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19fa [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 864, Ack: 640, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 864    (relative sequence number)
    Acknowledgement number: 640    (relative ack number)
```

```
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64132
    Checksum: 0x713e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     30 5.636882    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: .lpoptions

Frame 30 (254 bytes on wire, 254 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.634534000
    Time delta from previous packet: 0.006902000 seconds
    Time since reference or first frame: 5.636882000 seconds
    Frame Number: 30
    Packet Length: 254 bytes
    Capture Length: 254 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 240
    Identification: 0x9ca4 (40100)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
```

```
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x193d [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 864, Ack: 640, Len: 188
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 864    (relative sequence number)
    Next sequence number: 1052    (relative sequence number)
    Acknowledgement number: 640    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x2a50 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 184
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 28
        Time from request: 0.006902000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
```

```
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 128
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 116
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 116
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 129
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
```

```
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
     31 5.636956    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=640 Ack=1052 Win=65535 Len=0 TSV=636883955 TSER=1545526513

Frame 31 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.634608000
    Time delta from previous packet: 0.000074000 seconds
    Time since reference or first frame: 5.636956000 seconds
    Frame Number: 31
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5965 (22885)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d38 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 640, Ack: 1052, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 640    (relative sequence number)
```

```
    Acknowledgement number: 1052    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x6b07 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     32 5.637157    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.mysql_history

Frame 32 (182 bytes on wire, 182 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.634809000
    Time delta from previous packet: 0.000275000 seconds
    Time since reference or first frame: 5.637157000 seconds
    Frame Number: 32
    Packet Length: 182 bytes
    Capture Length: 182 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 168
    Identification: 0x5966 (22886)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
```

```
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cc3 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 640, Ack: 1052, Len: 116
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 640    (relative sequence number)
    Next sequence number: 756    (relative sequence number)
    Acknowledgement number: 1052    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5bd9 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 112
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 34
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
```

```
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 129
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 44
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 44
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 47
```

```
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.mysql_history

No.     Time        Source                Destination           Protocol Info
     33 5.641543    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=1052 Ack=756 Win=64124 Len=0 TSV=1545526513
TSER=636883955

Frame 33 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.639195000
    Time delta from previous packet: 0.004386000 seconds
    Time since reference or first frame: 5.641543000 seconds
    Frame Number: 33
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9ca5 (40101)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19f8 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
```

```
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 1052, Ack: 756, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 1052    (relative sequence number)
    Acknowledgement number: 756    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64124
    Checksum: 0x7016 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     34 5.644112    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: .mysql_history

Frame 34 (262 bytes on wire, 262 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.641764000
    Time delta from previous packet: 0.006955000 seconds
    Time since reference or first frame: 5.644112000 seconds
    Frame Number: 34
    Packet Length: 262 bytes
    Capture Length: 262 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
```

```
        .... ...0 = ECN-CE: 0
    Total Length: 248
    Identification: 0x9ca6 (40102)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1933 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 1052, Ack: 756, Len: 196
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 1052    (relative sequence number)
    Next sequence number: 1248    (relative sequence number)
    Acknowledgement number: 756    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x320f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 192
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 32
        Time from request: 0.006955000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
```

```
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 129
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 124
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 124
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
```

```
        Byte Count (BCC): 137
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
     35 5.644207    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=756 Ack=1248 Win=65535 Len=0 TSV=636883955 TSER=1545526513

Frame 35 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.641859000
    Time delta from previous packet: 0.000095000 seconds
    Time since reference or first frame: 5.644207000 seconds
    Frame Number: 35
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5967 (22887)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d36 [correct]
    Source: 192.168.1.106 (192.168.1.106)
```

```
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 756, Ack: 1248, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 756    (relative sequence number)
    Acknowledgement number: 1248    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x69cf [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     36 5.644485    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.ssh

Frame 36 (162 bytes on wire, 162 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.642137000
    Time delta from previous packet: 0.000373000 seconds
    Time since reference or first frame: 5.644485000 seconds
    Frame Number: 36
    Packet Length: 162 bytes
    Capture Length: 162 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
```

```
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 148
    Identification: 0x5968 (22888)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cd5 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 756, Ack: 1248, Len: 96
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 756    (relative sequence number)
    Next sequence number: 852    (relative sequence number)
    Acknowledgement number: 1248    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xb309 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 92
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 38
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
```

```
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 130
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 24
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 24
        Parameter Offset: 68
```

```
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 27
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.ssh

No.     Time        Source                Destination           Protocol Info
     37 5.648932    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=1248 Ack=852 Win=64144 Len=0 TSV=1545526513
TSER=636883955

Frame 37 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.646584000
    Time delta from previous packet: 0.004447000 seconds
    Time since reference or first frame: 5.648932000 seconds
    Frame Number: 37
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9ca7 (40103)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
```

```
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19f6 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 1248, Ack: 852, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 1248    (relative sequence number)
    Acknowledgement number: 852    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64144
    Checksum: 0x6ede [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     38 5.651737    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: .ssh

Frame 38 (242 bytes on wire, 242 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.649389000
    Time delta from previous packet: 0.007252000 seconds
    Time since reference or first frame: 5.651737000 seconds
    Frame Number: 38
    Packet Length: 242 bytes
    Capture Length: 242 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
```

```
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 228
    Identification: 0x9ca8 (40104)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1945 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 1248, Ack: 852, Len: 176
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 1248    (relative sequence number)
    Next sequence number: 1424    (relative sequence number)
    Acknowledgement number: 852    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x9f4c [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 172
SMB (Server Message Block Protocol)
    SMB Header
```

```
        Server Component: SMB
        Response to: 36
        Time from request: 0.007252000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 130
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 104
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
```

```
        Data Count: 104
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 117
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
     39 5.651788    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=852 Ack=1424 Win=65535 Len=0 TSV=636883955 TSER=1545526513

Frame 39 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.649440000
    Time delta from previous packet: 0.000051000 seconds
    Time since reference or first frame: 5.651788000 seconds
    Frame Number: 39
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5969 (22889)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
```

```
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d34 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 852, Ack: 1424, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 852    (relative sequence number)
    Acknowledgement number: 1424    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x68bf [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     40 5.652247    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.TemporaryItems

Frame 40 (184 bytes on wire, 184 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.649899000
    Time delta from previous packet: 0.000510000 seconds
    Time since reference or first frame: 5.652247000 seconds
    Frame Number: 40
    Packet Length: 184 bytes
    Capture Length: 184 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 170
    Identification: 0x596a (22890)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cbd [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 852, Ack: 1424, Len: 118
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 852    (relative sequence number)
    Next sequence number: 970    (relative sequence number)
    Acknowledgement number: 1424    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x3987 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 114
```

```
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 42
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 131
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 46
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
```

```
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 46
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 49
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.TemporaryItems

No.     Time        Source                Destination           Protocol Info
     41 5.656749    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=1424 Ack=970 Win=64122 Len=0 TSV=1545526513
TSER=636883955

Frame 41 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.654401000
    Time delta from previous packet: 0.004502000 seconds
    Time since reference or first frame: 5.656749000 seconds
    Frame Number: 41
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
```

```
    Identification: 0x9ca9 (40105)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19f4 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 1424, Ack: 970, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 1424    (relative sequence number)
    Acknowledgement number: 970    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64122
    Checksum: 0x6dce [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     42 5.659154    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: .TemporaryItems

Frame 42 (262 bytes on wire, 262 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.656806000
    Time delta from previous packet: 0.006907000 seconds
    Time since reference or first frame: 5.659154000 seconds
    Frame Number: 42
    Packet Length: 262 bytes
    Capture Length: 262 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
```

```
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 248
    Identification: 0x9caa (40106)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x192f [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 1424, Ack: 970, Len: 196
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 1424    (relative sequence number)
    Next sequence number: 1620    (relative sequence number)
    Acknowledgement number: 970    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x404e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
```

```
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 192
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 40
        Time from request: 0.006907000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 131
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
```

```
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 124
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 124
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 137
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
     43 5.659208    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=970 Ack=1620 Win=65535 Len=0 TSV=636883955 TSER=1545526513

Frame 43 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.656860000
    Time delta from previous packet: 0.000054000 seconds
    Time since reference or first frame: 5.659208000 seconds
    Frame Number: 43
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
```

```
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x596b (22891)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d32 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 970, Ack: 1620, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 970    (relative sequence number)
    Acknowledgement number: 1620    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x6785 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     44 5.659718    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.Trash

Frame 44 (166 bytes on wire, 166 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.657370000
    Time delta from previous packet: 0.000564000 seconds
    Time since reference or first frame: 5.659718000 seconds
    Frame Number: 44
    Packet Length: 166 bytes
    Capture Length: 166 bytes
```

```
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 152
    Identification: 0x596c (22892)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5ccd [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 970, Ack: 1620, Len: 100
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 970    (relative sequence number)
    Next sequence number: 1070    (relative sequence number)
    Acknowledgement number: 1620    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xfaaa [correct]
    Options: (12 bytes)
        NOP
        NOP
```

```
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 96
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 46
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 132
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 28
```

```
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 28
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 31
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.Trash

No.     Time        Source                Destination           Protocol Info
     45 5.665697    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=1620 Ack=1070 Win=64140 Len=0 TSV=1545526513
TSER=636883955

Frame 45 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.663349000
    Time delta from previous packet: 0.005979000 seconds
    Time since reference or first frame: 5.665697000 seconds
    Frame Number: 45
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
```

```
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cab (40107)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19f2 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 1620, Ack: 1070, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 1620    (relative sequence number)
    Acknowledgement number: 1070    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64140
    Checksum: 0x6c94 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     46 5.668335    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: .Trash

Frame 46 (246 bytes on wire, 246 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.665987000
    Time delta from previous packet: 0.008617000 seconds
```

```
    Time since reference or first frame: 5.668335000 seconds
    Frame Number: 46
    Packet Length: 246 bytes
    Capture Length: 246 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 232
    Identification: 0x9cac (40108)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x193d [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 1620, Ack: 1070, Len: 180
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 1620    (relative sequence number)
    Next sequence number: 1800    (relative sequence number)
    Acknowledgement number: 1070    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
```

```
    Checksum: 0x7d22 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 176
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 44
        Time from request: 0.008617000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
```

```
        Process ID: 1
        User ID: 100
        Multiplex ID: 132
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 108
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 108
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 121
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
     47 5.668403    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=1070 Ack=1800 Win=65535 Len=0 TSV=636883955
TSER=1545526513

Frame 47 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.666055000
    Time delta from previous packet: 0.000068000 seconds
    Time since reference or first frame: 5.668403000 seconds
    Frame Number: 47
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x596d (22893)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d30 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 1070, Ack: 1800, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 1070    (relative sequence number)
    Acknowledgement number: 1800    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x666d [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     48 5.668842    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.viminfo
```

```
Frame 48 (170 bytes on wire, 170 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.666494000
    Time delta from previous packet: 0.000507000 seconds
    Time since reference or first frame: 5.668842000 seconds
    Frame Number: 48
    Packet Length: 170 bytes
    Capture Length: 170 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 156
    Identification: 0x596e (22894)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cc7 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 1070, Ack: 1800, Len: 104
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 1070    (relative sequence number)
    Next sequence number: 1174    (relative sequence number)
    Acknowledgement number: 1800    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
```

```
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x027e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 100
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 50
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
```

```
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 133
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 32
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 32
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 35
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.viminfo

No.     Time        Source                Destination           Protocol Info
     49 5.674123    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=1800 Ack=1174 Win=64136 Len=0 TSV=1545526513
TSER=636883955

Frame 49 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.671775000
    Time delta from previous packet: 0.005281000 seconds
    Time since reference or first frame: 5.674123000 seconds
    Frame Number: 49
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
```

```
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cad (40109)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19f0 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 1800, Ack: 1174, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 1800    (relative sequence number)
    Acknowledgement number: 1174    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64136
    Checksum: 0x6b7c [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis
```

```
No.     Time        Source                Destination           Protocol Info
     50 5.676537    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: .viminfo

Frame 50 (250 bytes on wire, 250 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.674189000
    Time delta from previous packet: 0.007695000 seconds
    Time since reference or first frame: 5.676537000 seconds
    Frame Number: 50
    Packet Length: 250 bytes
    Capture Length: 250 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 236
    Identification: 0x9cae (40110)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1937 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 1800, Ack: 1174, Len: 184
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 1800    (relative sequence number)
    Next sequence number: 1984    (relative sequence number)
    Acknowledgement number: 1174    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
```

```
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xa44e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 180
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 48
        Time from request: 0.007695000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
```

```
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 133
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 112
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 112
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 125
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
     51 5.676625    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=1174 Ack=1984 Win=65535 Len=0 TSV=636883955
TSER=1545526513

Frame 51 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.674277000
    Time delta from previous packet: 0.000088000 seconds
    Time since reference or first frame: 5.676625000 seconds
    Frame Number: 51
    Packet Length: 66 bytes
```

```
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x596f (22895)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d2e [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 1174, Ack: 1984, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 1174    (relative sequence number)
    Acknowledgement number: 1984    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x654d [correct]
    Options: (12 bytes)
        NOP
        NOP
```

```
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     52 5.676914    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Backups

Frame 52 (168 bytes on wire, 168 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.674566000
    Time delta from previous packet: 0.000377000 seconds
    Time since reference or first frame: 5.676914000 seconds
    Frame Number: 52
    Packet Length: 168 bytes
    Capture Length: 168 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 154
    Identification: 0x5970 (22896)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cc7 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 1174, Ack: 1984, Len: 102
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 1174    (relative sequence number)
    Next sequence number: 1276    (relative sequence number)
    Acknowledgement number: 1984    (relative ack number)
    Header length: 32 bytes
```

```
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5d68 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 98
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 54
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
```

```
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 134
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 30
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 30
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 33
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Backups

No.     Time        Source                Destination           Protocol Info
     53 5.681745    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=1984 Ack=1276 Win=64138 Len=0 TSV=1545526513
TSER=636883955

Frame 53 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.679397000
```

```
    Time delta from previous packet: 0.004831000 seconds
    Time since reference or first frame: 5.681745000 seconds
    Frame Number: 53
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9caf (40111)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19ee [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 1984, Ack: 1276, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 1984    (relative sequence number)
    Acknowledgement number: 1276    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64138
```

```
    Checksum: 0x6a5c [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     54 5.684161    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Backups

Frame 54 (246 bytes on wire, 246 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.681813000
    Time delta from previous packet: 0.007247000 seconds
    Time since reference or first frame: 5.684161000 seconds
    Frame Number: 54
    Packet Length: 246 bytes
    Capture Length: 246 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 232
    Identification: 0x9cb0 (40112)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1939 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 1984, Ack: 1276, Len: 180
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
```

```
    Sequence number: 1984    (relative sequence number)
    Next sequence number: 2164    (relative sequence number)
    Acknowledgement number: 1276    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x0a32 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 176
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 52
        Time from request: 0.007247000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
```

```
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 134
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 108
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 108
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 121
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
     55 5.684211    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=1276 Ack=2164 Win=65535 Len=0 TSV=636883955
TSER=1545526513
```

```
Frame 55 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.681863000
    Time delta from previous packet: 0.000050000 seconds
    Time since reference or first frame: 5.684211000 seconds
    Frame Number: 55
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5971 (22897)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d2c [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 1276, Ack: 2164, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 1276    (relative sequence number)
    Acknowledgement number: 2164    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
```

```
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x6433 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     56 5.684699    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Desktop

Frame 56 (168 bytes on wire, 168 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.682351000
    Time delta from previous packet: 0.000538000 seconds
    Time since reference or first frame: 5.684699000 seconds
    Frame Number: 56
    Packet Length: 168 bytes
    Capture Length: 168 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 154
    Identification: 0x5972 (22898)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cc5 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 1276, Ack: 2164, Len: 102
```

```
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 1276    (relative sequence number)
    Next sequence number: 1378    (relative sequence number)
    Acknowledgement number: 2164    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x4a4e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 98
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 58
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
```

```
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 135
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 30
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 30
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 33
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Desktop

No.     Time        Source                Destination           Protocol Info
```

```
     57 5.688497    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=2164 Ack=1378 Win=64138 Len=0 TSV=1545526513
TSER=636883955

Frame 57 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.686149000
    Time delta from previous packet: 0.003798000 seconds
    Time since reference or first frame: 5.688497000 seconds
    Frame Number: 57
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cb1 (40113)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19ec [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 2164, Ack: 1378, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 2164    (relative sequence number)
    Acknowledgement number: 1378    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64138
    Checksum: 0x6942 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     58 5.691417    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Desktop

Frame 58 (246 bytes on wire, 246 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.689069000
    Time delta from previous packet: 0.006718000 seconds
    Time since reference or first frame: 5.691417000 seconds
    Frame Number: 58
    Packet Length: 246 bytes
    Capture Length: 246 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 232
    Identification: 0x9cb2 (40114)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1937 [correct]
```

```
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 2164, Ack: 1378, Len: 180
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 2164    (relative sequence number)
    Next sequence number: 2344    (relative sequence number)
    Acknowledgement number: 1378    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x7503 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 176
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 56
        Time from request: 0.006718000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
```

```
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 135
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 108
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 108
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 121
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data
```

```
No.     Time        Source                Destination           Protocol Info
     59 5.691463    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=1378 Ack=2344 Win=65535 Len=0 TSV=636883955
TSER=1545526513

Frame 59 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.689115000
    Time delta from previous packet: 0.000046000 seconds
    Time since reference or first frame: 5.691463000 seconds
    Frame Number: 59
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5973 (22899)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d2a [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 1378, Ack: 2344, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 1378    (relative sequence number)
    Acknowledgement number: 2344    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
```

```
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x6319 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     60 5.691854    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Documents

Frame 60 (172 bytes on wire, 172 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.689506000
    Time delta from previous packet: 0.000437000 seconds
    Time since reference or first frame: 5.691854000 seconds
    Frame Number: 60
    Packet Length: 172 bytes
    Capture Length: 172 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 158
    Identification: 0x5974 (22900)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x5cbf [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 1378, Ack: 2344, Len: 106
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 1378    (relative sequence number)
    Next sequence number: 1484    (relative sequence number)
    Acknowledgement number: 2344    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x701f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 102
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 62
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
```

```
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 136
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 34
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 34
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 37
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
```

```
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Documents

No.     Time        Source                Destination           Protocol Info
     61 5.696927    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=2344 Ack=1484 Win=64134 Len=0 TSV=1545526513
TSER=636883955

Frame 61 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.694579000
    Time delta from previous packet: 0.005073000 seconds
    Time since reference or first frame: 5.696927000 seconds
    Frame Number: 61
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cb3 (40115)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19ea [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 2344, Ack: 1484, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 2344    (relative sequence number)
```

```
    Acknowledgement number: 1484    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64134
    Checksum: 0x6828 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     62 5.699418    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Documents

Frame 62 (250 bytes on wire, 250 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.697070000
    Time delta from previous packet: 0.007564000 seconds
    Time since reference or first frame: 5.699418000 seconds
    Frame Number: 62
    Packet Length: 250 bytes
    Capture Length: 250 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 236
    Identification: 0x9cb4 (40116)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
```

```
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1931 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 2344, Ack: 1484, Len: 184
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 2344    (relative sequence number)
    Next sequence number: 2528    (relative sequence number)
    Acknowledgement number: 1484    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xcc52 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 180
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 60
        Time from request: 0.007564000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
```

```
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 136
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 112
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 112
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 125
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
```

```
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
     63 5.699461    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=1484 Ack=2528 Win=65535 Len=0 TSV=636883955
TSER=1545526513

Frame 63 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.697113000
    Time delta from previous packet: 0.000043000 seconds
    Time since reference or first frame: 5.699461000 seconds
    Frame Number: 63
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5975 (22901)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d28 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 1484, Ack: 2528, Len: 0
    Source port: 51751 (51751)
```

```
    Destination port: netbios-ssn (139)
    Sequence number: 1484    (relative sequence number)
    Acknowledgement number: 2528    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x61f7 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     64 5.699859    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Library

Frame 64 (168 bytes on wire, 168 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.697511000
    Time delta from previous packet: 0.000441000 seconds
    Time since reference or first frame: 5.699859000 seconds
    Frame Number: 64
    Packet Length: 168 bytes
    Capture Length: 168 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 154
    Identification: 0x5976 (22902)
```

```
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cc1 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 1484, Ack: 2528, Len: 102
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 1484    (relative sequence number)
    Next sequence number: 1586    (relative sequence number)
    Acknowledgement number: 2528    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x4b12 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 98
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 66
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
```

```
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 137
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 30
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 30
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
```

```
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 33
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Library

No.     Time        Source                Destination           Protocol Info
     65 5.703748    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=2528 Ack=1586 Win=64138 Len=0 TSV=1545526513
TSER=636883955

Frame 65 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.701400000
    Time delta from previous packet: 0.003889000 seconds
    Time since reference or first frame: 5.703748000 seconds
    Frame Number: 65
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cb5 (40117)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19e8 [correct]
    Source: 192.168.1.108 (192.168.1.108)
```

```
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 2528, Ack: 1586, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 2528    (relative sequence number)
    Acknowledgement number: 1586    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64138
    Checksum: 0x6706 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     66 5.706590    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Library

Frame 66 (246 bytes on wire, 246 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.704242000
    Time delta from previous packet: 0.006731000 seconds
    Time since reference or first frame: 5.706590000 seconds
    Frame Number: 66
    Packet Length: 246 bytes
    Capture Length: 246 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
```

```
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 232
    Identification: 0x9cb6 (40118)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1933 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 2528, Ack: 1586, Len: 180
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 2528    (relative sequence number)
    Next sequence number: 2708    (relative sequence number)
    Acknowledgement number: 1586    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x7b9e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 176
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 64
        Time from request: 0.006731000 seconds
        SMB Command: Trans2 (0x32)
```

```
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 137
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 108
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 108
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
```

```
        Reserved: 00
        Byte Count (BCC): 121
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
     67 5.706632    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=1586 Ack=2708 Win=65535 Len=0 TSV=636883955
TSER=1545526513

Frame 67 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.704284000
    Time delta from previous packet: 0.000042000 seconds
    Time since reference or first frame: 5.706632000 seconds
    Frame Number: 67
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5977 (22903)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
```

```
    Header checksum: 0x5d26 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 1586, Ack: 2708, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 1586    (relative sequence number)
    Acknowledgement number: 2708    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x60dd [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     68 5.707035    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Movies

Frame 68 (166 bytes on wire, 166 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.704687000
    Time delta from previous packet: 0.000445000 seconds
    Time since reference or first frame: 5.707035000 seconds
    Frame Number: 68
    Packet Length: 166 bytes
    Capture Length: 166 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
```

```
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 152
    Identification: 0x5978 (22904)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cc1 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 1586, Ack: 2708, Len: 100
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 1586    (relative sequence number)
    Next sequence number: 1686    (relative sequence number)
    Acknowledgement number: 2708    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xab02 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 96
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 70
```

```
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 138
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 28
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
```

```
        Parameter Count: 28
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 31
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Movies

No.     Time        Source                Destination           Protocol Info
     69 5.711326    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=2708 Ack=1686 Win=64140 Len=0 TSV=1545526513
TSER=636883955

Frame 69 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.708978000
    Time delta from previous packet: 0.004291000 seconds
    Time since reference or first frame: 5.711326000 seconds
    Frame Number: 69
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cb7 (40119)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
```

```
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19e6 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 2708, Ack: 1686, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 2708    (relative sequence number)
    Acknowledgement number: 1686    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64140
    Checksum: 0x65ec [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     70 5.714127    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Movies

Frame 70 (246 bytes on wire, 246 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.711779000
    Time delta from previous packet: 0.007092000 seconds
    Time since reference or first frame: 5.714127000 seconds
    Frame Number: 70
    Packet Length: 246 bytes
    Capture Length: 246 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 232
    Identification: 0x9cb8 (40120)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1931 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 2708, Ack: 1686, Len: 180
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 2708    (relative sequence number)
    Next sequence number: 2888    (relative sequence number)
    Acknowledgement number: 1686    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xea56 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 176
```

```
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 68
        Time from request: 0.007092000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 138
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 108
        Reserved: 0000
        Parameter Count: 10
```

```
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 108
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 121
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
     71 5.714167    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=1686 Ack=2888 Win=65535 Len=0 TSV=636883955
TSER=1545526513

Frame 71 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.711819000
    Time delta from previous packet: 0.000040000 seconds
    Time since reference or first frame: 5.714167000 seconds
    Frame Number: 71
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5979 (22905)
    Flags: 0x04 (Don't Fragment)
```

```
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d24 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 1686, Ack: 2888, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 1686    (relative sequence number)
    Acknowledgement number: 2888    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5fc5 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     72 5.714542    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Music

Frame 72 (164 bytes on wire, 164 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.712194000
    Time delta from previous packet: 0.000415000 seconds
    Time since reference or first frame: 5.714542000 seconds
    Frame Number: 72
    Packet Length: 164 bytes
    Capture Length: 164 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
```

```
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 150
    Identification: 0x597a (22906)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cc1 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 1686, Ack: 2888, Len: 98
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 1686    (relative sequence number)
    Next sequence number: 1784    (relative sequence number)
    Acknowledgement number: 2888    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1af5 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
```

```
        .... ...0 = Add 0 to length
    Length: 94
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 74
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 139
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 26
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
```

```
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 26
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 29
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Music

No.     Time        Source                Destination           Protocol Info
     73 5.718976    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=2888 Ack=1784 Win=64142 Len=0 TSV=1545526513
TSER=636883955

Frame 73 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.716628000
    Time delta from previous packet: 0.004434000 seconds
    Time since reference or first frame: 5.718976000 seconds
    Frame Number: 73
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
```

```
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cb9 (40121)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19e4 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 2888, Ack: 1784, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 2888    (relative sequence number)
    Acknowledgement number: 1784    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64142
    Checksum: 0x64d4 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     74 5.721715    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Music

Frame 74 (242 bytes on wire, 242 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.719367000
    Time delta from previous packet: 0.007173000 seconds
    Time since reference or first frame: 5.721715000 seconds
    Frame Number: 74
    Packet Length: 242 bytes
    Capture Length: 242 bytes
```

```
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 228
    Identification: 0x9cba (40122)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1933 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 2888, Ack: 1784, Len: 176
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 2888    (relative sequence number)
    Next sequence number: 3064    (relative sequence number)
    Acknowledgement number: 1784    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x5385 [correct]
    Options: (12 bytes)
        NOP
        NOP
```

```
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 172
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 72
        Time from request: 0.007173000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 139
    Trans2 Response (0x32)
```

```
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 104
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 104
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 117
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
     75 5.721776    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=1784 Ack=3064 Win=65535 Len=0 TSV=636883955
TSER=1545526513

Frame 75 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.719428000
    Time delta from previous packet: 0.000061000 seconds
    Time since reference or first frame: 5.721776000 seconds
    Frame Number: 75
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
```

```
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x597b (22907)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d22 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 1784, Ack: 3064, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 1784    (relative sequence number)
    Acknowledgement number: 3064    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5eb3 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     76 5.722233    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \mysql

Frame 76 (164 bytes on wire, 164 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.719885000
    Time delta from previous packet: 0.000518000 seconds
    Time since reference or first frame: 5.722233000 seconds
    Frame Number: 76
```

```
    Packet Length: 164 bytes
    Capture Length: 164 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 150
    Identification: 0x597c (22908)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cbf [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 1784, Ack: 3064, Len: 98
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 1784    (relative sequence number)
    Next sequence number: 1882    (relative sequence number)
    Acknowledgement number: 3064    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xe3e2 [correct]
    Options: (12 bytes)
```

```
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 94
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 78
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 140
    Trans2 Request (0x32)
```

```
        Word Count (WCT): 15
        Total Parameter Count: 26
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 26
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 29
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \mysql

No.     Time        Source                Destination           Protocol Info
     77 5.726248    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=3064 Ack=1882 Win=64142 Len=0 TSV=1545526513
TSER=636883955

Frame 77 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.723900000
    Time delta from previous packet: 0.004015000 seconds
    Time since reference or first frame: 5.726248000 seconds
    Frame Number: 77
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cbb (40123)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19e2 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 3064, Ack: 1882, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 3064    (relative sequence number)
    Acknowledgement number: 1882    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64142
    Checksum: 0x63c2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     78 5.729034    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: mysql
```

```
Frame 78 (242 bytes on wire, 242 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.726686000
    Time delta from previous packet: 0.006801000 seconds
    Time since reference or first frame: 5.729034000 seconds
    Frame Number: 78
    Packet Length: 242 bytes
    Capture Length: 242 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 228
    Identification: 0x9cbc (40124)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1931 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 3064, Ack: 1882, Len: 176
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 3064    (relative sequence number)
    Next sequence number: 3240    (relative sequence number)
    Acknowledgement number: 1882    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
```

```
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xcdb7 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 172
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 76
        Time from request: 0.006801000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
```

```
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 140
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 104
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 104
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 117
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
     79 5.729080    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=1882 Ack=3240 Win=65535 Len=0 TSV=636883955
TSER=1545526513

Frame 79 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.726732000
    Time delta from previous packet: 0.000046000 seconds
    Time since reference or first frame: 5.729080000 seconds
    Frame Number: 79
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
```

```
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x597d (22909)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d20 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 1882, Ack: 3240, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 1882    (relative sequence number)
    Acknowledgement number: 3240    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5da1 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
```

```
     80 5.729426    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Picture 1.png

Frame 80 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.727078000
    Time delta from previous packet: 0.000392000 seconds
    Time since reference or first frame: 5.729426000 seconds
    Frame Number: 80
    Packet Length: 180 bytes
    Capture Length: 180 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x597e (22910)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cad [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 1882, Ack: 3240, Len: 114
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 1882    (relative sequence number)
    Next sequence number: 1996    (relative sequence number)
    Acknowledgement number: 3240    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x777e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 82
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
```

```
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 141
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 42
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 42
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 45
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Picture 1.png

No.     Time        Source                Destination           Protocol Info
     81 5.733774    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=3240 Ack=1996 Win=64126 Len=0 TSV=1545526513
TSER=636883955

Frame 81 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.731426000
    Time delta from previous packet: 0.004348000 seconds
    Time since reference or first frame: 5.733774000 seconds
    Frame Number: 81
    Packet Length: 66 bytes
```

```
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cbd (40125)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19e0 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 3240, Ack: 1996, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 3240    (relative sequence number)
    Acknowledgement number: 1996    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64126
    Checksum: 0x62b0 [correct]
    Options: (12 bytes)
        NOP
        NOP
```

```
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     82 5.736326    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Picture 1.png

Frame 82 (258 bytes on wire, 258 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.733978000
    Time delta from previous packet: 0.006900000 seconds
    Time since reference or first frame: 5.736326000 seconds
    Frame Number: 82
    Packet Length: 258 bytes
    Capture Length: 258 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 244
    Identification: 0x9cbe (40126)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x191f [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 3240, Ack: 1996, Len: 192
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 3240    (relative sequence number)
    Next sequence number: 3432    (relative sequence number)
    Acknowledgement number: 1996    (relative ack number)
    Header length: 32 bytes
```

```
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x338f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 188
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 80
        Time from request: 0.006900000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
```

```
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 141
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 120
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 120
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 133
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
     83 5.736419    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=1996 Ack=3432 Win=65535 Len=0 TSV=636883955
TSER=1545526513

Frame 83 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.734071000
    Time delta from previous packet: 0.000093000 seconds
    Time since reference or first frame: 5.736419000 seconds
```

```
    Frame Number: 83
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x597f (22911)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d1e [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 1996, Ack: 3432, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 1996    (relative sequence number)
    Acknowledgement number: 3432    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5c6f [correct]
    Options: (12 bytes)
```

```
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     84 5.736712    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Pictures

Frame 84 (170 bytes on wire, 170 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.734364000
    Time delta from previous packet: 0.000386000 seconds
    Time since reference or first frame: 5.736712000 seconds
    Frame Number: 84
    Packet Length: 170 bytes
    Capture Length: 170 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 156
    Identification: 0x5980 (22912)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cb5 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 1996, Ack: 3432, Len: 104
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 1996    (relative sequence number)
    Next sequence number: 2100    (relative sequence number)
```

```
    Acknowledgement number: 3432    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xc67f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 100
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 86
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
```

```
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 142
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 32
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 32
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 35
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Pictures

No.     Time        Source                Destination           Protocol Info
     85 5.740759    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=3432 Ack=2100 Win=64136 Len=0 TSV=1545526513
TSER=636883955
```

```
Frame 85 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.738411000
    Time delta from previous packet: 0.004047000 seconds
    Time since reference or first frame: 5.740759000 seconds
    Frame Number: 85
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cbf (40127)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19de [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 3432, Ack: 2100, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 3432    (relative sequence number)
    Acknowledgement number: 2100    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
```

```
        .... ...0 = Fin: Not set
    Window size: 64136
    Checksum: 0x617e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     86 5.743342    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Pictures

Frame 86 (250 bytes on wire, 250 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.740994000
    Time delta from previous packet: 0.006630000 seconds
    Time since reference or first frame: 5.743342000 seconds
    Frame Number: 86
    Packet Length: 250 bytes
    Capture Length: 250 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 236
    Identification: 0x9cc0 (40128)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1925 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 3432, Ack: 2100, Len: 184
```

```
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 3432    (relative sequence number)
    Next sequence number: 3616    (relative sequence number)
    Acknowledgement number: 2100    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xfdcf [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 180
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 84
        Time from request: 0.006630000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
```

```
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 142
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 112
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 112
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 125
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
```

```
     87 5.743394    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=2100 Ack=3616 Win=65535 Len=0 TSV=636883955
TSER=1545526513

Frame 87 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.741046000
    Time delta from previous packet: 0.000052000 seconds
    Time since reference or first frame: 5.743394000 seconds
    Frame Number: 87
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5981 (22913)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d1c [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 2100, Ack: 3616, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 2100    (relative sequence number)
    Acknowledgement number: 3616    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5b4f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     88 5.743833    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Public

Frame 88 (166 bytes on wire, 166 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.741485000
    Time delta from previous packet: 0.000491000 seconds
    Time since reference or first frame: 5.743833000 seconds
    Frame Number: 88
    Packet Length: 166 bytes
    Capture Length: 166 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 152
    Identification: 0x5982 (22914)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cb7 [correct]
```

```
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 2100, Ack: 3616, Len: 100
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 2100    (relative sequence number)
    Next sequence number: 2200    (relative sequence number)
    Acknowledgement number: 3616    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xb474 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 96
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 90
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
```

```
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 143
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 28
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 28
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 31
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
```

```
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Public

No.     Time        Source                Destination           Protocol Info
     89 5.748985    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=3616 Ack=2200 Win=64140 Len=0 TSV=1545526513
TSER=636883955

Frame 89 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.746637000
    Time delta from previous packet: 0.005152000 seconds
    Time since reference or first frame: 5.748985000 seconds
    Frame Number: 89
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cc1 (40129)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19dc [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 3616, Ack: 2200, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 3616    (relative sequence number)
    Acknowledgement number: 2200    (relative ack number)
```

```
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64140
    Checksum: 0x605e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     90 5.751673    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Public

Frame 90 (246 bytes on wire, 246 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.749325000
    Time delta from previous packet: 0.007840000 seconds
    Time since reference or first frame: 5.751673000 seconds
    Frame Number: 90
    Packet Length: 246 bytes
    Capture Length: 246 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 232
    Identification: 0x9cc2 (40130)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
```

```
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1927 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 3616, Ack: 2200, Len: 180
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 3616    (relative sequence number)
    Next sequence number: 3796    (relative sequence number)
    Acknowledgement number: 2200    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x41b7 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 176
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 88
        Time from request: 0.007840000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
```

```
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 143
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 108
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 108
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 121
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
```

```
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
     91 5.751725    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=2200 Ack=3796 Win=65535 Len=0 TSV=636883955
TSER=1545526513

Frame 91 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.749377000
    Time delta from previous packet: 0.000052000 seconds
    Time since reference or first frame: 5.751725000 seconds
    Frame Number: 91
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5983 (22915)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d1a [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 2200, Ack: 3796, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
```

```
    Sequence number: 2200    (relative sequence number)
    Acknowledgement number: 3796    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5a37 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     92 5.752385    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.emacs.d\Contents

Frame 92 (188 bytes on wire, 188 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.750037000
    Time delta from previous packet: 0.000712000 seconds
    Time since reference or first frame: 5.752385000 seconds
    Frame Number: 92
    Packet Length: 188 bytes
    Capture Length: 188 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 174
    Identification: 0x5984 (22916)
    Flags: 0x04 (Don't Fragment)
```

```
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c9f [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 2200, Ack: 3796, Len: 122
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 2200    (relative sequence number)
    Next sequence number: 2322    (relative sequence number)
    Acknowledgement number: 3796    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x9dea [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 118
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 94
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
```

```
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 144
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 50
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 50
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
```

```
        Byte Count (BCC): 53
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.emacs.d\Contents

No.     Time        Source                Destination           Protocol Info
     93 5.756519    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=3796 Ack=2322 Win=64118 Len=0 TSV=1545526513
TSER=636883955

Frame 93 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.754171000
    Time delta from previous packet: 0.004134000 seconds
    Time since reference or first frame: 5.756519000 seconds
    Frame Number: 93
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cc3 (40131)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19da [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
```

```
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 3796, Ack: 2322, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 3796    (relative sequence number)
    Acknowledgement number: 2322    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64118
    Checksum: 0x5f46 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     94 5.758574    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Error: STATUS_NO_SUCH_FILE

Frame 94 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.756226000
    Time delta from previous packet: 0.006189000 seconds
    Time since reference or first frame: 5.758574000 seconds
    Frame Number: 94
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
```

```
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9cc4 (40132)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19b2 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 3796, Ack: 2322, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 3796    (relative sequence number)
    Next sequence number: 3835    (relative sequence number)
    Acknowledgement number: 2322    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xe78a [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 92
        Time from request: 0.006189000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_NO_SUCH_FILE (0xc000000f)
```

```
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 144
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
     95 5.758627    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=2322 Ack=3835 Win=65535 Len=0 TSV=636883955
TSER=1545526513

Frame 95 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.756279000
    Time delta from previous packet: 0.000053000 seconds
    Time since reference or first frame: 5.758627000 seconds
```

```
    Frame Number: 95
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5985 (22917)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d18 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 2322, Ack: 3835, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 2322    (relative sequence number)
    Acknowledgement number: 3835    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5996 [correct]
    Options: (12 bytes)
```

```
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     96 5.758889    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.emacs.d\Contents

Frame 96 (188 bytes on wire, 188 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.756541000
    Time delta from previous packet: 0.000315000 seconds
    Time since reference or first frame: 5.758889000 seconds
    Frame Number: 96
    Packet Length: 188 bytes
    Capture Length: 188 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 174
    Identification: 0x5986 (22918)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c9d [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 2322, Ack: 3835, Len: 122
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 2322    (relative sequence number)
    Next sequence number: 2444    (relative sequence number)
```

```
    Acknowledgement number: 3835    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x9c49 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 118
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 98
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
```

```
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 145
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 50
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 50
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 53
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.emacs.d\Contents

No.     Time        Source                Destination           Protocol Info
     97 5.763631    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=3835 Ack=2444 Win=64118 Len=0 TSV=1545526513
TSER=636883955
```

```
Frame 97 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.761283000
    Time delta from previous packet: 0.004742000 seconds
    Time since reference or first frame: 5.763631000 seconds
    Frame Number: 97
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cc5 (40133)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19d8 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 3835, Ack: 2444, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 3835    (relative sequence number)
    Acknowledgement number: 2444    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
```

```
        .... ...0 = Fin: Not set
    Window size: 64118
    Checksum: 0x5ea5 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
     98 5.765366    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Error: STATUS_NO_SUCH_FILE

Frame 98 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.763018000
    Time delta from previous packet: 0.006477000 seconds
    Time since reference or first frame: 5.765366000 seconds
    Frame Number: 98
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9cc6 (40134)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19b0 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 3835, Ack: 2444, Len: 39
```

```
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 3835    (relative sequence number)
    Next sequence number: 3874    (relative sequence number)
    Acknowledgement number: 2444    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xe5e9 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 96
        Time from request: 0.006477000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_NO_SUCH_FILE (0xc000000f)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
```

```
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 145
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
     99 5.765418    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=2444 Ack=3874 Win=65535 Len=0 TSV=636883955
TSER=1545526513

Frame 99 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.763070000
    Time delta from previous packet: 0.000052000 seconds
    Time since reference or first frame: 5.765418000 seconds
    Frame Number: 99
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
```

```
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5987 (22919)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d16 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 2444, Ack: 3874, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 2444    (relative sequence number)
    Acknowledgement number: 3874    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x58f5 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    100 5.768117    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Sites

Frame 100 (164 bytes on wire, 164 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.765769000
    Time delta from previous packet: 0.002751000 seconds
    Time since reference or first frame: 5.768117000 seconds
    Frame Number: 100
```

```
    Packet Length: 164 bytes
    Capture Length: 164 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 150
    Identification: 0x5988 (22920)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cb3 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 2444, Ack: 3874, Len: 98
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 2444    (relative sequence number)
    Next sequence number: 2542    (relative sequence number)
    Acknowledgement number: 3874    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x0625 [correct]
    Options: (12 bytes)
```

```
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 94
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 102
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 146
    Trans2 Request (0x32)
```

```
        Word Count (WCT): 15
        Total Parameter Count: 26
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 26
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 29
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Sites

No.     Time        Source                Destination           Protocol Info
    101 5.771079    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=3874 Ack=2542 Win=64142 Len=0 TSV=1545526513
TSER=636883955

Frame 101 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.768731000
    Time delta from previous packet: 0.002962000 seconds
    Time since reference or first frame: 5.771079000 seconds
    Frame Number: 101
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cc7 (40135)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19d6 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 3874, Ack: 2542, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 3874    (relative sequence number)
    Acknowledgement number: 2542    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64142
    Checksum: 0x5e04 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    102 5.773927    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Sites
```

```
Frame 102 (242 bytes on wire, 242 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.771579000
    Time delta from previous packet: 0.005810000 seconds
    Time since reference or first frame: 5.773927000 seconds
    Frame Number: 102
    Packet Length: 242 bytes
    Capture Length: 242 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 228
    Identification: 0x9cc8 (40136)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1925 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 3874, Ack: 2542, Len: 176
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 3874    (relative sequence number)
    Next sequence number: 4050    (relative sequence number)
    Acknowledgement number: 2542    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
```

```
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xe3e7 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 172
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 100
        Time from request: 0.005810000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
```

```
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 146
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 104
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 104
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 117
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    103 5.774004    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=2542 Ack=4050 Win=65535 Len=0 TSV=636883955
TSER=1545526513

Frame 103 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.771656000
    Time delta from previous packet: 0.000077000 seconds
    Time since reference or first frame: 5.774004000 seconds
    Frame Number: 103
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
```

```
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5989 (22921)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d14 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 2542, Ack: 4050, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 2542    (relative sequence number)
    Acknowledgement number: 4050    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x57e3 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
```

```
    104 5.775297    192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \.DS_Store

Frame 104 (176 bytes on wire, 176 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.772949000
    Time delta from previous packet: 0.001370000 seconds
    Time since reference or first frame: 5.775297000 seconds
    Frame Number: 104
    Packet Length: 176 bytes
    Capture Length: 176 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 162
    Identification: 0x598a (22922)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5ca5 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 2542, Ack: 4050, Len: 110
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 2542    (relative sequence number)
    Next sequence number: 2652    (relative sequence number)
    Acknowledgement number: 4050    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x2689 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 106
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 106
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
```

```
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 147
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Reserved: 00
        File Name Len: 20
        Create Flags: 0x00000000
        Root FID: 0x00000000
        Access Mask: 0x00020001
        Allocation Size: 0
        File Attributes: 0x00000080
        Share Access: 0x00000007
        Disposition: Open (if file exists open it, else fail) (1)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 23
        File Name: \.DS_Store

No.     Time        Source                Destination           Protocol Info
    105 5.779070    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=4050 Ack=2652 Win=64130 Len=0 TSV=1545526513
TSER=636883955

Frame 105 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.776722000
    Time delta from previous packet: 0.003773000 seconds
    Time since reference or first frame: 5.779070000 seconds
    Frame Number: 105
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
```

```
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cc9 (40137)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19d4 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 4050, Ack: 2652, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 4050    (relative sequence number)
    Acknowledgement number: 2652    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64130
    Checksum: 0x5cf2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    106 5.783404    192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x3168

Frame 106 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.781056000
    Time delta from previous packet: 0.008107000 seconds
```

```
    Time since reference or first frame: 5.783404000 seconds
    Frame Number: 106
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9cca (40138)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1968 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 4050, Ack: 2652, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 4050    (relative sequence number)
    Next sequence number: 4157    (relative sequence number)
    Acknowledgement number: 2652    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
```

```
    Checksum: 0xc604 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 103
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 104
        Time from request: 0.008107000 seconds
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
```

```
        Process ID: 1
        User ID: 100
        Multiplex ID: 147
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
        FID: 0x3168
        Create action: The file existed and was opened (1)
        Created: Sep 22, 2006 18:40:31.000000000
        Last Access: Dec 11, 2006 15:20:55.000000000
        Last Write: Dec 10, 2006 01:50:09.000000000
        Change: Dec 10, 2006 01:50:09.000000000
        File Attributes: 0x00000002
        Allocation Size: 1048576
        End Of File: 12292
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    107 5.783480    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=2652 Ack=4157 Win=65535 Len=0 TSV=636883955
TSER=1545526513

Frame 107 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.781132000
    Time delta from previous packet: 0.000076000 seconds
    Time since reference or first frame: 5.783480000 seconds
    Frame Number: 107
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
```

```
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x598b (22923)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d12 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 2652, Ack: 4157, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 2652    (relative sequence number)
    Acknowledgement number: 4157    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x570a [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883955, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    108 5.783672    192.168.1.106         192.168.1.108         SMB      Read
AndX Request, FID: 0x3168, 12292 bytes at offset 0

Frame 108 (129 bytes on wire, 129 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.781324000
    Time delta from previous packet: 0.000268000 seconds
    Time since reference or first frame: 5.783672000 seconds
    Frame Number: 108
    Packet Length: 129 bytes
    Capture Length: 129 bytes
```

```
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 115
    Identification: 0x598c (22924)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cd2 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 2652, Ack: 4157, Len: 63
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 2652    (relative sequence number)
    Next sequence number: 2715    (relative sequence number)
    Acknowledgement number: 4157    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x11b5 [correct]
    Options: (12 bytes)
        NOP
        NOP
```

```
        Time stamp: tsval 636883955, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 59
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 110
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 148
    Read AndX Request (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
```

```
        Reserved: 00
        AndXOffset: 0
        FID: 0x3168
        Offset: 0
        Max Count Low: 12292
        Min Count: 12292
        Max Count High (multiply with 64K): 0
        Remaining: 12292
        High Offset: 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    109 5.788809    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=4157 Ack=2715 Win=64177 Len=0 TSV=1545526513
TSER=636883955

Frame 109 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.786461000
    Time delta from previous packet: 0.005137000 seconds
    Time since reference or first frame: 5.788809000 seconds
    Frame Number: 109
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9ccb (40139)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19d2 [correct]
    Source: 192.168.1.108 (192.168.1.108)
```

```
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 4157, Ack: 2715, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 4157    (relative sequence number)
    Acknowledgement number: 2715    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64177
    Checksum: 0x5c19 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    110 5.797496    192.168.1.108         192.168.1.106         SMB      Read
AndX Response, FID: 0x3168, 12292 bytes

Frame 110 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.795148000
    Time delta from previous packet: 0.013824000 seconds
    Time since reference or first frame: 5.797496000 seconds
    Frame Number: 110
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
```

```
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x9ccc (40140)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1429 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 4157, Ack: 2715, Len: 1448
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 4157    (relative sequence number)
    Next sequence number: 5605    (relative sequence number)
    Acknowledgement number: 2715    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xa94f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    Last frame of this PDU: 119
    Time until the last segment of this PDU: 0.081363000 seconds
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 12351
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 108
```

```
        Time from request: 0.013824000 seconds
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 148
    Read AndX Response (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3168
        Remaining: 65535
        Data Compaction Mode: 0
        Reserved: 0000
        Data Length Low: 12292
        Data Offset: 59
```

```
        Data Length High (multiply with 64K): 0
        Reserved: 000000000000
        Byte Count (BCC): 12292
        File Data: Incomplete. Only 1385 of 12292 bytes

No.     Time        Source                Destination           Protocol Info
    111 5.806242    192.168.1.108         192.168.1.106         TCP
[Continuation to #110] netbios-ssn > 51751 [ACK] Seq=5605 Ack=2715 Win=64240
Len=1448 TSV=1545526513 TSER=636883955

Frame 111 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.803894000
    Time delta from previous packet: 0.008746000 seconds
    Time since reference or first frame: 5.806242000 seconds
    Frame Number: 111
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x9ccd (40141)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1428 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 5605, Ack: 2715, Len: 1448
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 5605    (relative sequence number)
```

```
    Next sequence number: 7053    (relative sequence number)
    Acknowledgement number: 2715    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x4482 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    This is a continuation to the PDU in frame: 110

No.     Time        Source                Destination           Protocol Info
    112 5.818817    192.168.1.108         192.168.1.106         TCP
[Continuation to #110] netbios-ssn > 51751 [ACK] Seq=7053 Ack=2715 Win=64240
Len=1448 TSV=1545526513 TSER=636883955

Frame 112 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.816469000
    Time delta from previous packet: 0.021321000 seconds
    Time since reference or first frame: 5.818817000 seconds
    Frame Number: 112
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x9cce (40142)
```

```
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1427 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 7053, Ack: 2715, Len: 1448
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 7053    (relative sequence number)
    Next sequence number: 8501    (relative sequence number)
    Acknowledgement number: 2715    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x0392 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    This is a continuation to the PDU in frame: 110

No.     Time        Source                Destination           Protocol Info
    113 5.825550    192.168.1.108         192.168.1.106         TCP
[Continuation to #110] netbios-ssn > 51751 [ACK] Seq=8501 Ack=2715 Win=64240
Len=1448 TSV=1545526513 TSER=636883955

Frame 113 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.823202000
    Time delta from previous packet: 0.028054000 seconds
    Time since reference or first frame: 5.825550000 seconds
    Frame Number: 113
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
```

```
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x9ccf (40143)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1426 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 8501, Ack: 2715, Len: 1448
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 8501    (relative sequence number)
    Next sequence number: 9949    (relative sequence number)
    Acknowledgement number: 2715    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xf080 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
```

```
    This is a continuation to the PDU in frame: 110

No.     Time        Source                Destination           Protocol Info
    114 5.833908    192.168.1.108         192.168.1.106         TCP
[Continuation to #110] netbios-ssn > 51751 [ACK] Seq=9949 Ack=2715 Win=64240
Len=1448 TSV=1545526513 TSER=636883955

Frame 114 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.831560000
    Time delta from previous packet: 0.036412000 seconds
    Time since reference or first frame: 5.833908000 seconds
    Frame Number: 114
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x9cd0 (40144)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1425 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 9949, Ack: 2715, Len: 1448
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 9949    (relative sequence number)
    Next sequence number: 11397    (relative sequence number)
    Acknowledgement number: 2715    (relative ack number)
    Header length: 32 bytes
```

```
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xe169 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    This is a continuation to the PDU in frame: 110

No.     Time        Source                Destination           Protocol Info
    115 5.859447    192.168.1.108         192.168.1.106         TCP
[Continuation to #110] netbios-ssn > 51751 [ACK] Seq=11397 Ack=2715 Win=64240
Len=1448 TSV=1545526513 TSER=636883955

Frame 115 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.857099000
    Time delta from previous packet: 0.061951000 seconds
    Time since reference or first frame: 5.859447000 seconds
    Frame Number: 115
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x9cd1 (40145)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
```

```
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1424 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 11397, Ack: 2715, Len: 1448
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 11397    (relative sequence number)
    Next sequence number: 12845    (relative sequence number)
    Acknowledgement number: 2715    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x4036 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    This is a continuation to the PDU in frame: 110

No.     Time        Source                Destination           Protocol Info
    116 5.859536    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=2715 Ack=12845 Win=65535 Len=0 TSV=636883956
TSER=1545526513

Frame 116 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.857188000
    Time delta from previous packet: 0.062040000 seconds
    Time since reference or first frame: 5.859536000 seconds
    Frame Number: 116
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
```

```
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x598d (22925)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d10 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 2715, Ack: 12845, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 2715    (relative sequence number)
    Acknowledgement number: 12845    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x34da [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883956, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
```

```
    117 5.867963    192.168.1.108         192.168.1.106         TCP
[Continuation to #110] netbios-ssn > 51751 [ACK] Seq=12845 Ack=2715 Win=64240
Len=1448 TSV=1545526513 TSER=636883955

Frame 117 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.865615000
    Time delta from previous packet: 0.070467000 seconds
    Time since reference or first frame: 5.867963000 seconds
    Frame Number: 117
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x9cd2 (40146)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1423 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 12845, Ack: 2715, Len: 1448
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 12845    (relative sequence number)
    Next sequence number: 14293    (relative sequence number)
    Acknowledgement number: 2715    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
```

```
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x3442 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    This is a continuation to the PDU in frame: 110

No.     Time        Source                Destination           Protocol Info
    118 5.874797    192.168.1.108         192.168.1.106         TCP
[Continuation to #110] netbios-ssn > 51751 [ACK] Seq=14293 Ack=2715 Win=64240
Len=1448 TSV=1545526513 TSER=636883955

Frame 118 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.872449000
    Time delta from previous packet: 0.077301000 seconds
    Time since reference or first frame: 5.874797000 seconds
    Frame Number: 118
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x9cd3 (40147)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x1422 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 14293, Ack: 2715, Len: 1448
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 14293    (relative sequence number)
    Next sequence number: 15741    (relative sequence number)
    Acknowledgement number: 2715    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x2e9a [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    This is a continuation to the PDU in frame: 110

No.     Time        Source                Destination           Protocol Info
    119 5.878859    192.168.1.108         192.168.1.106         TCP
[Continuation to #110] netbios-ssn > 51751 [PSH, ACK] Seq=15741 Ack=2715
Win=64240 Len=771 TSV=1545526513 TSER=636883955

Frame 119 (837 bytes on wire, 837 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.876511000
    Time delta from previous packet: 0.081363000 seconds
    Time since reference or first frame: 5.878859000 seconds
    Frame Number: 119
    Packet Length: 837 bytes
    Capture Length: 837 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 823
    Identification: 0x9cd4 (40148)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x16c6 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 15741, Ack: 2715, Len: 771
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 15741    (relative sequence number)
    Next sequence number: 16512    (relative sequence number)
    Acknowledgement number: 2715    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x2b8f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526513, tsecr 636883955
    This is a continuation to the PDU in frame: 110

No.     Time        Source                Destination           Protocol Info
```

```
    120 5.878968    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=2715 Ack=16512 Win=65535 Len=0 TSV=636883956
TSER=1545526513

Frame 120 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.876620000
    Time delta from previous packet: 0.081472000 seconds
    Time since reference or first frame: 5.878968000 seconds
    Frame Number: 120
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x598e (22926)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d0f [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 2715, Ack: 16512, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 2715    (relative sequence number)
    Acknowledgement number: 16512    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x2687 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883956, tsecr 1545526513
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    121 5.879160    192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x3168

Frame 121 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.876812000
    Time delta from previous packet: 0.081664000 seconds
    Time since reference or first frame: 5.879160000 seconds
    Frame Number: 121
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
    Identification: 0x598f (22927)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5ce1 [correct]
```

```
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 2715, Ack: 16512, Len: 45
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 2715    (relative sequence number)
    Next sequence number: 2760    (relative sequence number)
    Acknowledgement number: 16512    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xa461 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883956, tsecr 1545526513
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 123
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
```

```
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 149
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x3168
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    122 5.886296    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=16512 Ack=2760 Win=64195 Len=0 TSV=1545526514
TSER=636883956

Frame 122 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.883948000
    Time delta from previous packet: 0.007136000 seconds
    Time since reference or first frame: 5.886296000 seconds
    Frame Number: 122
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
```

```
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cd5 (40149)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19c8 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 16512, Ack: 2760, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 16512    (relative sequence number)
    Acknowledgement number: 2760    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64195
    Checksum: 0x2b95 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526514, tsecr 636883956
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    123 5.888447    192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 123 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.886099000
```

```
    Time delta from previous packet: 0.009287000 seconds
    Time since reference or first frame: 5.888447000 seconds
    Frame Number: 123
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9cd6 (40150)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19a0 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 16512, Ack: 2760, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 16512    (relative sequence number)
    Next sequence number: 16551    (relative sequence number)
    Acknowledgement number: 2760    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
```

```
    Window size: 64240
    Checksum: 0xdd36 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526514, tsecr 636883956
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 121
        Time from request: 0.009287000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
```

```
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 149
    Close Response (0x04)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    124 5.889093    192.168.1.106         192.168.1.108         SMB      Trans2
Request, QUERY_FS_INFO, Info Allocation

Frame 124 (140 bytes on wire, 140 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.886745000
    Time delta from previous packet: 0.000646000 seconds
    Time since reference or first frame: 5.889093000 seconds
    Frame Number: 124
    Packet Length: 140 bytes
    Capture Length: 140 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 126
    Identification: 0x5990 (22928)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cc3 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 2760, Ack: 16551, Len: 74
    Source port: 51751 (51751)
```

```
    Destination port: netbios-ssn (139)
    Sequence number: 2760    (relative sequence number)
    Next sequence number: 2834    (relative sequence number)
    Acknowledgement number: 16551    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x98d3 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883956, tsecr 1545526514
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 70
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 126
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
```

```
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 150
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 2
        Total Data Count: 0
        Max Parameter Count: 4
        Max Data Count: 18
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 2
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: QUERY_FS_INFO (0x0003)
        Byte Count (BCC): 5
        Padding: 000000
        QUERY_FS_INFO Parameters
            Level of Interest: Info Allocation (0x0001)

No.     Time        Source                Destination           Protocol Info
    125 5.892310    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=16551 Ack=2834 Win=64166 Len=0 TSV=1545526514
TSER=636883956

Frame 125 (66 bytes on wire, 66 bytes captured)
```

```
    Arrival Time: Dec 11, 2006 15:20:57.889962000
    Time delta from previous packet: 0.003217000 seconds
    Time since reference or first frame: 5.892310000 seconds
    Frame Number: 125
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cd7 (40151)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19c6 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 16551, Ack: 2834, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 16551    (relative sequence number)
    Acknowledgement number: 2834    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
```

```
    Window size: 64166
    Checksum: 0x2b41 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526514, tsecr 636883956
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    126 5.894229    192.168.1.108         192.168.1.106         SMB      Trans2
Response, QUERY_FS_INFO

Frame 126 (144 bytes on wire, 144 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.891881000
    Time delta from previous packet: 0.005136000 seconds
    Time since reference or first frame: 5.894229000 seconds
    Frame Number: 126
    Packet Length: 144 bytes
    Capture Length: 144 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 130
    Identification: 0x9cd8 (40152)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1977 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 16551, Ack: 2834, Len: 78
    Source port: netbios-ssn (139)
```

```
    Destination port: 51751 (51751)
    Sequence number: 16551    (relative sequence number)
    Next sequence number: 16629    (relative sequence number)
    Acknowledgement number: 2834    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x7328 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526514, tsecr 636883956
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 74
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 124
        Time from request: 0.005136000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
```

```
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 150
    Trans2 Response (0x32)
        Subcommand: QUERY_FS_INFO (0x0003)
        Word Count (WCT): 10
        Total Parameter Count: 0
        Total Data Count: 18
        Reserved: 0000
        Parameter Count: 0
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 18
        Data Offset: 56
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 19
        Padding: 00
        QUERY_FS_INFO Data

No.     Time        Source                Destination           Protocol Info
    127 5.909201    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=2834 Ack=16629 Win=65535 Len=0 TSV=636883956
TSER=1545526514

Frame 127 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:57.906853000
    Time delta from previous packet: 0.014972000 seconds
    Time since reference or first frame: 5.909201000 seconds
    Frame Number: 127
    Packet Length: 66 bytes
    Capture Length: 66 bytes
```

```
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5991 (22929)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5d0c [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 2834, Ack: 16629, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 2834    (relative sequence number)
    Acknowledgement number: 16629    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x259a [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883956, tsecr 1545526514
```

```
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    128 7.337969    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.emacs.d\Contents

Frame 128 (188 bytes on wire, 188 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:59.335621000
    Time delta from previous packet: 1.443740000 seconds
    Time since reference or first frame: 7.337969000 seconds
    Frame Number: 128
    Packet Length: 188 bytes
    Capture Length: 188 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 174
    Identification: 0x59a6 (22950)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c7d [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 2834, Ack: 16629, Len: 122
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 2834    (relative sequence number)
    Next sequence number: 2956    (relative sequence number)
    Acknowledgement number: 16629    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
```

```
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x624b [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883958, tsecr 1545526514
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 118
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 130
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
```

```
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 151
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 50
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 50
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 53
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.emacs.d\Contents

No.     Time        Source                Destination           Protocol Info
    129 7.341480    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=16629 Ack=2956 Win=64118 Len=0 TSV=1545526516
TSER=636883958

Frame 129 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:59.339132000
```

```
    Time delta from previous packet: 0.003511000 seconds
    Time since reference or first frame: 7.341480000 seconds
    Frame Number: 129
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cd9 (40153)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19c4 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 16629, Ack: 2956, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 16629    (relative sequence number)
    Acknowledgement number: 2956    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64118
```

```
    Checksum: 0x2aa5 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526516, tsecr 636883958
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    130 7.343585    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Error: STATUS_NO_SUCH_FILE

Frame 130 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:59.341237000
    Time delta from previous packet: 0.005616000 seconds
    Time since reference or first frame: 7.343585000 seconds
    Frame Number: 130
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9cda (40154)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x199c [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 16629, Ack: 2956, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
```

```
    Sequence number: 16629    (relative sequence number)
    Next sequence number: 16668    (relative sequence number)
    Acknowledgement number: 2956    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xabe9 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526516, tsecr 636883958
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 128
        Time from request: 0.005616000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_NO_SUCH_FILE (0xc000000f)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
```

```
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 151
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    131 7.343663    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=2956 Ack=16668 Win=65535 Len=0 TSV=636883959
TSER=1545526516

Frame 131 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:59.341315000
    Time delta from previous packet: 0.000078000 seconds
    Time since reference or first frame: 7.343663000 seconds
    Frame Number: 131
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
```

```
    Total Length: 52
    Identification: 0x59a7 (22951)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cf6 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 2956, Ack: 16668, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 2956    (relative sequence number)
    Acknowledgement number: 16668    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x24f4 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883959, tsecr 1545526516
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    132 7.343873    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.emacs.d\Contents

Frame 132 (188 bytes on wire, 188 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:59.341525000
    Time delta from previous packet: 0.000288000 seconds
    Time since reference or first frame: 7.343873000 seconds
    Frame Number: 132
    Packet Length: 188 bytes
    Capture Length: 188 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
```

```
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 174
    Identification: 0x59a8 (22952)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c7b [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 2956, Ack: 16668, Len: 122
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 2956    (relative sequence number)
    Next sequence number: 3078    (relative sequence number)
    Acknowledgement number: 16668    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x60a7 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883959, tsecr 1545526516
```

```
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 118
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 134
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 152
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 50
        Total Data Count: 0
```

```
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 50
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 53
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.emacs.d\Contents

No.     Time        Source                Destination           Protocol Info
    133 7.348659    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=16668 Ack=3078 Win=64118 Len=0 TSV=1545526516
TSER=636883959

Frame 133 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:59.346311000
    Time delta from previous packet: 0.004786000 seconds
    Time since reference or first frame: 7.348659000 seconds
    Frame Number: 133
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
```

```
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cdb (40155)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19c2 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 16668, Ack: 3078, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 16668    (relative sequence number)
    Acknowledgement number: 3078    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64118
    Checksum: 0x2a03 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526516, tsecr 636883959
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    134 7.350339    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Error: STATUS_NO_SUCH_FILE

Frame 134 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:59.347991000
    Time delta from previous packet: 0.006466000 seconds
    Time since reference or first frame: 7.350339000 seconds
```

```
    Frame Number: 134
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9cdc (40156)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x199a [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 16668, Ack: 3078, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 16668    (relative sequence number)
    Next sequence number: 16707    (relative sequence number)
    Acknowledgement number: 3078    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xaa47 [correct]
```

```
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526516, tsecr 636883959
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 132
        Time from request: 0.006466000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_NO_SUCH_FILE (0xc000000f)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
```

```
        User ID: 100
        Multiplex ID: 152
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    135 7.350388    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=3078 Ack=16707 Win=65535 Len=0 TSV=636883959
TSER=1545526516

Frame 135 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:20:59.348040000
    Time delta from previous packet: 0.000049000 seconds
    Time since reference or first frame: 7.350388000 seconds
    Frame Number: 135
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59a9 (22953)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cf4 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 3078, Ack: 16707, Len: 0
    Source port: 51751 (51751)
```

```
    Destination port: netbios-ssn (139)
    Sequence number: 3078    (relative sequence number)
    Acknowledgement number: 16707    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x2453 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883959, tsecr 1545526516
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    136 9.442540    192.168.1.106         192.168.1.108         SMB      Trans2
Request, QUERY_FS_INFO, Info Allocation

Frame 136 (140 bytes on wire, 140 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.440192000
    Time delta from previous packet: 2.092201000 seconds
    Time since reference or first frame: 9.442540000 seconds
    Frame Number: 136
    Packet Length: 140 bytes
    Capture Length: 140 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 126
    Identification: 0x59aa (22954)
```

```
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5ca9 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 3078, Ack: 16707, Len: 74
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 3078    (relative sequence number)
    Next sequence number: 3152    (relative sequence number)
    Acknowledgement number: 16707    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x93f0 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526516
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 70
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 138
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
```

```
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 153
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 2
        Total Data Count: 0
        Max Parameter Count: 4
        Max Data Count: 18
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 2
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
```

```
        Subcommand: QUERY_FS_INFO (0x0003)
        Byte Count (BCC): 5
        Padding: 000000
        QUERY_FS_INFO Parameters
            Level of Interest: Info Allocation (0x0001)

No.     Time        Source                Destination           Protocol Info
    137 9.445990    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=16707 Ack=3152 Win=64166 Len=0 TSV=1545526521
TSER=636883963

Frame 137 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.443642000
    Time delta from previous packet: 0.003450000 seconds
    Time since reference or first frame: 9.445990000 seconds
    Frame Number: 137
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cdd (40157)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19c0 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 16707, Ack: 3152, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
```

```
    Sequence number: 16707    (relative sequence number)
    Acknowledgement number: 3152    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64166
    Checksum: 0x2959 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    138 9.448353    192.168.1.108         192.168.1.106         SMB      Trans2
Response, QUERY_FS_INFO

Frame 138 (144 bytes on wire, 144 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.446005000
    Time delta from previous packet: 0.005813000 seconds
    Time since reference or first frame: 9.448353000 seconds
    Frame Number: 138
    Packet Length: 144 bytes
    Capture Length: 144 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 130
    Identification: 0x9cde (40158)
    Flags: 0x04 (Don't Fragment)
```

```
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1971 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 16707, Ack: 3152, Len: 78
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 16707    (relative sequence number)
    Next sequence number: 16785    (relative sequence number)
    Acknowledgement number: 3152    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x6e40 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 74
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 136
        Time from request: 0.005813000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
```

```
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 153
    Trans2 Response (0x32)
        Subcommand: QUERY_FS_INFO (0x0003)
        Word Count (WCT): 10
        Total Parameter Count: 0
        Total Data Count: 18
        Reserved: 0000
        Parameter Count: 0
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 18
        Data Offset: 56
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 19
        Padding: 00
        QUERY_FS_INFO Data
```

```
No.     Time        Source                Destination           Protocol Info
    139 9.448437    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=3152 Ack=16785 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 139 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.446089000
    Time delta from previous packet: 0.000084000 seconds
    Time since reference or first frame: 9.448437000 seconds
    Frame Number: 139
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59ab (22955)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cf2 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 3152, Ack: 16785, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 3152    (relative sequence number)
    Acknowledgement number: 16785    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
```

```
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x23b2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    140 9.496435    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Audio.mov

Frame 140 (172 bytes on wire, 172 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.494087000
    Time delta from previous packet: 0.048082000 seconds
    Time since reference or first frame: 9.496435000 seconds
    Frame Number: 140
    Packet Length: 172 bytes
    Capture Length: 172 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 158
    Identification: 0x59ac (22956)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
```

```
    Header checksum: 0x5c87 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 3152, Ack: 16785, Len: 106
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 3152    (relative sequence number)
    Next sequence number: 3258    (relative sequence number)
    Acknowledgement number: 16785    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5eb8 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 102
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 142
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
```

```
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 154
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 34
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 34
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 37
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
```

```
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Audio.mov

No.     Time        Source                Destination           Protocol Info
    141 9.499684    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=16785 Ack=3258 Win=64134 Len=0 TSV=1545526521
TSER=636883963

Frame 141 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.497336000
    Time delta from previous packet: 0.003249000 seconds
    Time since reference or first frame: 9.499684000 seconds
    Frame Number: 141
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cdf (40159)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19be [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 16785, Ack: 3258, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 16785    (relative sequence number)
    Acknowledgement number: 3258    (relative ack number)
```

```
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64134
    Checksum: 0x28c1 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    142 9.502143    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Error: STATUS_NO_SUCH_FILE

Frame 142 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.499795000
    Time delta from previous packet: 0.005708000 seconds
    Time since reference or first frame: 9.502143000 seconds
    Frame Number: 142
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9ce0 (40160)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
```

```
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1996 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 16785, Ack: 3258, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 16785    (relative sequence number)
    Next sequence number: 16824    (relative sequence number)
    Acknowledgement number: 3258    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xa715 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 140
        Time from request: 0.005708000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_NO_SUCH_FILE (0xc000000f)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
```

```
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 154
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    143 9.502190    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=3258 Ack=16824 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 143 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.499842000
    Time delta from previous packet: 0.000047000 seconds
    Time since reference or first frame: 9.502190000 seconds
    Frame Number: 143
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
```

```
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59ad (22957)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cf0 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 3258, Ack: 16824, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 3258    (relative sequence number)
    Acknowledgement number: 16824    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x2321 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
```

```
    144 9.502467    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Audio.mov

Frame 144 (172 bytes on wire, 172 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.500119000
    Time delta from previous packet: 0.000324000 seconds
    Time since reference or first frame: 9.502467000 seconds
    Frame Number: 144
    Packet Length: 172 bytes
    Capture Length: 172 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 158
    Identification: 0x59ae (22958)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c85 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 3258, Ack: 16824, Len: 106
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 3258    (relative sequence number)
    Next sequence number: 3364    (relative sequence number)
    Acknowledgement number: 16824    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5d27 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 102
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 146
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
```

```
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 155
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 34
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 34
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 37
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Audio.mov

No.     Time        Source                Destination           Protocol Info
    145 9.506489    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=16824 Ack=3364 Win=64134 Len=0 TSV=1545526521
TSER=636883963

Frame 145 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.504141000
    Time delta from previous packet: 0.004022000 seconds
    Time since reference or first frame: 9.506489000 seconds
    Frame Number: 145
    Packet Length: 66 bytes
```

```
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9ce1 (40161)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19bc [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 16824, Ack: 3364, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 16824    (relative sequence number)
    Acknowledgement number: 3364    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64134
    Checksum: 0x2830 [correct]
    Options: (12 bytes)
        NOP
        NOP
```

```
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    146 9.508471    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Error: STATUS_NO_SUCH_FILE

Frame 146 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.506123000
    Time delta from previous packet: 0.006004000 seconds
    Time since reference or first frame: 9.508471000 seconds
    Frame Number: 146
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9ce2 (40162)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1994 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 16824, Ack: 3364, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 16824    (relative sequence number)
    Next sequence number: 16863    (relative sequence number)
    Acknowledgement number: 3364    (relative ack number)
    Header length: 32 bytes
```

```
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xa584 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 144
        Time from request: 0.006004000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_NO_SUCH_FILE (0xc000000f)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
```

```
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 155
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    147 9.508517    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=3364 Ack=16863 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 147 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.506169000
    Time delta from previous packet: 0.000046000 seconds
    Time since reference or first frame: 9.508517000 seconds
    Frame Number: 147
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59af (22959)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
```

```
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cee [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 3364, Ack: 16863, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 3364    (relative sequence number)
    Acknowledgement number: 16863    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x2290 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    148 9.508653    192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \Audio.mov

Frame 148 (176 bytes on wire, 176 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.506305000
    Time delta from previous packet: 0.000182000 seconds
    Time since reference or first frame: 9.508653000 seconds
    Frame Number: 148
    Packet Length: 176 bytes
    Capture Length: 176 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
```

```
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 162
    Identification: 0x59b0 (22960)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c7f [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 3364, Ack: 16863, Len: 110
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 3364    (relative sequence number)
    Next sequence number: 3474    (relative sequence number)
    Acknowledgement number: 16863    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x8735 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
```

```
    Length: 106
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 150
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 156
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Reserved: 00
        File Name Len: 20
        Create Flags: 0x00000000
```

```
        Root FID: 0x00000000
        Access Mask: 0x00000002
        Allocation Size: 0
        File Attributes: 0x000000a0
        Share Access: 0x00000007
        Disposition: Create (if file exists fail, else create it) (2)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 23
        File Name: \Audio.mov

No.     Time        Source                Destination           Protocol Info
    149 9.513354    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=16863 Ack=3474 Win=64130 Len=0 TSV=1545526521
TSER=636883963

Frame 149 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.511006000
    Time delta from previous packet: 0.004701000 seconds
    Time since reference or first frame: 9.513354000 seconds
    Frame Number: 149
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9ce3 (40163)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19ba [correct]
```

```
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 16863, Ack: 3474, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 16863    (relative sequence number)
    Acknowledgement number: 3474    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64130
    Checksum: 0x279f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    150 9.515851    192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x3169

Frame 150 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.513503000
    Time delta from previous packet: 0.007198000 seconds
    Time since reference or first frame: 9.515851000 seconds
    Frame Number: 150
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
```

```
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9ce4 (40164)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x194e [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 16863, Ack: 3474, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 16863    (relative sequence number)
    Next sequence number: 16970    (relative sequence number)
    Acknowledgement number: 3474    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xbeb2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 103
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 148
        Time from request: 0.007198000 seconds
```

```
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 156
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
        FID: 0x3169
        Create action: The file did not exist but was created (2)
        Created: Dec 11, 2006 15:23:30.000000000
        Last Access: Dec 11, 2006 15:23:30.000000000
        Last Write: Dec 11, 2006 15:23:30.000000000
        Change: Dec 11, 2006 15:23:30.000000000
```

```
        File Attributes: 0x00000020
        Allocation Size: 0
        End Of File: 0
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    151 9.515889    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=3474 Ack=16970 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 151 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.513541000
    Time delta from previous packet: 0.000038000 seconds
    Time since reference or first frame: 9.515889000 seconds
    Frame Number: 151
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59b1 (22961)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cec [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 3474, Ack: 16970, Len: 0
```

```
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 3474    (relative sequence number)
    Acknowledgement number: 16970    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x21b7 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    152 9.515961    192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x3169

Frame 152 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.513613000
    Time delta from previous packet: 0.000110000 seconds
    Time since reference or first frame: 9.515961000 seconds
    Frame Number: 152
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
```

```
    Identification: 0x59b2 (22962)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cbe [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 3474, Ack: 16970, Len: 45
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 3474    (relative sequence number)
    Next sequence number: 3519    (relative sequence number)
    Acknowledgement number: 16970    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x9790 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 154
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
```

```
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 157
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x3169
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    153 9.522805    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=16970 Ack=3519 Win=64195 Len=0 TSV=1545526521
TSER=636883963

Frame 153 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.520457000
    Time delta from previous packet: 0.006844000 seconds
    Time since reference or first frame: 9.522805000 seconds
    Frame Number: 153
    Packet Length: 66 bytes
    Capture Length: 66 bytes
```

```
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9ce5 (40165)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19b8 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 16970, Ack: 3519, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 16970    (relative sequence number)
    Acknowledgement number: 3519    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64195
    Checksum: 0x26c6 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
```

```
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    154 9.524116    192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 154 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.521768000
    Time delta from previous packet: 0.008155000 seconds
    Time since reference or first frame: 9.524116000 seconds
    Frame Number: 154
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9ce6 (40166)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1990 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 16970, Ack: 3519, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 16970    (relative sequence number)
    Next sequence number: 17009    (relative sequence number)
    Acknowledgement number: 3519    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
```

```
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xd067 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 152
        Time from request: 0.008155000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
```

```
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 157
    Close Response (0x04)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    155 9.524198    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=3519 Ack=17009 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 155 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.521850000
    Time delta from previous packet: 0.000082000 seconds
    Time since reference or first frame: 9.524198000 seconds
    Frame Number: 155
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59b3 (22963)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
```

```
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cea [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 3519, Ack: 17009, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 3519    (relative sequence number)
    Acknowledgement number: 17009    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x2163 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    156 9.524346    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Audio.mov

Frame 156 (172 bytes on wire, 172 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.521998000
    Time delta from previous packet: 0.000230000 seconds
    Time since reference or first frame: 9.524346000 seconds
    Frame Number: 156
    Packet Length: 172 bytes
    Capture Length: 172 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 158
    Identification: 0x59b4 (22964)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c7f [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 3519, Ack: 17009, Len: 106
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 3519    (relative sequence number)
    Next sequence number: 3625    (relative sequence number)
    Acknowledgement number: 17009    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5869 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 102
```

```
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 158
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 158
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 34
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
```

```
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 34
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 37
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Audio.mov

No.     Time        Source                Destination           Protocol Info
    157 9.528529    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=17009 Ack=3625 Win=64134 Len=0 TSV=1545526521
TSER=636883963

Frame 157 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.526181000
    Time delta from previous packet: 0.004183000 seconds
    Time since reference or first frame: 9.528529000 seconds
    Frame Number: 157
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
```

```
    Identification: 0x9ce7 (40167)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19b6 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17009, Ack: 3625, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17009    (relative sequence number)
    Acknowledgement number: 3625    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64134
    Checksum: 0x2672 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    158 9.531491    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Audio.mov

Frame 158 (250 bytes on wire, 250 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.529143000
    Time delta from previous packet: 0.007145000 seconds
    Time since reference or first frame: 9.531491000 seconds
    Frame Number: 158
    Packet Length: 250 bytes
    Capture Length: 250 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
```

```
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 236
    Identification: 0x9ce8 (40168)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18fd [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17009, Ack: 3625, Len: 184
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17009    (relative sequence number)
    Next sequence number: 17193    (relative sequence number)
    Acknowledgement number: 3625    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x792f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
```

```
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 180
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 156
        Time from request: 0.007145000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 158
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
```

```
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 112
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 112
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 125
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    159 9.531541    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=3625 Ack=17193 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 159 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.529193000
    Time delta from previous packet: 0.000050000 seconds
    Time since reference or first frame: 9.531541000 seconds
    Frame Number: 159
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
```

```
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59b5 (22965)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5ce8 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 3625, Ack: 17193, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 3625    (relative sequence number)
    Acknowledgement number: 17193    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x2041 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    160 9.531800    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \._Audio.mov

Frame 160 (176 bytes on wire, 176 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.529452000
    Time delta from previous packet: 0.000309000 seconds
    Time since reference or first frame: 9.531800000 seconds
    Frame Number: 160
    Packet Length: 176 bytes
```

```
    Capture Length: 176 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 162
    Identification: 0x59b6 (22966)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c79 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 3625, Ack: 17193, Len: 110
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 3625    (relative sequence number)
    Next sequence number: 3735    (relative sequence number)
    Acknowledgement number: 17193    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xc932 [correct]
    Options: (12 bytes)
        NOP
```

```
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 106
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 162
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 159
    Trans2 Request (0x32)
        Word Count (WCT): 15
```

```
        Total Parameter Count: 38
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 38
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 41
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    161 9.536228    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=17193 Ack=3735 Win=64130 Len=0 TSV=1545526521
TSER=636883963

Frame 161 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.533880000
    Time delta from previous packet: 0.004428000 seconds
    Time since reference or first frame: 9.536228000 seconds
    Frame Number: 161
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
```

```
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9ce9 (40169)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19b4 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17193, Ack: 3735, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17193    (relative sequence number)
    Acknowledgement number: 3735    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64130
    Checksum: 0x2550 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    162 9.538012    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Error: STATUS_NO_SUCH_FILE

Frame 162 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.535664000
```

```
    Time delta from previous packet: 0.006212000 seconds
    Time since reference or first frame: 9.538012000 seconds
    Frame Number: 162
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9cea (40170)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x198c [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17193, Ack: 3735, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17193    (relative sequence number)
    Next sequence number: 17232    (relative sequence number)
    Acknowledgement number: 3735    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
```

```
    Window size: 64240
    Checksum: 0x9ea0 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 160
        Time from request: 0.006212000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_NO_SUCH_FILE (0xc000000f)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
```

```
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 159
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    163 9.538064    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=3735 Ack=17232 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 163 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.535716000
    Time delta from previous packet: 0.000052000 seconds
    Time since reference or first frame: 9.538064000 seconds
    Frame Number: 163
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59b7 (22967)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5ce6 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
```

```
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 3735, Ack: 17232, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 3735    (relative sequence number)
    Acknowledgement number: 17232    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1fac [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    164 9.538224    192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \Audio.mov

Frame 164 (176 bytes on wire, 176 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.535876000
    Time delta from previous packet: 0.000212000 seconds
    Time since reference or first frame: 9.538224000 seconds
    Frame Number: 164
    Packet Length: 176 bytes
    Capture Length: 176 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
```

```
        .... ...0 = ECN-CE: 0
    Total Length: 162
    Identification: 0x59b8 (22968)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c77 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 3735, Ack: 17232, Len: 110
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 3735    (relative sequence number)
    Next sequence number: 3845    (relative sequence number)
    Acknowledgement number: 17232    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xa051 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 106
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 166
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
```

```
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 160
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Reserved: 00
        File Name Len: 20
        Create Flags: 0x00000000
        Root FID: 0x00000000
        Access Mask: 0x00020001
        Allocation Size: 0
        File Attributes: 0x00000080
        Share Access: 0x00000007
        Disposition: Open (if file exists open it, else fail) (1)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
```

```
        Security Flags: 0x00
        Byte Count (BCC): 23
        File Name: \Audio.mov

No.     Time        Source                Destination           Protocol Info
    165 9.542773    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=17232 Ack=3845 Win=64130 Len=0 TSV=1545526521
TSER=636883963

Frame 165 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.540425000
    Time delta from previous packet: 0.004549000 seconds
    Time since reference or first frame: 9.542773000 seconds
    Frame Number: 165
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9ceb (40171)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19b2 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17232, Ack: 3845, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17232    (relative sequence number)
    Acknowledgement number: 3845    (relative ack number)
```

```
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64130
    Checksum: 0x24bb [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    166 9.545286    192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x316a

Frame 166 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.542938000
    Time delta from previous packet: 0.007062000 seconds
    Time since reference or first frame: 9.545286000 seconds
    Frame Number: 166
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9cec (40172)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
```

```
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1946 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17232, Ack: 3845, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17232    (relative sequence number)
    Next sequence number: 17339    (relative sequence number)
    Acknowledgement number: 3845    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xb7ce [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 103
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 164
        Time from request: 0.007062000 seconds
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
```

```
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 160
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
        FID: 0x316a
        Create action: The file existed and was opened (1)
        Created: Dec 11, 2006 15:23:30.000000000
        Last Access: Dec 11, 2006 15:23:30.000000000
        Last Write: Dec 11, 2006 15:23:30.000000000
        Change: Dec 11, 2006 15:23:30.000000000
        File Attributes: 0x00000020
        Allocation Size: 0
        End Of File: 0
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0
```

```
No.     Time        Source                Destination           Protocol Info
    167 9.545334    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=3845 Ack=17339 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 167 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.542986000
    Time delta from previous packet: 0.000048000 seconds
    Time since reference or first frame: 9.545334000 seconds
    Frame Number: 167
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59b9 (22969)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5ce4 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 3845, Ack: 17339, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 3845    (relative sequence number)
    Acknowledgement number: 17339    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
```

```
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1ed3 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    168 9.545434    192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x316a

Frame 168 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.543086000
    Time delta from previous packet: 0.000148000 seconds
    Time since reference or first frame: 9.545434000 seconds
    Frame Number: 168
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
    Identification: 0x59ba (22970)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
```

```
    Header checksum: 0x5cb6 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 3845, Ack: 17339, Len: 45
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 3845    (relative sequence number)
    Next sequence number: 3890    (relative sequence number)
    Acknowledgement number: 17339    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x90ab [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 170
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
```

```
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 161
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x316a
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    169 9.550220    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=17339 Ack=3890 Win=64195 Len=0 TSV=1545526521
TSER=636883963

Frame 169 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.547872000
    Time delta from previous packet: 0.004786000 seconds
    Time since reference or first frame: 9.550220000 seconds
    Frame Number: 169
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
```

```
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9ced (40173)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19b0 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17339, Ack: 3890, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17339    (relative sequence number)
    Acknowledgement number: 3890    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64195
    Checksum: 0x23e2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    170 9.551863    192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 170 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.549515000
```

```
    Time delta from previous packet: 0.006429000 seconds
    Time since reference or first frame: 9.551863000 seconds
    Frame Number: 170
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9cee (40174)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1988 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17339, Ack: 3890, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17339    (relative sequence number)
    Next sequence number: 17378    (relative sequence number)
    Acknowledgement number: 3890    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
```

```
    Window size: 64240
    Checksum: 0xc983 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 168
        Time from request: 0.006429000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
```

```
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 161
    Close Response (0x04)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    171 9.551909    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=3890 Ack=17378 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 171 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.549561000
    Time delta from previous packet: 0.000046000 seconds
    Time since reference or first frame: 9.551909000 seconds
    Frame Number: 171
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59bb (22971)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5ce2 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 3890, Ack: 17378, Len: 0
```

```
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 3890    (relative sequence number)
    Acknowledgement number: 17378    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1e7f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    172 9.552810    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \._Audio.mov

Frame 172 (176 bytes on wire, 176 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.550462000
    Time delta from previous packet: 0.000947000 seconds
    Time since reference or first frame: 9.552810000 seconds
    Frame Number: 172
    Packet Length: 176 bytes
    Capture Length: 176 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 162
```

```
    Identification: 0x59bc (22972)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c73 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 3890, Ack: 17378, Len: 110
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 3890    (relative sequence number)
    Next sequence number: 4000    (relative sequence number)
    Acknowledgement number: 17378    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xc470 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 106
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 174
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
```

```
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 162
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 38
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 38
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
```

```
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 41
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    173 9.556523    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=17378 Ack=4000 Win=64130 Len=0 TSV=1545526521
TSER=636883963

Frame 173 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.554175000
    Time delta from previous packet: 0.003713000 seconds
    Time since reference or first frame: 9.556523000 seconds
    Frame Number: 173
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cef (40175)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19ae [correct]
```

```
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17378, Ack: 4000, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17378    (relative sequence number)
    Acknowledgement number: 4000    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64130
    Checksum: 0x238e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    174 9.558808    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Error: STATUS_NO_SUCH_FILE

Frame 174 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.556460000
    Time delta from previous packet: 0.005998000 seconds
    Time since reference or first frame: 9.558808000 seconds
    Frame Number: 174
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
```

```
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9cf0 (40176)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1986 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17378, Ack: 4000, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17378    (relative sequence number)
    Next sequence number: 17417    (relative sequence number)
    Acknowledgement number: 4000    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x99de [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 172
        Time from request: 0.005998000 seconds
```

```
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_NO_SUCH_FILE (0xc000000f)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 162
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    175 9.558876    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=4000 Ack=17417 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 175 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.556528000
```

```
    Time delta from previous packet: 0.000068000 seconds
    Time since reference or first frame: 9.558876000 seconds
    Frame Number: 175
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59bd (22973)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5ce0 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4000, Ack: 17417, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4000    (relative sequence number)
    Acknowledgement number: 17417    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
```

```
    Checksum: 0x1dea [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    176 9.559106    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \._Audio.mov

Frame 176 (176 bytes on wire, 176 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.556758000
    Time delta from previous packet: 0.000298000 seconds
    Time since reference or first frame: 9.559106000 seconds
    Frame Number: 176
    Packet Length: 176 bytes
    Capture Length: 176 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 162
    Identification: 0x59be (22974)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c71 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4000, Ack: 17417, Len: 110
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
```

```
    Sequence number: 4000    (relative sequence number)
    Next sequence number: 4110    (relative sequence number)
    Acknowledgement number: 17417    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xc2db [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 106
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 178
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
```

```
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 163
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 38
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 38
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 41
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
```

```
    177 9.563832    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=17417 Ack=4110 Win=64130 Len=0 TSV=1545526521
TSER=636883963

Frame 177 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.561484000
    Time delta from previous packet: 0.004726000 seconds
    Time since reference or first frame: 9.563832000 seconds
    Frame Number: 177
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cf1 (40177)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19ac [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17417, Ack: 4110, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17417    (relative sequence number)
    Acknowledgement number: 4110    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64130
    Checksum: 0x22f9 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    178 9.565503    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Error: STATUS_NO_SUCH_FILE

Frame 178 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.563155000
    Time delta from previous packet: 0.006397000 seconds
    Time since reference or first frame: 9.565503000 seconds
    Frame Number: 178
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9cf2 (40178)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1984 [correct]
```

```
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17417, Ack: 4110, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17417    (relative sequence number)
    Next sequence number: 17456    (relative sequence number)
    Acknowledgement number: 4110    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x9849 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 176
        Time from request: 0.006397000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_NO_SUCH_FILE (0xc000000f)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
```

```
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 163
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    179 9.565560    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=4110 Ack=17456 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 179 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.563212000
    Time delta from previous packet: 0.000057000 seconds
    Time since reference or first frame: 9.565560000 seconds
    Frame Number: 179
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
```

```
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59bf (22975)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cde [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4110, Ack: 17456, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4110    (relative sequence number)
    Acknowledgement number: 17456    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1d55 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    180 9.565691    192.168.1.106         192.168.1.108         SMB      Trans2
Request, QUERY_PATH_INFO, Query File Basic Info, Path: \

Frame 180 (148 bytes on wire, 148 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.563343000
```

```
    Time delta from previous packet: 0.000188000 seconds
    Time since reference or first frame: 9.565691000 seconds
    Frame Number: 180
    Packet Length: 148 bytes
    Capture Length: 148 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 134
    Identification: 0x59c0 (22976)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c8b [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4110, Ack: 17456, Len: 82
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4110    (relative sequence number)
    Next sequence number: 4192    (relative sequence number)
    Acknowledgement number: 17456    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
```

```
    Window size: 65535
    Checksum: 0xe4da [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 78
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 182
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
```

```
        User ID: 100
        Multiplex ID: 164
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 10
        Total Data Count: 0
        Max Parameter Count: 2
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: QUERY_PATH_INFO (0x0005)
        Byte Count (BCC): 13
        Padding: 000000
        QUERY_PATH_INFO Parameters
            Level of Interest: Query File Basic Info (257)
            Reserved: 00000000
            File Name: \

No.     Time        Source                Destination           Protocol Info
    181 9.570582    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=17456 Ack=4192 Win=64158 Len=0 TSV=1545526521
TSER=636883963

Frame 181 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.568234000
    Time delta from previous packet: 0.004891000 seconds
    Time since reference or first frame: 9.570582000 seconds
    Frame Number: 181
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cf3 (40179)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19aa [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17456, Ack: 4192, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17456    (relative sequence number)
    Acknowledgement number: 4192    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64158
    Checksum: 0x2264 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    182 9.572478    192.168.1.108         192.168.1.106         SMB      Trans2
Response, QUERY_PATH_INFO
```

```
Frame 182 (166 bytes on wire, 166 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.570130000
    Time delta from previous packet: 0.006787000 seconds
    Time since reference or first frame: 9.572478000 seconds
    Frame Number: 182
    Packet Length: 166 bytes
    Capture Length: 166 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 152
    Identification: 0x9cf4 (40180)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1945 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17456, Ack: 4192, Len: 100
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17456    (relative sequence number)
    Next sequence number: 17556    (relative sequence number)
    Acknowledgement number: 4192    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
```

```
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x6260 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 96
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 180
        Time from request: 0.006787000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
```

```
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 164
    Trans2 Response (0x32)
        Subcommand: QUERY_PATH_INFO (0x0005)
        Word Count (WCT): 10
        Total Parameter Count: 2
        Total Data Count: 36
        Reserved: 0000
        Parameter Count: 2
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 36
        Data Offset: 60
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 41
        Padding: 00
        QUERY_PATH_INFO Parameters
            EA Error offset: 0
        Padding: 0000
        QUERY_PATH_INFO Data

No.     Time        Source                Destination           Protocol Info
    183 9.572514    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=4192 Ack=17556 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 183 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.570166000
    Time delta from previous packet: 0.000036000 seconds
    Time since reference or first frame: 9.572514000 seconds
    Frame Number: 183
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
```

```
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59c1 (22977)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cdc [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4192, Ack: 17556, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4192    (relative sequence number)
    Acknowledgement number: 17556    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1c9f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    184 9.572613    192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \._Audio.mov

Frame 184 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.570265000
    Time delta from previous packet: 0.000135000 seconds
```

```
    Time since reference or first frame: 9.572613000 seconds
    Frame Number: 184
    Packet Length: 180 bytes
    Capture Length: 180 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x59c2 (22978)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c69 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4192, Ack: 17556, Len: 114
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4192    (relative sequence number)
    Next sequence number: 4306    (relative sequence number)
    Acknowledgement number: 17556    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
```

```
    Checksum: 0xe537 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 186
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
```

```
        Multiplex ID: 165
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Reserved: 00
        File Name Len: 24
        Create Flags: 0x00000000
        Root FID: 0x00000000
        Access Mask: 0x00000002
        Allocation Size: 0
        File Attributes: 0x000000a2
        Share Access: 0x00000007
        Disposition: Create (if file exists fail, else create it) (2)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 27
        File Name: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    185 9.577572    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=17556 Ack=4306 Win=64126 Len=0 TSV=1545526521
TSER=636883963

Frame 185 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.575224000
    Time delta from previous packet: 0.004959000 seconds
    Time since reference or first frame: 9.577572000 seconds
    Frame Number: 185
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
```

```
    Identification: 0x9cf5 (40181)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19a8 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17556, Ack: 4306, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17556    (relative sequence number)
    Acknowledgement number: 4306    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64126
    Checksum: 0x21ae [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    186 9.580658    192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x316b

Frame 186 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.578310000
    Time delta from previous packet: 0.008045000 seconds
    Time since reference or first frame: 9.580658000 seconds
    Frame Number: 186
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
```

```
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9cf6 (40182)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x193c [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17556, Ack: 4306, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17556    (relative sequence number)
    Next sequence number: 17663    (relative sequence number)
    Acknowledgement number: 4306    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xabbd [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
```

```
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 103
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 184
        Time from request: 0.008045000 seconds
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 165
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
```

```
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
        FID: 0x316b
        Create action: The file did not exist but was created (2)
        Created: Dec 11, 2006 15:23:30.000000000
        Last Access: Dec 11, 2006 15:23:30.000000000
        Last Write: Dec 11, 2006 15:23:30.000000000
        Change: Dec 11, 2006 15:23:30.000000000
        File Attributes: 0x00000022
        Allocation Size: 0
        End Of File: 0
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    187 9.580732    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=4306 Ack=17663 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 187 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.578384000
    Time delta from previous packet: 0.000074000 seconds
    Time since reference or first frame: 9.580732000 seconds
    Frame Number: 187
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59c3 (22979)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
```

```
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cda [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4306, Ack: 17663, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4306    (relative sequence number)
    Acknowledgement number: 17663    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1bc2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    188 9.580858    192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x316b

Frame 188 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.578510000
    Time delta from previous packet: 0.000200000 seconds
    Time since reference or first frame: 9.580858000 seconds
    Frame Number: 188
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
```

```
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
    Identification: 0x59c4 (22980)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cac [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4306, Ack: 17663, Len: 45
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4306    (relative sequence number)
    Next sequence number: 4351    (relative sequence number)
    Acknowledgement number: 17663    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x8899 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
```

```
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 190
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 166
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x316b
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
```

```
    189 9.590285    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=17663 Ack=4351 Win=64195 Len=0 TSV=1545526521
TSER=636883963

Frame 189 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.587937000
    Time delta from previous packet: 0.009427000 seconds
    Time since reference or first frame: 9.590285000 seconds
    Frame Number: 189
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cf7 (40183)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19a6 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17663, Ack: 4351, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17663    (relative sequence number)
    Acknowledgement number: 4351    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64195
    Checksum: 0x20d1 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    190 9.591979    192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 190 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.589631000
    Time delta from previous packet: 0.011121000 seconds
    Time since reference or first frame: 9.591979000 seconds
    Frame Number: 190
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9cf8 (40184)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x197e [correct]
```

```
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17663, Ack: 4351, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17663    (relative sequence number)
    Next sequence number: 17702    (relative sequence number)
    Acknowledgement number: 4351    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xc172 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 188
        Time from request: 0.011121000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
```

```
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 166
    Close Response (0x04)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    191 9.592056    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=4351 Ack=17702 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 191 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.589708000
    Time delta from previous packet: 0.000077000 seconds
    Time since reference or first frame: 9.592056000 seconds
    Frame Number: 191
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
```

```
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59c5 (22981)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cd8 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4351, Ack: 17702, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4351    (relative sequence number)
    Acknowledgement number: 17702    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1b6e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    192 9.592205    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \._Audio.mov

Frame 192 (176 bytes on wire, 176 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.589857000
    Time delta from previous packet: 0.000226000 seconds
```

```
    Time since reference or first frame: 9.592205000 seconds
    Frame Number: 192
    Packet Length: 176 bytes
    Capture Length: 176 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 162
    Identification: 0x59c6 (22982)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c69 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4351, Ack: 17702, Len: 110
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4351    (relative sequence number)
    Next sequence number: 4461    (relative sequence number)
    Acknowledgement number: 17702    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
```

```
    Checksum: 0xbc5f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 106
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 194
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
```

```
        Multiplex ID: 167
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 38
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 38
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 41
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    193 9.596258    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=17702 Ack=4461 Win=64130 Len=0 TSV=1545526521
TSER=636883963

Frame 193 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.593910000
    Time delta from previous packet: 0.004053000 seconds
    Time since reference or first frame: 9.596258000 seconds
    Frame Number: 193
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
```

```
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cf9 (40185)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19a4 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17702, Ack: 4461, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17702    (relative sequence number)
    Acknowledgement number: 4461    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64130
    Checksum: 0x207d [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    194 9.599247    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: ._Audio.mov
```

```
Frame 194 (254 bytes on wire, 254 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.596899000
    Time delta from previous packet: 0.007042000 seconds
    Time since reference or first frame: 9.599247000 seconds
    Frame Number: 194
    Packet Length: 254 bytes
    Capture Length: 254 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 240
    Identification: 0x9cfa (40186)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18e7 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17702, Ack: 4461, Len: 188
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17702    (relative sequence number)
    Next sequence number: 17890    (relative sequence number)
    Acknowledgement number: 4461    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
```

```
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x281e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 184
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 192
        Time from request: 0.007042000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
```

```
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 167
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 116
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 116
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 129
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    195 9.599303    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=4461 Ack=17890 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 195 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.596955000
    Time delta from previous packet: 0.000056000 seconds
    Time since reference or first frame: 9.599303000 seconds
    Frame Number: 195
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
```

```
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59c7 (22983)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cd6 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4461, Ack: 17890, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4461    (relative sequence number)
    Acknowledgement number: 17890    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1a44 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
```

```
    196 9.599560    192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \._Audio.mov

Frame 196 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.597212000
    Time delta from previous packet: 0.000313000 seconds
    Time since reference or first frame: 9.599560000 seconds
    Frame Number: 196
    Packet Length: 180 bytes
    Capture Length: 180 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x59c8 (22984)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c63 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4461, Ack: 17890, Len: 114
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4461    (relative sequence number)
    Next sequence number: 4575    (relative sequence number)
    Acknowledgement number: 17890    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xfbdc [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 198
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
```

```
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 168
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Reserved: 00
        File Name Len: 24
        Create Flags: 0x00000000
        Root FID: 0x00000000
        Access Mask: 0x00020007
        Allocation Size: 0
        File Attributes: 0x00000080
        Share Access: 0x00000007
        Disposition: Open (if file exists open it, else fail) (1)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 27
        File Name: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    197 9.604919    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=17890 Ack=4575 Win=64126 Len=0 TSV=1545526521
TSER=636883963

Frame 197 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.602571000
    Time delta from previous packet: 0.005359000 seconds
    Time since reference or first frame: 9.604919000 seconds
    Frame Number: 197
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
```

```
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cfb (40187)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19a2 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17890, Ack: 4575, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17890    (relative sequence number)
    Acknowledgement number: 4575    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64126
    Checksum: 0x1f53 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    198 9.607307    192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x316c

Frame 198 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.604959000
    Time delta from previous packet: 0.007747000 seconds
```

```
    Time since reference or first frame: 9.607307000 seconds
    Frame Number: 198
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9cfc (40188)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1936 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17890, Ack: 4575, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17890    (relative sequence number)
    Next sequence number: 17997    (relative sequence number)
    Acknowledgement number: 4575    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
```

```
    Checksum: 0xa662 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 103
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 196
        Time from request: 0.007747000 seconds
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
```

```
        Process ID: 1
        User ID: 100
        Multiplex ID: 168
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
        FID: 0x316c
        Create action: The file existed and was opened (1)
        Created: Dec 11, 2006 15:23:30.000000000
        Last Access: Dec 11, 2006 15:23:30.000000000
        Last Write: Dec 11, 2006 15:23:30.000000000
        Change: Dec 11, 2006 15:23:30.000000000
        File Attributes: 0x00000022
        Allocation Size: 0
        End Of File: 0
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    199 9.607364    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=4575 Ack=17997 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 199 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.605016000
    Time delta from previous packet: 0.000057000 seconds
    Time since reference or first frame: 9.607364000 seconds
    Frame Number: 199
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
```

```
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59c9 (22985)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cd4 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4575, Ack: 17997, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4575    (relative sequence number)
    Acknowledgement number: 17997    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1967 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    200 9.607650    192.168.1.106         192.168.1.108         SMB      Write
AndX Request, FID: 0x316c, 82 bytes at offset 0

Frame 200 (216 bytes on wire, 216 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.605302000
    Time delta from previous packet: 0.000343000 seconds
    Time since reference or first frame: 9.607650000 seconds
    Frame Number: 200
    Packet Length: 216 bytes
    Capture Length: 216 bytes
```

```
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 202
    Identification: 0x59ca (22986)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c3d [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4575, Ack: 17997, Len: 150
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4575    (relative sequence number)
    Next sequence number: 4725    (relative sequence number)
    Acknowledgement number: 17997    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xd067 [correct]
    Options: (12 bytes)
        NOP
        NOP
```

```
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 146
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 202
        SMB Command: Write AndX (0x2f)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 169
    Write AndX Request (0x2f)
        Word Count (WCT): 14
        AndXCommand: No further commands (0xff)
```

```
        Reserved: 00
        AndXOffset: 0
        FID: 0x316c
        Offset: 0
        Reserved: 00000000
        Write Mode: 0x0000
        Remaining: 0
        Data Length High (multiply with 64K): 0
        Data Length Low: 82
        Data Offset: 64
        High Offset: 0
        Byte Count (BCC): 83
        Padding: EE
        File Data: 000516070002000000000000000000000000000000000000...

No.     Time        Source                Destination           Protocol Info
    201 9.612054    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=17997 Ack=4725 Win=64090 Len=0 TSV=1545526521
TSER=636883963

Frame 201 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.609706000
    Time delta from previous packet: 0.004404000 seconds
    Time since reference or first frame: 9.612054000 seconds
    Frame Number: 201
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cfd (40189)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
```

```
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x19a0 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17997, Ack: 4725, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17997    (relative sequence number)
    Acknowledgement number: 4725    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64090
    Checksum: 0x1e76 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    202 9.614176    192.168.1.108         192.168.1.106         SMB      Write
AndX Response, FID: 0x316c, 82 bytes

Frame 202 (117 bytes on wire, 117 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.611828000
    Time delta from previous packet: 0.006526000 seconds
    Time since reference or first frame: 9.614176000 seconds
    Frame Number: 202
    Packet Length: 117 bytes
    Capture Length: 117 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
```

```
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 103
    Identification: 0x9cfe (40190)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x196c [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 17997, Ack: 4725, Len: 51
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 17997    (relative sequence number)
    Next sequence number: 18048    (relative sequence number)
    Acknowledgement number: 4725    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x8945 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 47
SMB (Server Message Block Protocol)
    SMB Header
```

```
        Server Component: SMB
        Response to: 200
        Time from request: 0.006526000 seconds
        SMB Command: Write AndX (0x2f)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 169
    Write AndX Response (0x2f)
        Word Count (WCT): 6
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x316c
        Count Low: 82
        Remaining: 0
        Count High (multiply with 64K): 0
```

```
        Reserved: 0000
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    203 9.614264    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=4725 Ack=18048 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 203 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.611916000
    Time delta from previous packet: 0.000088000 seconds
    Time since reference or first frame: 9.614264000 seconds
    Frame Number: 203
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59cb (22987)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cd2 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4725, Ack: 18048, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4725    (relative sequence number)
    Acknowledgement number: 18048    (relative ack number)
    Header length: 32 bytes
```

```
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x189e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    204 9.614478    192.168.1.106         192.168.1.108         SMB      Flush
Request, FID: 0x316c

Frame 204 (107 bytes on wire, 107 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.612130000
    Time delta from previous packet: 0.000302000 seconds
    Time since reference or first frame: 9.614478000 seconds
    Frame Number: 204
    Packet Length: 107 bytes
    Capture Length: 107 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 93
    Identification: 0x59cc (22988)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
```

```
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5ca8 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4725, Ack: 18048, Len: 41
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4725    (relative sequence number)
    Next sequence number: 4766    (relative sequence number)
    Acknowledgement number: 18048    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x827c [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 37
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 207
        SMB Command: Flush (0x05)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
```

```
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 170
    Flush Request (0x05)
        Word Count (WCT): 1
        FID: 0x316c
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    205 9.614552    192.168.1.106         192.168.1.108         SMB      Trans2
Request, QUERY_FS_INFO, Info Allocation

Frame 205 (140 bytes on wire, 140 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.612204000
    Time delta from previous packet: 0.000074000 seconds
    Time since reference or first frame: 9.614552000 seconds
    Frame Number: 205
    Packet Length: 140 bytes
    Capture Length: 140 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 126
    Identification: 0x59cd (22989)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c86 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4766, Ack: 18048, Len: 74
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4766    (relative sequence number)
    Next sequence number: 4840    (relative sequence number)
    Acknowledgement number: 18048    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x7616 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 70
```

```
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 211
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 171
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 2
        Total Data Count: 0
        Max Parameter Count: 4
        Max Data Count: 18
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
```

```
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 2
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: QUERY_FS_INFO (0x0003)
        Byte Count (BCC): 5
        Padding: 000000
        QUERY_FS_INFO Parameters
            Level of Interest: Info Allocation (0x0001)

No.     Time        Source                Destination           Protocol Info
    206 9.619777    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=18048 Ack=4766 Win=64199 Len=0 TSV=1545526521
TSER=636883963

Frame 206 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.617429000
    Time delta from previous packet: 0.005225000 seconds
    Time since reference or first frame: 9.619777000 seconds
    Frame Number: 206
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9cff (40191)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
```

```
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x199e [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18048, Ack: 4766, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18048    (relative sequence number)
    Acknowledgement number: 4766    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64199
    Checksum: 0x1dad [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    207 9.621771    192.168.1.108         192.168.1.106         SMB      Flush
Response

Frame 207 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.619423000
    Time delta from previous packet: 0.007219000 seconds
    Time since reference or first frame: 9.621771000 seconds
    Frame Number: 207
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d00 (40192)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1976 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18048, Ack: 4766, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18048    (relative sequence number)
    Next sequence number: 18087    (relative sequence number)
    Acknowledgement number: 4766    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xb952 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
```

```
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 204
        Time from request: 0.007293000 seconds
        SMB Command: Flush (0x05)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 170
    Flush Response (0x05)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
```

```
    208 9.621816    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=4840 Ack=18087 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 208 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.619468000
    Time delta from previous packet: 0.000045000 seconds
    Time since reference or first frame: 9.621816000 seconds
    Frame Number: 208
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59ce (22990)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5ccf [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4840, Ack: 18087, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4840    (relative sequence number)
    Acknowledgement number: 18087    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1804 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    209 9.621908    192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x316c

Frame 209 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.619560000
    Time delta from previous packet: 0.000137000 seconds
    Time since reference or first frame: 9.621908000 seconds
    Frame Number: 209
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
    Identification: 0x59cf (22991)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5ca1 [correct]
```

```
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4840, Ack: 18087, Len: 45
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4840    (relative sequence number)
    Next sequence number: 4885    (relative sequence number)
    Acknowledgement number: 18087    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x7eda [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 214
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
```

```
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 172
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x316c
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    210 9.623433    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=18087 Ack=4840 Win=64166 Len=0 TSV=1545526521
TSER=636883963

Frame 210 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.621085000
    Time delta from previous packet: 0.001525000 seconds
    Time since reference or first frame: 9.623433000 seconds
    Frame Number: 210
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
```

```
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d01 (40193)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x199c [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18087, Ack: 4840, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18087    (relative sequence number)
    Acknowledgement number: 4840    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64166
    Checksum: 0x1d5d [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    211 9.627832    192.168.1.108         192.168.1.106         SMB      Trans2
Response, QUERY_FS_INFO

Frame 211 (144 bytes on wire, 144 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.625484000
```

```
    Time delta from previous packet: 0.005924000 seconds
    Time since reference or first frame: 9.627832000 seconds
    Frame Number: 211
    Packet Length: 144 bytes
    Capture Length: 144 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 130
    Identification: 0x9d02 (40194)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x194d [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18087, Ack: 4840, Len: 78
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18087    (relative sequence number)
    Next sequence number: 18165    (relative sequence number)
    Acknowledgement number: 4840    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
```

```
    Window size: 64240
    Checksum: 0x5044 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 74
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 205
        Time from request: 0.013280000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
```

```
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 171
    Trans2 Response (0x32)
        Subcommand: QUERY_FS_INFO (0x0003)
        Word Count (WCT): 10
        Total Parameter Count: 0
        Total Data Count: 18
        Reserved: 0000
        Parameter Count: 0
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 18
        Data Offset: 56
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 19
        Padding: 00
        QUERY_FS_INFO Data

No.     Time        Source                Destination           Protocol Info
    212 9.627894    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=4885 Ack=18165 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 212 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.625546000
    Time delta from previous packet: 0.000062000 seconds
    Time since reference or first frame: 9.627894000 seconds
    Frame Number: 212
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
```

```
    Total Length: 52
    Identification: 0x59d0 (22992)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5ccd [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4885, Ack: 18165, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4885    (relative sequence number)
    Acknowledgement number: 18165    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1789 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    213 9.631467    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=18165 Ack=4885 Win=64195 Len=0 TSV=1545526521
TSER=636883963

Frame 213 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.629119000
    Time delta from previous packet: 0.003635000 seconds
    Time since reference or first frame: 9.631467000 seconds
    Frame Number: 213
    Packet Length: 66 bytes
    Capture Length: 66 bytes
```

```
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d03 (40195)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x199a [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18165, Ack: 4885, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18165    (relative sequence number)
    Acknowledgement number: 4885    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64195
    Checksum: 0x1cc5 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
```

```
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    214 9.633337    192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 214 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.630989000
    Time delta from previous packet: 0.005505000 seconds
    Time since reference or first frame: 9.633337000 seconds
    Frame Number: 214
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d04 (40196)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1972 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18165, Ack: 4885, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18165    (relative sequence number)
    Next sequence number: 18204    (relative sequence number)
    Acknowledgement number: 4885    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
```

```
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xb766 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 209
        Time from request: 0.011429000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
```

```
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 172
    Close Response (0x04)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    215 9.633428    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=4885 Ack=18204 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 215 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.631080000
    Time delta from previous packet: 0.000091000 seconds
    Time since reference or first frame: 9.633428000 seconds
    Frame Number: 215
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59d1 (22993)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
```

```
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5ccc [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4885, Ack: 18204, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4885    (relative sequence number)
    Acknowledgement number: 18204    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1762 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    216 9.633758    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \._Audio.mov

Frame 216 (176 bytes on wire, 176 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.631410000
    Time delta from previous packet: 0.000421000 seconds
    Time since reference or first frame: 9.633758000 seconds
    Frame Number: 216
    Packet Length: 176 bytes
    Capture Length: 176 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 162
    Identification: 0x59d2 (22994)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c5d [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4885, Ack: 18204, Len: 110
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4885    (relative sequence number)
    Next sequence number: 4995    (relative sequence number)
    Acknowledgement number: 18204    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xb253 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 106
```

```
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 218
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 173
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 38
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
```

```
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 38
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 41
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    217 9.638074    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=18204 Ack=4995 Win=64130 Len=0 TSV=1545526521
TSER=636883963

Frame 217 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.635726000
    Time delta from previous packet: 0.004316000 seconds
    Time since reference or first frame: 9.638074000 seconds
    Frame Number: 217
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
```

```
    Identification: 0x9d05 (40197)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1998 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18204, Ack: 4995, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18204    (relative sequence number)
    Acknowledgement number: 4995    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64130
    Checksum: 0x1c71 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    218 9.640832    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: ._Audio.mov

Frame 218 (254 bytes on wire, 254 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.638484000
    Time delta from previous packet: 0.007074000 seconds
    Time since reference or first frame: 9.640832000 seconds
    Frame Number: 218
    Packet Length: 254 bytes
    Capture Length: 254 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
```

```
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 240
    Identification: 0x9d06 (40198)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18db [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18204, Ack: 4995, Len: 188
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18204    (relative sequence number)
    Next sequence number: 18392    (relative sequence number)
    Acknowledgement number: 4995    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xbc11 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
```

```
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 184
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 216
        Time from request: 0.007074000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 173
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
```

```
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 116
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 116
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 129
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    219 9.640943    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=4995 Ack=18392 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 219 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.638595000
    Time delta from previous packet: 0.000111000 seconds
    Time since reference or first frame: 9.640943000 seconds
    Frame Number: 219
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
```

```
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59d3 (22995)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cca [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4995, Ack: 18392, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4995    (relative sequence number)
    Acknowledgement number: 18392    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1638 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    220 9.641088    192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \._Audio.mov

Frame 220 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.638740000
    Time delta from previous packet: 0.000256000 seconds
    Time since reference or first frame: 9.641088000 seconds
    Frame Number: 220
    Packet Length: 180 bytes
```

```
    Capture Length: 180 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x59d4 (22996)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c57 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 4995, Ack: 18392, Len: 114
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 4995    (relative sequence number)
    Next sequence number: 5109    (relative sequence number)
    Acknowledgement number: 18392    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xf7d0 [correct]
    Options: (12 bytes)
        NOP
```

```
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 222
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 174
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
```

```
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Reserved: 00
        File Name Len: 24
        Create Flags: 0x00000000
        Root FID: 0x00000000
        Access Mask: 0x00020001
        Allocation Size: 0
        File Attributes: 0x00000080
        Share Access: 0x00000007
        Disposition: Open (if file exists open it, else fail) (1)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 27
        File Name: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    221 9.646613    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=18392 Ack=5109 Win=64126 Len=0 TSV=1545526521
TSER=636883963

Frame 221 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.644265000
    Time delta from previous packet: 0.005525000 seconds
    Time since reference or first frame: 9.646613000 seconds
    Frame Number: 221
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d07 (40199)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
```

```
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1996 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18392, Ack: 5109, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18392    (relative sequence number)
    Acknowledgement number: 5109    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64126
    Checksum: 0x1b47 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    222 9.648968    192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x316d

Frame 222 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.646620000
    Time delta from previous packet: 0.007880000 seconds
    Time since reference or first frame: 9.648968000 seconds
    Frame Number: 222
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
```

```
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9d08 (40200)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x192a [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18392, Ack: 5109, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18392    (relative sequence number)
    Next sequence number: 18499    (relative sequence number)
    Acknowledgement number: 5109    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x3956 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
```

```
    Length: 103
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 220
        Time from request: 0.007880000 seconds
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 174
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
```

```
        FID: 0x316d
        Create action: The file existed and was opened (1)
        Created: Dec 11, 2006 15:23:30.000000000
        Last Access: Dec 11, 2006 15:23:30.000000000
        Last Write: Dec 11, 2006 15:23:30.000000000
        Change: Dec 11, 2006 15:23:30.000000000
        File Attributes: 0x00000022
        Allocation Size: 1048576
        End Of File: 82
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    223 9.649023    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=5109 Ack=18499 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 223 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.646675000
    Time delta from previous packet: 0.000055000 seconds
    Time since reference or first frame: 9.649023000 seconds
    Frame Number: 223
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59d5 (22997)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x5cc8 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5109, Ack: 18499, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5109    (relative sequence number)
    Acknowledgement number: 18499    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x155b [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    224 9.649207    192.168.1.106         192.168.1.108         SMB      Read
AndX Request, FID: 0x316d, 82 bytes at offset 0

Frame 224 (129 bytes on wire, 129 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.646859000
    Time delta from previous packet: 0.000239000 seconds
    Time since reference or first frame: 9.649207000 seconds
    Frame Number: 224
    Packet Length: 129 bytes
    Capture Length: 129 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
```

```
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 115
    Identification: 0x59d6 (22998)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c88 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5109, Ack: 18499, Len: 63
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5109    (relative sequence number)
    Next sequence number: 5172    (relative sequence number)
    Acknowledgement number: 18499    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x4417 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 59
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
```

```
        Response in: 226
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 175
    Read AndX Request (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x316d
        Offset: 0
        Max Count Low: 82
        Min Count: 82
        Max Count High (multiply with 64K): 0
        Remaining: 82
        High Offset: 0
```

```
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    225 9.653579    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=18499 Ack=5172 Win=64177 Len=0 TSV=1545526521
TSER=636883963

Frame 225 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.651231000
    Time delta from previous packet: 0.004372000 seconds
    Time since reference or first frame: 9.653579000 seconds
    Frame Number: 225
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d09 (40201)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1994 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18499, Ack: 5172, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18499    (relative sequence number)
    Acknowledgement number: 5172    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
```

```
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64177
    Checksum: 0x1a6a [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    226 9.655876    192.168.1.108         192.168.1.106         SMB      Read
AndX Response, FID: 0x316d, 82 bytes

Frame 226 (211 bytes on wire, 211 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.653528000
    Time delta from previous packet: 0.006669000 seconds
    Time since reference or first frame: 9.655876000 seconds
    Frame Number: 226
    Packet Length: 211 bytes
    Capture Length: 211 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 197
    Identification: 0x9d0a (40202)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
```

```
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1902 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18499, Ack: 5172, Len: 145
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18499    (relative sequence number)
    Next sequence number: 18644    (relative sequence number)
    Acknowledgement number: 5172    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x47ce [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 141
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 224
        Time from request: 0.006669000 seconds
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
```

```
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 175
    Read AndX Response (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x316d
        Remaining: 65535
        Data Compaction Mode: 0
        Reserved: 0000
        Data Length Low: 82
        Data Offset: 59
        Data Length High (multiply with 64K): 0
        Reserved: 000000000000
        Byte Count (BCC): 82
        File Data: 000516070002000000000000000000000000000000000000...

No.     Time        Source                Destination           Protocol Info
    227 9.655939    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=5172 Ack=18644 Win=65535 Len=0 TSV=636883963
TSER=1545526521
```

```
Frame 227 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.653591000
    Time delta from previous packet: 0.000063000 seconds
    Time since reference or first frame: 9.655939000 seconds
    Frame Number: 227
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59d7 (22999)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cc6 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5172, Ack: 18644, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5172    (relative sequence number)
    Acknowledgement number: 18644    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
```

```
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x148b [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    228 9.656161    192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x316d

Frame 228 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.653813000
    Time delta from previous packet: 0.000285000 seconds
    Time since reference or first frame: 9.656161000 seconds
    Frame Number: 228
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
    Identification: 0x59d8 (23000)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c98 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5172, Ack: 18644, Len: 45
```

```
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5172    (relative sequence number)
    Next sequence number: 5217    (relative sequence number)
    Acknowledgement number: 18644    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x7760 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 230
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
```

```
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 176
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x316d
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    229 9.660134    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=18644 Ack=5217 Win=64195 Len=0 TSV=1545526521
TSER=636883963

Frame 229 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.657786000
    Time delta from previous packet: 0.003973000 seconds
    Time since reference or first frame: 9.660134000 seconds
    Frame Number: 229
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
```

```
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d0b (40203)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1992 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18644, Ack: 5217, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18644    (relative sequence number)
    Acknowledgement number: 5217    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64195
    Checksum: 0x199a [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    230 9.662097    192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 230 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.659749000
    Time delta from previous packet: 0.005936000 seconds
    Time since reference or first frame: 9.662097000 seconds
    Frame Number: 230
    Packet Length: 105 bytes
    Capture Length: 105 bytes
```

```
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d0c (40204)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x196a [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18644, Ack: 5217, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18644    (relative sequence number)
    Next sequence number: 18683    (relative sequence number)
    Acknowledgement number: 5217    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xb03b [correct]
    Options: (12 bytes)
        NOP
        NOP
```

```
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 228
        Time from request: 0.005936000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 176
    Close Response (0x04)
```

```
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    231 9.662138    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=5217 Ack=18683 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 231 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.659790000
    Time delta from previous packet: 0.000041000 seconds
    Time since reference or first frame: 9.662138000 seconds
    Frame Number: 231
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59d9 (23001)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cc4 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5217, Ack: 18683, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5217    (relative sequence number)
    Acknowledgement number: 18683    (relative ack number)
    Header length: 32 bytes
```

```
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1437 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    232 9.662666    192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \._Audio.mov

Frame 232 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.660318000
    Time delta from previous packet: 0.000569000 seconds
    Time since reference or first frame: 9.662666000 seconds
    Frame Number: 232
    Packet Length: 180 bytes
    Capture Length: 180 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x59da (23002)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
```

```
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c51 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5217, Ack: 18683, Len: 114
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5217    (relative sequence number)
    Next sequence number: 5331    (relative sequence number)
    Acknowledgement number: 18683    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xf2cf [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 234
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
```

```
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 177
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Reserved: 00
        File Name Len: 24
        Create Flags: 0x00000000
        Root FID: 0x00000000
        Access Mask: 0x00020001
        Allocation Size: 0
        File Attributes: 0x00000080
        Share Access: 0x00000007
        Disposition: Open (if file exists open it, else fail) (1)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 27
        File Name: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
```

```
    233 9.667009    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=18683 Ack=5331 Win=64126 Len=0 TSV=1545526521
TSER=636883963

Frame 233 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.664661000
    Time delta from previous packet: 0.004343000 seconds
    Time since reference or first frame: 9.667009000 seconds
    Frame Number: 233
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d0d (40205)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1990 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18683, Ack: 5331, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18683    (relative sequence number)
    Acknowledgement number: 5331    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64126
    Checksum: 0x1946 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    234 9.668928    192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x316e

Frame 234 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.666580000
    Time delta from previous packet: 0.006262000 seconds
    Time since reference or first frame: 9.668928000 seconds
    Frame Number: 234
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9d0e (40206)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1924 [correct]
```

```
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18683, Ack: 5331, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18683    (relative sequence number)
    Next sequence number: 18790    (relative sequence number)
    Acknowledgement number: 5331    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x3355 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 103
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 232
        Time from request: 0.006262000 seconds
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
```

```
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 177
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
        FID: 0x316e
        Create action: The file existed and was opened (1)
        Created: Dec 11, 2006 15:23:30.000000000
        Last Access: Dec 11, 2006 15:23:30.000000000
        Last Write: Dec 11, 2006 15:23:30.000000000
        Change: Dec 11, 2006 15:23:30.000000000
        File Attributes: 0x00000022
        Allocation Size: 1048576
        End Of File: 82
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    235 9.669004    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=5331 Ack=18790 Win=65535 Len=0 TSV=636883963
TSER=1545526521
```

```
Frame 235 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.666656000
    Time delta from previous packet: 0.000076000 seconds
    Time since reference or first frame: 9.669004000 seconds
    Frame Number: 235
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59db (23003)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cc2 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5331, Ack: 18790, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5331    (relative sequence number)
    Acknowledgement number: 18790    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
```

```
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x135a [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    236 9.669206    192.168.1.106         192.168.1.108         SMB      Read
AndX Request, FID: 0x316e, 82 bytes at offset 0

Frame 236 (129 bytes on wire, 129 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.666858000
    Time delta from previous packet: 0.000278000 seconds
    Time since reference or first frame: 9.669206000 seconds
    Frame Number: 236
    Packet Length: 129 bytes
    Capture Length: 129 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 115
    Identification: 0x59dc (23004)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c82 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5331, Ack: 18790, Len: 63
```

```
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5331    (relative sequence number)
    Next sequence number: 5394    (relative sequence number)
    Acknowledgement number: 18790    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x3f15 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 59
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 238
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
```

```
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 178
    Read AndX Request (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x316e
        Offset: 0
        Max Count Low: 82
        Min Count: 82
        Max Count High (multiply with 64K): 0
        Remaining: 82
        High Offset: 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    237 9.673753    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=18790 Ack=5394 Win=64177 Len=0 TSV=1545526521
TSER=636883963

Frame 237 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.671405000
    Time delta from previous packet: 0.004547000 seconds
    Time since reference or first frame: 9.673753000 seconds
    Frame Number: 237
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
```

```
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d0f (40207)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x198e [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18790, Ack: 5394, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18790    (relative sequence number)
    Acknowledgement number: 5394    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64177
    Checksum: 0x1869 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    238 9.675807    192.168.1.108         192.168.1.106         SMB      Read
AndX Response, FID: 0x316e, 82 bytes
```

```
Frame 238 (211 bytes on wire, 211 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.673459000
    Time delta from previous packet: 0.006601000 seconds
    Time since reference or first frame: 9.675807000 seconds
    Frame Number: 238
    Packet Length: 211 bytes
    Capture Length: 211 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 197
    Identification: 0x9d10 (40208)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18fc [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18790, Ack: 5394, Len: 145
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18790    (relative sequence number)
    Next sequence number: 18935    (relative sequence number)
    Acknowledgement number: 5394    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
```

```
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x42cd [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 141
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 236
        Time from request: 0.006601000 seconds
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
```

```
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 178
    Read AndX Response (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x316e
        Remaining: 65535
        Data Compaction Mode: 0
        Reserved: 0000
        Data Length Low: 82
        Data Offset: 59
        Data Length High (multiply with 64K): 0
        Reserved: 000000000000
        Byte Count (BCC): 82
        File Data: 000516070002000000000000000000000000000000000000...

No.     Time        Source                Destination           Protocol Info
    239 9.675883    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=5394 Ack=18935 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 239 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.673535000
    Time delta from previous packet: 0.000076000 seconds
    Time since reference or first frame: 9.675883000 seconds
    Frame Number: 239
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
```

```
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59dd (23005)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cc0 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5394, Ack: 18935, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5394    (relative sequence number)
    Acknowledgement number: 18935    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x128a [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    240 9.676088    192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x316e

Frame 240 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.673740000
    Time delta from previous packet: 0.000281000 seconds
    Time since reference or first frame: 9.676088000 seconds
    Frame Number: 240
    Packet Length: 111 bytes
    Capture Length: 111 bytes
```

```
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
    Identification: 0x59de (23006)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c92 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5394, Ack: 18935, Len: 45
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5394    (relative sequence number)
    Next sequence number: 5439    (relative sequence number)
    Acknowledgement number: 18935    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x725e [correct]
    Options: (12 bytes)
        NOP
        NOP
```

```
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 242
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 179
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x316e
```

```
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    241 9.680531    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=18935 Ack=5439 Win=64195 Len=0 TSV=1545526521
TSER=636883963

Frame 241 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.678183000
    Time delta from previous packet: 0.004443000 seconds
    Time since reference or first frame: 9.680531000 seconds
    Frame Number: 241
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d11 (40209)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x198c [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18935, Ack: 5439, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18935    (relative sequence number)
    Acknowledgement number: 5439    (relative ack number)
    Header length: 32 bytes
```

```
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64195
    Checksum: 0x1799 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    242 9.682121    192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 242 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.679773000
    Time delta from previous packet: 0.006033000 seconds
    Time since reference or first frame: 9.682121000 seconds
    Frame Number: 242
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d12 (40210)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
```

```
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1964 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18935, Ack: 5439, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18935    (relative sequence number)
    Next sequence number: 18974    (relative sequence number)
    Acknowledgement number: 5439    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xab3a [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 240
        Time from request: 0.006033000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
```

```
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 179
    Close Response (0x04)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    243 9.682165    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=5439 Ack=18974 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 243 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.679817000
    Time delta from previous packet: 0.000044000 seconds
    Time since reference or first frame: 9.682165000 seconds
    Frame Number: 243
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
```

```
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59df (23007)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cbe [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5439, Ack: 18974, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5439    (relative sequence number)
    Acknowledgement number: 18974    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1236 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    244 9.684129    192.168.1.106         192.168.1.108         SMB      Trans2
Request, QUERY_PATH_INFO, Query File Basic Info, Path: \
```

```
Frame 244 (148 bytes on wire, 148 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.681781000
    Time delta from previous packet: 0.002008000 seconds
    Time since reference or first frame: 9.684129000 seconds
    Frame Number: 244
    Packet Length: 148 bytes
    Capture Length: 148 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 134
    Identification: 0x59e0 (23008)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c6b [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5439, Ack: 18974, Len: 82
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5439    (relative sequence number)
    Next sequence number: 5521    (relative sequence number)
    Acknowledgement number: 18974    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
```

```
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xc9bb [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 78
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 247
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
```

```
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 180
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 10
        Total Data Count: 0
        Max Parameter Count: 2
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: QUERY_PATH_INFO (0x0005)
        Byte Count (BCC): 13
        Padding: 000000
        QUERY_PATH_INFO Parameters
            Level of Interest: Query File Basic Info (257)
            Reserved: 00000000
            File Name: \

No.     Time        Source                Destination           Protocol Info
    245 9.684270    00:17:ab:43:fd:35     Broadcast             ARP      Who has
192.168.1.105?  Gratuitous ARP

Frame 245 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.681922000
    Time delta from previous packet: 0.000141000 seconds
    Time since reference or first frame: 9.684270000 seconds
    Frame Number: 245
    Packet Length: 60 bytes
    Capture Length: 60 bytes
    Protocols in frame: eth:arp
Ethernet II, Src: 00:17:ab:43:fd:35 (00:17:ab:43:fd:35), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: 00:17:ab:43:fd:35 (00:17:ab:43:fd:35)
```

```
    Type: ARP (0x0806)
    Trailer: 000000000000000000000000000000000000
Address Resolution Protocol (request/gratuitous ARP)

No.     Time        Source                Destination           Protocol Info
    246 9.687892    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=18974 Ack=5521 Win=64158 Len=0 TSV=1545526521
TSER=636883963

Frame 246 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.685544000
    Time delta from previous packet: 0.003763000 seconds
    Time since reference or first frame: 9.687892000 seconds
    Frame Number: 246
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d13 (40211)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x198a [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18974, Ack: 5521, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18974    (relative sequence number)
    Acknowledgement number: 5521    (relative ack number)
```

```
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64158
    Checksum: 0x1745 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    247 9.690157    192.168.1.108         192.168.1.106         SMB      Trans2
Response, QUERY_PATH_INFO

Frame 247 (166 bytes on wire, 166 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.687809000
    Time delta from previous packet: 0.006028000 seconds
    Time since reference or first frame: 9.690157000 seconds
    Frame Number: 247
    Packet Length: 166 bytes
    Capture Length: 166 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 152
    Identification: 0x9d14 (40212)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
```

```
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1925 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 18974, Ack: 5521, Len: 100
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 18974    (relative sequence number)
    Next sequence number: 19074    (relative sequence number)
    Acknowledgement number: 5521    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x4741 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 96
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 244
        Time from request: 0.006028000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
```

```
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 180
    Trans2 Response (0x32)
        Subcommand: QUERY_PATH_INFO (0x0005)
        Word Count (WCT): 10
        Total Parameter Count: 2
        Total Data Count: 36
        Reserved: 0000
        Parameter Count: 2
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 36
        Data Offset: 60
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 41
        Padding: 00
        QUERY_PATH_INFO Parameters
            EA Error offset: 0
        Padding: 0000
        QUERY_PATH_INFO Data
```

```
No.     Time        Source                Destination           Protocol Info
    248 9.690204    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=5521 Ack=19074 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 248 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.687856000
    Time delta from previous packet: 0.000047000 seconds
    Time since reference or first frame: 9.690204000 seconds
    Frame Number: 248
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59e1 (23009)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cbc [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5521, Ack: 19074, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5521    (relative sequence number)
    Acknowledgement number: 19074    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
```

```
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1180 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    249 9.690533    192.168.1.106         192.168.1.108         SMB      Trans2
Request, QUERY_FS_INFO, Info Allocation

Frame 249 (140 bytes on wire, 140 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.688185000
    Time delta from previous packet: 0.000376000 seconds
    Time since reference or first frame: 9.690533000 seconds
    Frame Number: 249
    Packet Length: 140 bytes
    Capture Length: 140 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 126
    Identification: 0x59e2 (23010)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x5c71 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5521, Ack: 19074, Len: 74
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5521    (relative sequence number)
    Next sequence number: 5595    (relative sequence number)
    Acknowledgement number: 19074    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x6521 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 70
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 251
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
```

```
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 181
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 2
        Total Data Count: 0
        Max Parameter Count: 4
        Max Data Count: 18
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 2
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: QUERY_FS_INFO (0x0003)
        Byte Count (BCC): 5
        Padding: 000000
        QUERY_FS_INFO Parameters
            Level of Interest: Info Allocation (0x0001)
```

```
No.     Time        Source                Destination           Protocol Info
    250 9.694131    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=19074 Ack=5595 Win=64166 Len=0 TSV=1545526521
TSER=636883963

Frame 250 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.691783000
    Time delta from previous packet: 0.003598000 seconds
    Time since reference or first frame: 9.694131000 seconds
    Frame Number: 250
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d15 (40213)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1988 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19074, Ack: 5595, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19074    (relative sequence number)
    Acknowledgement number: 5595    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
```

```
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64166
    Checksum: 0x168f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    251 9.695826    192.168.1.108         192.168.1.106         SMB      Trans2
Response, QUERY_FS_INFO

Frame 251 (144 bytes on wire, 144 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.693478000
    Time delta from previous packet: 0.005293000 seconds
    Time since reference or first frame: 9.695826000 seconds
    Frame Number: 251
    Packet Length: 144 bytes
    Capture Length: 144 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 130
    Identification: 0x9d16 (40214)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
```

```
    Header checksum: 0x1939 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19074, Ack: 5595, Len: 78
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19074    (relative sequence number)
    Next sequence number: 19152    (relative sequence number)
    Acknowledgement number: 5595    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x3f76 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 74
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 249
        Time from request: 0.005293000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
```

```
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 181
    Trans2 Response (0x32)
        Subcommand: QUERY_FS_INFO (0x0003)
        Word Count (WCT): 10
        Total Parameter Count: 0
        Total Data Count: 18
        Reserved: 0000
        Parameter Count: 0
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 18
        Data Offset: 56
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 19
        Padding: 00
        QUERY_FS_INFO Data

No.     Time        Source                Destination           Protocol Info
    252 9.695881    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=5595 Ack=19152 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 252 (66 bytes on wire, 66 bytes captured)
```

```
    Arrival Time: Dec 11, 2006 15:21:01.693533000
    Time delta from previous packet: 0.000055000 seconds
    Time since reference or first frame: 9.695881000 seconds
    Frame Number: 252
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59e3 (23011)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cba [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5595, Ack: 19152, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5595    (relative sequence number)
    Acknowledgement number: 19152    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
```

```
    Window size: 65535
    Checksum: 0x10e8 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    253 9.697558    192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \._Audio.mov

Frame 253 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.695210000
    Time delta from previous packet: 0.001732000 seconds
    Time since reference or first frame: 9.697558000 seconds
    Frame Number: 253
    Packet Length: 180 bytes
    Capture Length: 180 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x59e4 (23012)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c47 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5595, Ack: 19152, Len: 114
    Source port: 51751 (51751)
```

```
    Destination port: netbios-ssn (139)
    Sequence number: 5595    (relative sequence number)
    Next sequence number: 5709    (relative sequence number)
    Acknowledgement number: 19152    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xea80 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 255
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
```

```
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 182
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Reserved: 00
        File Name Len: 24
        Create Flags: 0x00000000
        Root FID: 0x00000000
        Access Mask: 0x00020001
        Allocation Size: 0
        File Attributes: 0x00000080
        Share Access: 0x00000007
        Disposition: Open (if file exists open it, else fail) (1)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 27
        File Name: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    254 9.700711    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=19152 Ack=5709 Win=64126 Len=0 TSV=1545526521
TSER=636883963

Frame 254 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.698363000
    Time delta from previous packet: 0.003153000 seconds
    Time since reference or first frame: 9.700711000 seconds
    Frame Number: 254
    Packet Length: 66 bytes
```

```
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d17 (40215)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1986 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19152, Ack: 5709, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19152    (relative sequence number)
    Acknowledgement number: 5709    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64126
    Checksum: 0x15f7 [correct]
    Options: (12 bytes)
        NOP
        NOP
```

```
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    255 9.703162    192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x316f

Frame 255 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.700814000
    Time delta from previous packet: 0.005604000 seconds
    Time since reference or first frame: 9.703162000 seconds
    Frame Number: 255
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9d18 (40216)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x191a [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19152, Ack: 5709, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19152    (relative sequence number)
    Next sequence number: 19259    (relative sequence number)
    Acknowledgement number: 5709    (relative ack number)
    Header length: 32 bytes
```

```
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x2a06 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 103
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 253
        Time from request: 0.005604000 seconds
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
```

```
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 182
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
        FID: 0x316f
        Create action: The file existed and was opened (1)
        Created: Dec 11, 2006 15:23:30.000000000
        Last Access: Dec 11, 2006 15:23:30.000000000
        Last Write: Dec 11, 2006 15:23:30.000000000
        Change: Dec 11, 2006 15:23:30.000000000
        File Attributes: 0x00000022
        Allocation Size: 1048576
        End Of File: 82
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    256 9.703208    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=5709 Ack=19259 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 256 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.700860000
    Time delta from previous packet: 0.000046000 seconds
    Time since reference or first frame: 9.703208000 seconds
    Frame Number: 256
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
```

```
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59e5 (23013)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cb8 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5709, Ack: 19259, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5709    (relative sequence number)
    Acknowledgement number: 19259    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x100b [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
```

```
    257 9.703361    192.168.1.106         192.168.1.108         SMB      Read
AndX Request, FID: 0x316f, 82 bytes at offset 0

Frame 257 (129 bytes on wire, 129 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.701013000
    Time delta from previous packet: 0.000199000 seconds
    Time since reference or first frame: 9.703361000 seconds
    Frame Number: 257
    Packet Length: 129 bytes
    Capture Length: 129 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 115
    Identification: 0x59e6 (23014)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c78 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5709, Ack: 19259, Len: 63
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5709    (relative sequence number)
    Next sequence number: 5772    (relative sequence number)
    Acknowledgement number: 19259    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x36c5 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 59
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 259
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
```

```
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 183
    Read AndX Request (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x316f
        Offset: 0
        Max Count Low: 82
        Min Count: 82
        Max Count High (multiply with 64K): 0
        Remaining: 82
        High Offset: 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    258 9.707897    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=19259 Ack=5772 Win=64177 Len=0 TSV=1545526521
TSER=636883963

Frame 258 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.705549000
    Time delta from previous packet: 0.004536000 seconds
    Time since reference or first frame: 9.707897000 seconds
    Frame Number: 258
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
```

```
    Identification: 0x9d19 (40217)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1984 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19259, Ack: 5772, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19259    (relative sequence number)
    Acknowledgement number: 5772    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64177
    Checksum: 0x151a [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    259 9.710492    192.168.1.108         192.168.1.106         SMB      Read
AndX Response, FID: 0x316f, 82 bytes

Frame 259 (211 bytes on wire, 211 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.708144000
    Time delta from previous packet: 0.007131000 seconds
    Time since reference or first frame: 9.710492000 seconds
    Frame Number: 259
    Packet Length: 211 bytes
    Capture Length: 211 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
```

```
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 197
    Identification: 0x9d1a (40218)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18f2 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19259, Ack: 5772, Len: 145
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19259    (relative sequence number)
    Next sequence number: 19404    (relative sequence number)
    Acknowledgement number: 5772    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x3a7e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
```

```
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 141
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 257
        Time from request: 0.007131000 seconds
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 183
    Read AndX Response (0x2e)
        Word Count (WCT): 12
```

```
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x316f
        Remaining: 65535
        Data Compaction Mode: 0
        Reserved: 0000
        Data Length Low: 82
        Data Offset: 59
        Data Length High (multiply with 64K): 0
        Reserved: 000000000000
        Byte Count (BCC): 82
        File Data: 000516070002000000000000000000000000000000000000...

No.     Time        Source                Destination           Protocol Info
    260 9.710563    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=5772 Ack=19404 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 260 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.708215000
    Time delta from previous packet: 0.000071000 seconds
    Time since reference or first frame: 9.710563000 seconds
    Frame Number: 260
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59e7 (23015)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x5cb6 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5772, Ack: 19404, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5772    (relative sequence number)
    Acknowledgement number: 19404    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x0f3b [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    261 9.710763    192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x316f

Frame 261 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.708415000
    Time delta from previous packet: 0.000271000 seconds
    Time since reference or first frame: 9.710763000 seconds
    Frame Number: 261
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
```

```
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
    Identification: 0x59e8 (23016)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c88 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5772, Ack: 19404, Len: 45
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5772    (relative sequence number)
    Next sequence number: 5817    (relative sequence number)
    Acknowledgement number: 19404    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x6a0e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
```

```
        Response in: 263
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 184
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x316f
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    262 9.714966    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=19404 Ack=5817 Win=64195 Len=0 TSV=1545526521
TSER=636883963

Frame 262 (66 bytes on wire, 66 bytes captured)
```

```
    Arrival Time: Dec 11, 2006 15:21:01.712618000
    Time delta from previous packet: 0.004203000 seconds
    Time since reference or first frame: 9.714966000 seconds
    Frame Number: 262
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d1b (40219)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1982 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19404, Ack: 5817, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19404    (relative sequence number)
    Acknowledgement number: 5817    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
```

```
    Window size: 64195
    Checksum: 0x144a [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    263 9.717027    192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 263 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.714679000
    Time delta from previous packet: 0.006264000 seconds
    Time since reference or first frame: 9.717027000 seconds
    Frame Number: 263
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d1c (40220)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x195a [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19404, Ack: 5817, Len: 39
    Source port: netbios-ssn (139)
```

```
    Destination port: 51751 (51751)
    Sequence number: 19404    (relative sequence number)
    Next sequence number: 19443    (relative sequence number)
    Acknowledgement number: 5817    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xa2eb [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 261
        Time from request: 0.006264000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
```

```
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 184
    Close Response (0x04)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    264 9.717116    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=5817 Ack=19443 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 264 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.714768000
    Time delta from previous packet: 0.000089000 seconds
    Time since reference or first frame: 9.717116000 seconds
    Frame Number: 264
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
```

```
    Total Length: 52
    Identification: 0x59e9 (23017)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cb4 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5817, Ack: 19443, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5817    (relative sequence number)
    Acknowledgement number: 19443    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x0ee7 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    265 9.717473    192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \Audio.mov

Frame 265 (176 bytes on wire, 176 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.715125000
    Time delta from previous packet: 0.000446000 seconds
    Time since reference or first frame: 9.717473000 seconds
    Frame Number: 265
    Packet Length: 176 bytes
    Capture Length: 176 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
```

```
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 162
    Identification: 0x59ea (23018)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c45 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5817, Ack: 19443, Len: 110
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5817    (relative sequence number)
    Next sequence number: 5927    (relative sequence number)
    Acknowledgement number: 19443    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x708c [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
```

```
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 106
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 267
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 185
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
        AndXCommand: No further commands (0xff)
        Reserved: 00
```

```
        AndXOffset: 0
        Reserved: 00
        File Name Len: 20
        Create Flags: 0x00000000
        Root FID: 0x00000000
        Access Mask: 0x00020007
        Allocation Size: 0
        File Attributes: 0x00000080
        Share Access: 0x00000007
        Disposition: Open (if file exists open it, else fail) (1)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 23
        File Name: \Audio.mov

No.     Time        Source                Destination           Protocol Info
    266 9.721838    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=19443 Ack=5927 Win=64130 Len=0 TSV=1545526521
TSER=636883963

Frame 266 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.719490000
    Time delta from previous packet: 0.004365000 seconds
    Time since reference or first frame: 9.721838000 seconds
    Frame Number: 266
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d1d (40221)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
```

```
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1980 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19443, Ack: 5927, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19443    (relative sequence number)
    Acknowledgement number: 5927    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64130
    Checksum: 0x13f6 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    267 9.723983    192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x3170

Frame 267 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.721635000
    Time delta from previous packet: 0.006510000 seconds
    Time since reference or first frame: 9.723983000 seconds
    Frame Number: 267
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9d1e (40222)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1914 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19443, Ack: 5927, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19443    (relative sequence number)
    Next sequence number: 19550    (relative sequence number)
    Acknowledgement number: 5927    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x8809 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 103
```

```
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 265
        Time from request: 0.006510000 seconds
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 185
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
        FID: 0x3170
```

```
        Create action: The file existed and was opened (1)
        Created: Dec 11, 2006 15:23:30.000000000
        Last Access: Dec 11, 2006 15:23:30.000000000
        Last Write: Dec 11, 2006 15:23:30.000000000
        Change: Dec 11, 2006 15:23:30.000000000
        File Attributes: 0x00000020
        Allocation Size: 0
        End Of File: 0
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    268 9.724058    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=5927 Ack=19550 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 268 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.721710000
    Time delta from previous packet: 0.000075000 seconds
    Time since reference or first frame: 9.724058000 seconds
    Frame Number: 268
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59eb (23019)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
```

```
    Header checksum: 0x5cb2 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5927, Ack: 19550, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5927    (relative sequence number)
    Acknowledgement number: 19550    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x0e0e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    269 9.724158    192.168.1.106         192.168.1.108         SMB      Locking
AndX Request, FID: 0x3170

Frame 269 (141 bytes on wire, 141 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.721810000
    Time delta from previous packet: 0.000175000 seconds
    Time since reference or first frame: 9.724158000 seconds
    Frame Number: 269
    Packet Length: 141 bytes
    Capture Length: 141 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
```

```
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 127
    Identification: 0x59ec (23020)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c66 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 5927, Ack: 19550, Len: 75
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 5927    (relative sequence number)
    Next sequence number: 6002    (relative sequence number)
    Acknowledgement number: 19550    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x407f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 71
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 271
```

```
        SMB Command: Locking AndX (0x24)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 186
    Locking AndX Request (0x24)
        Word Count (WCT): 8
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3170
        Lock Type: 0x10
        Oplock Level: Client is not holding oplock on this file (0)
        Timeout: Return immediately (0)
        Number of Unlocks: 0
        Number of Locks: 1
        Byte Count (BCC): 20
        Locks
```

```
No.     Time        Source                Destination           Protocol Info
    270 9.728547    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=19550 Ack=6002 Win=64165 Len=0 TSV=1545526521
TSER=636883963

Frame 270 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.726199000
    Time delta from previous packet: 0.004389000 seconds
    Time since reference or first frame: 9.728547000 seconds
    Frame Number: 270
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d1f (40223)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x197e [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19550, Ack: 6002, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19550    (relative sequence number)
    Acknowledgement number: 6002    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
```

```
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64165
    Checksum: 0x131d [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    271 9.743930    192.168.1.108         192.168.1.106         SMB      Locking
AndX Response

Frame 271 (109 bytes on wire, 109 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.741582000
    Time delta from previous packet: 0.019772000 seconds
    Time since reference or first frame: 9.743930000 seconds
    Frame Number: 271
    Packet Length: 109 bytes
    Capture Length: 109 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 95
    Identification: 0x9d20 (40224)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x1952 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19550, Ack: 6002, Len: 43
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19550    (relative sequence number)
    Next sequence number: 19593    (relative sequence number)
    Acknowledgement number: 6002    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x7c99 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 39
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 269
        Time from request: 0.019772000 seconds
        SMB Command: Locking AndX (0x24)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
```

```
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 186
    Locking AndX Response (0x24)
        Word Count (WCT): 2
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    272 9.744025    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=6002 Ack=19593 Win=65535 Len=0 TSV=636883963
TSER=1545526521

Frame 272 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.741677000
    Time delta from previous packet: 0.000095000 seconds
    Time since reference or first frame: 9.744025000 seconds
    Frame Number: 272
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
```

```
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x59ed (23021)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5cb0 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 6002, Ack: 19593, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 6002    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x0d98 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
```

```
    273 9.748729    192.168.1.106         192.168.1.108         SMB      Write
AndX Request, FID: 0x3170, 61440 bytes at offset 0

Frame 273 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746381000
    Time delta from previous packet: 0.004799000 seconds
    Time since reference or first frame: 9.748729000 seconds
    Frame Number: 273
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x59ee (23022)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5707 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 6002, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 6002    (relative sequence number)
    Next sequence number: 7450    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xe265 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    Last frame of this PDU: 316
    Time until the last segment of this PDU: 0.138760000 seconds
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 61504
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 318
        SMB Command: Write AndX (0x2f)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
```

```
           .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 187
    Write AndX Request (0x2f)
        Word Count (WCT): 14
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3170
        Offset: 0
        Reserved: 00000000
        Write Mode: 0x0000
        Remaining: 0
        Data Length High (multiply with 64K): 0
        Data Length Low: 61440
        Data Offset: 64
        High Offset: 0
        Byte Count (BCC): 61441
        Padding: EE
        File Data: Incomplete. Only 1380 of 61440 bytes

No.     Time        Source                Destination           Protocol Info
    274 9.748763    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=7450 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 274 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746415000
    Time delta from previous packet: 0.000034000 seconds
    Time since reference or first frame: 9.748763000 seconds
    Frame Number: 274
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
```

```
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x59ef (23023)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5706 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 7450, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 7450    (relative sequence number)
    Next sequence number: 8898    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xf198 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    275 9.748779    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=8898 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 275 (1514 bytes on wire, 1514 bytes captured)
```

```
    Arrival Time: Dec 11, 2006 15:21:01.746431000
    Time delta from previous packet: 0.000050000 seconds
    Time since reference or first frame: 9.748779000 seconds
    Frame Number: 275
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x59f0 (23024)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5705 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 8898, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 8898    (relative sequence number)
    Next sequence number: 10346    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
```

```
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xc008 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    276 9.748796    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=10346 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 276 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746448000
    Time delta from previous packet: 0.000067000 seconds
    Time since reference or first frame: 9.748796000 seconds
    Frame Number: 276
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x59f1 (23025)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5704 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
```

```
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 10346, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 10346    (relative sequence number)
    Next sequence number: 11794    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xc8b9 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    277 9.748811    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=11794 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 277 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746463000
    Time delta from previous packet: 0.000082000 seconds
    Time since reference or first frame: 9.748811000 seconds
    Frame Number: 277
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
```

```
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x59f2 (23026)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5703 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 11794, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 11794    (relative sequence number)
    Next sequence number: 13242    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xdbd6 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    278 9.748828    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=13242 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 278 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746480000
    Time delta from previous packet: 0.000099000 seconds
```

```
    Time since reference or first frame: 9.748828000 seconds
    Frame Number: 278
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x59f3 (23027)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5702 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 13242, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 13242    (relative sequence number)
    Next sequence number: 14690    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
```

```
    Checksum: 0x9c99 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    279 9.748847    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=14690 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 279 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746499000
    Time delta from previous packet: 0.000118000 seconds
    Time since reference or first frame: 9.748847000 seconds
    Frame Number: 279
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x59f4 (23028)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5701 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 14690, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
```

```
    Destination port: netbios-ssn (139)
    Sequence number: 14690    (relative sequence number)
    Next sequence number: 16138    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xfdae [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    280 9.748865    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=16138 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 280 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746517000
    Time delta from previous packet: 0.000136000 seconds
    Time since reference or first frame: 9.748865000 seconds
    Frame Number: 280
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
```

```
    Total Length: 1500
    Identification: 0x59f5 (23029)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5700 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 16138, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 16138    (relative sequence number)
    Next sequence number: 17586    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x2251 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    281 9.748881    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=17586 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 281 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746533000
    Time delta from previous packet: 0.000152000 seconds
    Time since reference or first frame: 9.748881000 seconds
    Frame Number: 281
    Packet Length: 1514 bytes
```

```
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x59f6 (23030)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56ff [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 17586, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 17586    (relative sequence number)
    Next sequence number: 19034    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xffef [correct]
    Options: (12 bytes)
        NOP
```

```
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    282 9.748897    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=19034 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 282 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746549000
    Time delta from previous packet: 0.000168000 seconds
    Time since reference or first frame: 9.748897000 seconds
    Frame Number: 282
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x59f7 (23031)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56fe [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 19034, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 19034    (relative sequence number)
    Next sequence number: 20482    (relative sequence number)
```

```
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1161 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    283 9.748913    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=20482 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 283 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746565000
    Time delta from previous packet: 0.000184000 seconds
    Time since reference or first frame: 9.748913000 seconds
    Frame Number: 283
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x59f8 (23032)
    Flags: 0x04 (Don't Fragment)
```

```
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56fd [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 20482, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 20482    (relative sequence number)
    Next sequence number: 21930    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x6374 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    284 9.748930    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=21930 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 284 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746582000
    Time delta from previous packet: 0.000201000 seconds
    Time since reference or first frame: 9.748930000 seconds
    Frame Number: 284
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
```

```
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x59f9 (23033)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56fc [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 21930, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 21930    (relative sequence number)
    Next sequence number: 23378    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x9950 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
```

```
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    285 9.748946    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=23378 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 285 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746598000
    Time delta from previous packet: 0.000217000 seconds
    Time since reference or first frame: 9.748946000 seconds
    Frame Number: 285
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x59fa (23034)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56fb [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 23378, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 23378    (relative sequence number)
    Next sequence number: 24826    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
```

```
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x2bb8 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    286 9.748962    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=24826 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 286 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746614000
    Time delta from previous packet: 0.000233000 seconds
    Time since reference or first frame: 9.748962000 seconds
    Frame Number: 286
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x59fb (23035)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
```

```
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56fa [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 24826, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 24826    (relative sequence number)
    Next sequence number: 26274    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xcdc9 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    287 9.748978    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=26274 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 287 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746630000
    Time delta from previous packet: 0.000249000 seconds
    Time since reference or first frame: 9.748978000 seconds
    Frame Number: 287
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
```

```
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x59fc (23036)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56f9 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 26274, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 26274    (relative sequence number)
    Next sequence number: 27722    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x97e9 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
```

```
    288 9.748995    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=27722 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 288 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746647000
    Time delta from previous packet: 0.000266000 seconds
    Time since reference or first frame: 9.748995000 seconds
    Frame Number: 288
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x59fd (23037)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56f8 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 27722, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 27722    (relative sequence number)
    Next sequence number: 29170    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
```

```
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x8029 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    289 9.749014    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=29170 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 289 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746666000
    Time delta from previous packet: 0.000285000 seconds
    Time since reference or first frame: 9.749014000 seconds
    Frame Number: 289
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x59fe (23038)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x56f7 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 29170, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 29170    (relative sequence number)
    Next sequence number: 30618    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x668f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    290 9.749091    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=30618 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 290 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746743000
    Time delta from previous packet: 0.000362000 seconds
    Time since reference or first frame: 9.749091000 seconds
    Frame Number: 290
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x59ff (23039)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56f6 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 30618, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 30618    (relative sequence number)
    Next sequence number: 32066    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xf0e4 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
```

```
    291 9.749112    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=32066 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 291 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746764000
    Time delta from previous packet: 0.000383000 seconds
    Time since reference or first frame: 9.749112000 seconds
    Frame Number: 291
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a00 (23040)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56f5 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 32066, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 32066    (relative sequence number)
    Next sequence number: 33514    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
```

```
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xd40c [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    292 9.749128    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=33514 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 292 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746780000
    Time delta from previous packet: 0.000399000 seconds
    Time since reference or first frame: 9.749128000 seconds
    Frame Number: 292
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a01 (23041)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x56f4 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 33514, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 33514    (relative sequence number)
    Next sequence number: 34962    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x6995 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    293 9.749145    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=34962 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 293 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746797000
    Time delta from previous packet: 0.000416000 seconds
    Time since reference or first frame: 9.749145000 seconds
    Frame Number: 293
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a02 (23042)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56f3 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 34962, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 34962    (relative sequence number)
    Next sequence number: 36410    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x3a54 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
```

```
    294 9.749161    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=36410 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 294 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746813000
    Time delta from previous packet: 0.000432000 seconds
    Time since reference or first frame: 9.749161000 seconds
    Frame Number: 294
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a03 (23043)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56f2 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 36410, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 36410    (relative sequence number)
    Next sequence number: 37858    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
```

```
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x837b [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    295 9.749178    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=37858 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 295 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746830000
    Time delta from previous packet: 0.000449000 seconds
    Time since reference or first frame: 9.749178000 seconds
    Frame Number: 295
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a04 (23044)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x56f1 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 37858, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 37858    (relative sequence number)
    Next sequence number: 39306    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xef29 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    296 9.749194    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=39306 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 296 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746846000
    Time delta from previous packet: 0.000465000 seconds
    Time since reference or first frame: 9.749194000 seconds
    Frame Number: 296
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a05 (23045)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56f0 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 39306, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 39306    (relative sequence number)
    Next sequence number: 40754    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x69bd [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
```

```
    297 9.749210    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=40754 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 297 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746862000
    Time delta from previous packet: 0.000481000 seconds
    Time since reference or first frame: 9.749210000 seconds
    Frame Number: 297
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a06 (23046)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56ef [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 40754, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 40754    (relative sequence number)
    Next sequence number: 42202    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
```

```
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x6846 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    298 9.749226    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=42202 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 298 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746878000
    Time delta from previous packet: 0.000497000 seconds
    Time since reference or first frame: 9.749226000 seconds
    Frame Number: 298
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a07 (23047)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x56ee [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 42202, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 42202    (relative sequence number)
    Next sequence number: 43650    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x27b6 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    299 9.749243    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=43650 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 299 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746895000
    Time delta from previous packet: 0.000514000 seconds
    Time since reference or first frame: 9.749243000 seconds
    Frame Number: 299
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a08 (23048)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56ed [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 43650, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 43650    (relative sequence number)
    Next sequence number: 45098    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xf8a1 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
```

```
    300 9.749259    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=45098 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 300 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746911000
    Time delta from previous packet: 0.000530000 seconds
    Time since reference or first frame: 9.749259000 seconds
    Frame Number: 300
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a09 (23049)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56ec [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 45098, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 45098    (relative sequence number)
    Next sequence number: 46546    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
```

```
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x4f15 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    301 9.749275    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=46546 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 301 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746927000
    Time delta from previous packet: 0.000546000 seconds
    Time since reference or first frame: 9.749275000 seconds
    Frame Number: 301
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a0a (23050)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x56eb [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 46546, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 46546    (relative sequence number)
    Next sequence number: 47994    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1bcf [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    302 9.749291    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=47994 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 302 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746943000
    Time delta from previous packet: 0.000562000 seconds
    Time since reference or first frame: 9.749291000 seconds
    Frame Number: 302
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a0b (23051)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56ea [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 47994, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 47994    (relative sequence number)
    Next sequence number: 49442    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xb44f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
```

```
    303 9.749310    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=49442 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 303 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746962000
    Time delta from previous packet: 0.000581000 seconds
    Time since reference or first frame: 9.749310000 seconds
    Frame Number: 303
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a0c (23052)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56e9 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 49442, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 49442    (relative sequence number)
    Next sequence number: 50890    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
```

```
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x09d6 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    304 9.749325    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=50890 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 304 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746977000
    Time delta from previous packet: 0.000596000 seconds
    Time since reference or first frame: 9.749325000 seconds
    Frame Number: 304
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a0d (23053)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x56e8 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 50890, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 50890    (relative sequence number)
    Next sequence number: 52338    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xa050 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    305 9.749342    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=52338 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 305 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.746994000
    Time delta from previous packet: 0.000613000 seconds
    Time since reference or first frame: 9.749342000 seconds
    Frame Number: 305
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a0e (23054)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56e7 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 52338, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 52338    (relative sequence number)
    Next sequence number: 53786    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xe541 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
```

```
    306 9.749358    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=53786 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 306 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.747010000
    Time delta from previous packet: 0.000629000 seconds
    Time since reference or first frame: 9.749358000 seconds
    Frame Number: 306
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a0f (23055)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56e6 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 53786, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 53786    (relative sequence number)
    Next sequence number: 55234    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
```

```
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x2428 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    307 9.749374    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=55234 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 307 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.747026000
    Time delta from previous packet: 0.000645000 seconds
    Time since reference or first frame: 9.749374000 seconds
    Frame Number: 307
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a10 (23056)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x56e5 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 55234, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 55234    (relative sequence number)
    Next sequence number: 56682    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x93d7 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    308 9.749391    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=56682 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 308 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.747043000
    Time delta from previous packet: 0.000662000 seconds
    Time since reference or first frame: 9.749391000 seconds
    Frame Number: 308
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a11 (23057)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56e4 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 56682, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 56682    (relative sequence number)
    Next sequence number: 58130    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xdd57 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
```

```
    309 9.749408    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=58130 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 309 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.747060000
    Time delta from previous packet: 0.000679000 seconds
    Time since reference or first frame: 9.749408000 seconds
    Frame Number: 309
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a12 (23058)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56e3 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 58130, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 58130    (relative sequence number)
    Next sequence number: 59578    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
```

```
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x367c [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    310 9.749424    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=59578 Ack=19593 Win=65535
Len=1448 TSV=636883963 TSER=1545526521

Frame 310 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.747076000
    Time delta from previous packet: 0.000695000 seconds
    Time since reference or first frame: 9.749424000 seconds
    Frame Number: 310
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a13 (23059)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x56e2 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 59578, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 59578    (relative sequence number)
    Next sequence number: 61026    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xd8a8 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883963, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    311 9.887315    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=19593 Ack=29170 Win=41076 Len=0 TSV=1545526521
TSER=636883963

Frame 311 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.884967000
    Time delta from previous packet: 0.138586000 seconds
    Time since reference or first frame: 9.887315000 seconds
    Frame Number: 311
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d21 (40225)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x197c [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19593, Ack: 29170, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19593    (relative sequence number)
    Acknowledgement number: 29170    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 41076
    Checksum: 0x12a3 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526521, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    312 9.887406    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=61026 Ack=19593 Win=65535
Len=1448 TSV=636883964 TSER=1545526521
```

```
Frame 312 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.885058000
    Time delta from previous packet: 0.138677000 seconds
    Time since reference or first frame: 9.887406000 seconds
    Frame Number: 312
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a14 (23060)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56e1 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 61026, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 61026    (relative sequence number)
    Next sequence number: 62474    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
```

```
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xdf2f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    313 9.887440    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=62474 Ack=19593 Win=65535
Len=1448 TSV=636883964 TSER=1545526521

Frame 313 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.885092000
    Time delta from previous packet: 0.138711000 seconds
    Time since reference or first frame: 9.887440000 seconds
    Frame Number: 313
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a15 (23061)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56e0 [correct]
    Source: 192.168.1.106 (192.168.1.106)
```

```
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 62474, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 62474    (relative sequence number)
    Next sequence number: 63922    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x7569 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    314 9.887457    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=63922 Ack=19593 Win=65535
Len=1448 TSV=636883964 TSER=1545526521

Frame 314 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.885109000
    Time delta from previous packet: 0.138728000 seconds
    Time since reference or first frame: 9.887457000 seconds
    Frame Number: 314
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
```

```
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a16 (23062)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56df [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 63922, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 63922    (relative sequence number)
    Next sequence number: 65370    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x9f26 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    315 9.887473    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [ACK] Seq=65370 Ack=19593 Win=65535
Len=1448 TSV=636883964 TSER=1545526521

Frame 315 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.885125000
```

```
    Time delta from previous packet: 0.138744000 seconds
    Time since reference or first frame: 9.887473000 seconds
    Frame Number: 315
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a17 (23063)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56de [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 65370, Ack: 19593, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 65370    (relative sequence number)
    Next sequence number: 66818    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
```

```
    Window size: 65535
    Checksum: 0x50a0 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    316 9.887489    192.168.1.106         192.168.1.108         TCP
[Continuation to #273] 51751 > netbios-ssn [PSH, ACK] Seq=66818 Ack=19593
Win=65535 Len=692 TSV=636883964 TSER=1545526521

Frame 316 (758 bytes on wire, 758 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.885141000
    Time delta from previous packet: 0.138760000 seconds
    Time since reference or first frame: 9.887489000 seconds
    Frame Number: 316
    Packet Length: 758 bytes
    Capture Length: 758 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 744
    Identification: 0x5a18 (23064)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x59d1 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 66818, Ack: 19593, Len: 692
```

```
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 66818    (relative sequence number)
    Next sequence number: 67510    (relative sequence number)
    Acknowledgement number: 19593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xbc7b [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526521
    This is a continuation to the PDU in frame: 273

No.     Time        Source                Destination           Protocol Info
    317 9.906354    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=19593 Ack=67510 Win=64240 Len=0 TSV=1545526522
TSER=636883963

Frame 317 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.904006000
    Time delta from previous packet: 0.157625000 seconds
    Time since reference or first frame: 9.906354000 seconds
    Frame Number: 317
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
```

```
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d22 (40226)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x197b [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19593, Ack: 67510, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19593    (relative sequence number)
    Acknowledgement number: 67510    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x2261 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883963
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    318 9.908600    192.168.1.108         192.168.1.106         SMB      Write
AndX Response, FID: 0x3170, 61440 bytes

Frame 318 (117 bytes on wire, 117 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.906252000
    Time delta from previous packet: 0.159871000 seconds
    Time since reference or first frame: 9.908600000 seconds
    Frame Number: 318
    Packet Length: 117 bytes
    Capture Length: 117 bytes
```

```
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 103
    Identification: 0x9d23 (40227)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1947 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19593, Ack: 67510, Len: 51
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19593    (relative sequence number)
    Next sequence number: 19644    (relative sequence number)
    Acknowledgement number: 67510    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x8c17 [correct]
    Options: (12 bytes)
        NOP
        NOP
```

```
        Time stamp: tsval 1545526522, tsecr 636883963
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 47
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 273
        Time from request: 0.159871000 seconds
        SMB Command: Write AndX (0x2f)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 187
    Write AndX Response (0x2f)
```

```
        Word Count (WCT): 6
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3170
        Count Low: 61440
        Remaining: 0
        Count High (multiply with 64K): 0
        Reserved: 0000
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    319 9.908655    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=67510 Ack=19644 Win=65535 Len=0 TSV=636883964
TSER=1545526522

Frame 319 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.906307000
    Time delta from previous packet: 0.000055000 seconds
    Time since reference or first frame: 9.908655000 seconds
    Frame Number: 319
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a19 (23065)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c84 [correct]
    Source: 192.168.1.106 (192.168.1.106)
```

```
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 67510, Ack: 19644, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 67510    (relative sequence number)
    Acknowledgement number: 19644    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1d1e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    320 9.908877    192.168.1.106         192.168.1.108         SMB      Write
AndX Request, FID: 0x3170, 4933 bytes at offset 61440

Frame 320 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.906529000
    Time delta from previous packet: 0.000277000 seconds
    Time since reference or first frame: 9.908877000 seconds
    Frame Number: 320
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
```

```
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a1a (23066)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56db [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 67510, Ack: 19644, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 67510    (relative sequence number)
    Next sequence number: 68958    (relative sequence number)
    Acknowledgement number: 19644    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xb43a [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    Last frame of this PDU: 323
    Time until the last segment of this PDU: 0.000026000 seconds
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 4997
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 325
```

```
        SMB Command: Write AndX (0x2f)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 188
    Write AndX Request (0x2f)
        Word Count (WCT): 14
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3170
        Offset: 61440
        Reserved: 00000000
        Write Mode: 0x0000
        Remaining: 0
        Data Length High (multiply with 64K): 0
        Data Length Low: 4933
        Data Offset: 64
```

```
        High Offset: 0
        Byte Count (BCC): 4934
        Padding: EE
        File Data: Incomplete. Only 1380 of 4933 bytes

No.     Time        Source                Destination           Protocol Info
    321 9.908888    192.168.1.106         192.168.1.108         TCP
[Continuation to #320] 51751 > netbios-ssn [ACK] Seq=68958 Ack=19644 Win=65535
Len=1448 TSV=636883964 TSER=1545526522

Frame 321 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.906540000
    Time delta from previous packet: 0.000011000 seconds
    Time since reference or first frame: 9.908888000 seconds
    Frame Number: 321
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a1b (23067)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56da [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 68958, Ack: 19644, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 68958    (relative sequence number)
```

```
    Next sequence number: 70406    (relative sequence number)
    Acknowledgement number: 19644    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xdb80 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    This is a continuation to the PDU in frame: 320

No.     Time        Source                Destination           Protocol Info
    322 9.908897    192.168.1.106         192.168.1.108         TCP
[Continuation to #320] 51751 > netbios-ssn [ACK] Seq=70406 Ack=19644 Win=65535
Len=1448 TSV=636883964 TSER=1545526522

Frame 322 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.906549000
    Time delta from previous packet: 0.000020000 seconds
    Time since reference or first frame: 9.908897000 seconds
    Frame Number: 322
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x5a1c (23068)
```

```
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x56d9 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 70406, Ack: 19644, Len: 1448
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 70406    (relative sequence number)
    Next sequence number: 71854    (relative sequence number)
    Acknowledgement number: 19644    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x18d6 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    This is a continuation to the PDU in frame: 320

No.     Time        Source                Destination           Protocol Info
    323 9.908903    192.168.1.106         192.168.1.108         TCP
[Continuation to #320] 51751 > netbios-ssn [PSH, ACK] Seq=71854 Ack=19644
Win=65535 Len=657 TSV=636883964 TSER=1545526522

Frame 323 (723 bytes on wire, 723 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.906555000
    Time delta from previous packet: 0.000026000 seconds
    Time since reference or first frame: 9.908903000 seconds
    Frame Number: 323
    Packet Length: 723 bytes
    Capture Length: 723 bytes
    Protocols in frame: eth:ip:tcp
```

```
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 709
    Identification: 0x5a1d (23069)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x59ef [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 71854, Ack: 19644, Len: 657
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 71854    (relative sequence number)
    Next sequence number: 72511    (relative sequence number)
    Acknowledgement number: 19644    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x521e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
```

```
    This is a continuation to the PDU in frame: 320

No.     Time        Source                Destination           Protocol Info
    324 9.924647    192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=19644 Ack=72511 Win=64240 Len=0 TSV=1545526522
TSER=636883964

Frame 324 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.922299000
    Time delta from previous packet: 0.015770000 seconds
    Time since reference or first frame: 9.924647000 seconds
    Frame Number: 324
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d24 (40228)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1979 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19644, Ack: 72511, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19644    (relative sequence number)
    Acknowledgement number: 72511    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
```

```
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x0ea4 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    325 9.926331    192.168.1.108         192.168.1.106         SMB      Write
AndX Response, FID: 0x3170, 4933 bytes

Frame 325 (117 bytes on wire, 117 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.923983000
    Time delta from previous packet: 0.017454000 seconds
    Time since reference or first frame: 9.926331000 seconds
    Frame Number: 325
    Packet Length: 117 bytes
    Capture Length: 117 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 103
    Identification: 0x9d25 (40229)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
```

```
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1945 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19644, Ack: 72511, Len: 51
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19644    (relative sequence number)
    Next sequence number: 19695    (relative sequence number)
    Acknowledgement number: 72511    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x5416 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 47
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 320
        Time from request: 0.017454000 seconds
        SMB Command: Write AndX (0x2f)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
```

```
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 188
    Write AndX Response (0x2f)
        Word Count (WCT): 6
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3170
        Count Low: 4933
        Remaining: 0
        Count High (multiply with 64K): 0
        Reserved: 0000
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    326 9.926382    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=72511 Ack=19695 Win=65535 Len=0 TSV=636883964
TSER=1545526522

Frame 326 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.924034000
    Time delta from previous packet: 0.000051000 seconds
    Time since reference or first frame: 9.926382000 seconds
```

```
    Frame Number: 326
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a1e (23070)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c7f [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 72511, Ack: 19695, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 72511    (relative sequence number)
    Acknowledgement number: 19695    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x0962 [correct]
    Options: (12 bytes)
```

```
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    327 9.926615    192.168.1.106         192.168.1.108         SMB      Locking
AndX Request, FID: 0x3170

Frame 327 (141 bytes on wire, 141 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.924267000
    Time delta from previous packet: 0.000284000 seconds
    Time since reference or first frame: 9.926615000 seconds
    Frame Number: 327
    Packet Length: 141 bytes
    Capture Length: 141 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 127
    Identification: 0x5a1f (23071)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c33 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 72511, Ack: 19695, Len: 75
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 72511    (relative sequence number)
    Next sequence number: 72586    (relative sequence number)
```

```
    Acknowledgement number: 19695    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x38d3 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 71
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 329
        SMB Command: Locking AndX (0x24)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
```

```
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 189
    Locking AndX Request (0x24)
        Word Count (WCT): 8
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3170
        Lock Type: 0x10
        Oplock Level: Client is not holding oplock on this file (0)
        Timeout: Return immediately (0)
        Number of Unlocks: 1
        Number of Locks: 0
        Byte Count (BCC): 20
        Unlocks

No.     Time        Source                Destination           Protocol Info
    328 9.926731    192.168.1.106         192.168.1.108         SMB      Trans2
Request, QUERY_FS_INFO, Info Allocation

Frame 328 (140 bytes on wire, 140 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.924383000
    Time delta from previous packet: 0.000116000 seconds
    Time since reference or first frame: 9.926731000 seconds
    Frame Number: 328
    Packet Length: 140 bytes
    Capture Length: 140 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
```

```
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 126
    Identification: 0x5a20 (23072)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c33 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 72586, Ack: 19695, Len: 74
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 72586    (relative sequence number)
    Next sequence number: 72660    (relative sequence number)
    Acknowledgement number: 19695    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x53b8 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 70
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 332
```

```
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 190
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 2
        Total Data Count: 0
        Max Parameter Count: 4
        Max Data Count: 18
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
```

```
        Parameter Count: 2
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: QUERY_FS_INFO (0x0003)
        Byte Count (BCC): 5
        Padding: 000000
        QUERY_FS_INFO Parameters
            Level of Interest: Info Allocation (0x0001)

No.     Time        Source                Destination           Protocol Info
    329 9.932367    192.168.1.108         192.168.1.106         SMB      Locking
AndX Response

Frame 329 (109 bytes on wire, 109 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.930019000
    Time delta from previous packet: 0.005636000 seconds
    Time since reference or first frame: 9.932367000 seconds
    Frame Number: 329
    Packet Length: 109 bytes
    Capture Length: 109 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 95
    Identification: 0x9d26 (40230)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x194c [correct]
    Source: 192.168.1.108 (192.168.1.108)
```

```
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19695, Ack: 72586, Len: 43
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19695    (relative sequence number)
    Next sequence number: 19738    (relative sequence number)
    Acknowledgement number: 72586    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x74ed [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 39
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 327
        Time from request: 0.005752000 seconds
        SMB Command: Locking AndX (0x24)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
```

```
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 189
    Locking AndX Response (0x24)
        Word Count (WCT): 2
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    330 9.932421    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=72660 Ack=19738 Win=65535 Len=0 TSV=636883964
TSER=1545526522

Frame 330 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.930073000
    Time delta from previous packet: 0.000054000 seconds
    Time since reference or first frame: 9.932421000 seconds
    Frame Number: 330
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a21 (23073)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c7c [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 72660, Ack: 19738, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 72660    (relative sequence number)
    Acknowledgement number: 19738    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x08a2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    331 9.932542    192.168.1.106         192.168.1.108         SMB      Flush
Request, FID: 0x3170
```

```
Frame 331 (107 bytes on wire, 107 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.930194000
    Time delta from previous packet: 0.000175000 seconds
    Time since reference or first frame: 9.932542000 seconds
    Frame Number: 331
    Packet Length: 107 bytes
    Capture Length: 107 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 93
    Identification: 0x5a22 (23074)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c52 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 72660, Ack: 19738, Len: 41
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 72660    (relative sequence number)
    Next sequence number: 72701    (relative sequence number)
    Acknowledgement number: 19738    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
```

```
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5d7c [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 37
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 334
        SMB Command: Flush (0x05)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
```

```
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 191
    Flush Request (0x05)
        Word Count (WCT): 1
        FID: 0x3170
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    332 9.937052    192.168.1.108         192.168.1.106         SMB      Trans2
Response, QUERY_FS_INFO

Frame 332 (144 bytes on wire, 144 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.934704000
    Time delta from previous packet: 0.004510000 seconds
    Time since reference or first frame: 9.937052000 seconds
    Frame Number: 332
    Packet Length: 144 bytes
    Capture Length: 144 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 130
    Identification: 0x9d27 (40231)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1928 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19738, Ack: 72660, Len: 78
```

```
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19738    (relative sequence number)
    Next sequence number: 19816    (relative sequence number)
    Acknowledgement number: 72660    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x2de2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 74
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 328
        Time from request: 0.010321000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
```

```
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 190
    Trans2 Response (0x32)
        Subcommand: QUERY_FS_INFO (0x0003)
        Word Count (WCT): 10
        Total Parameter Count: 0
        Total Data Count: 18
        Reserved: 0000
        Parameter Count: 0
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 18
        Data Offset: 56
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 19
        Padding: 00
        QUERY_FS_INFO Data

No.     Time        Source                Destination           Protocol Info
    333 9.937146    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=72701 Ack=19816 Win=65535 Len=0 TSV=636883964
TSER=1545526522

Frame 333 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.934798000
    Time delta from previous packet: 0.000094000 seconds
    Time since reference or first frame: 9.937146000 seconds
    Frame Number: 333
```

```
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a23 (23075)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c7a [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 72701, Ack: 19816, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 72701    (relative sequence number)
    Acknowledgement number: 19816    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x082b [correct]
    Options: (12 bytes)
        NOP
```

```
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    334 9.940322    192.168.1.108         192.168.1.106         SMB      Flush
Response

Frame 334 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.937974000
    Time delta from previous packet: 0.003270000 seconds
    Time since reference or first frame: 9.940322000 seconds
    Frame Number: 334
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d28 (40232)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x194e [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19816, Ack: 72701, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19816    (relative sequence number)
    Next sequence number: 19855    (relative sequence number)
    Acknowledgement number: 72701    (relative ack number)
```

```
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x9408 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 331
        Time from request: 0.007780000 seconds
        SMB Command: Flush (0x05)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
```

```
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 191
    Flush Response (0x05)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    335 9.940396    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=72701 Ack=19855 Win=65535 Len=0 TSV=636883964
TSER=1545526522

Frame 335 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.938048000
    Time delta from previous packet: 0.000074000 seconds
    Time since reference or first frame: 9.940396000 seconds
    Frame Number: 335
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a24 (23076)
    Flags: 0x04 (Don't Fragment)
```

```
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c79 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 72701, Ack: 19855, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 72701    (relative sequence number)
    Acknowledgement number: 19855    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x0804 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    336 9.940522    192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x3170

Frame 336 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.938174000
    Time delta from previous packet: 0.000200000 seconds
    Time since reference or first frame: 9.940522000 seconds
    Frame Number: 336
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
```

```
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
    Identification: 0x5a25 (23077)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c4b [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 72701, Ack: 19855, Len: 45
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 72701    (relative sequence number)
    Next sequence number: 72746    (relative sequence number)
    Acknowledgement number: 19855    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5ad6 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
```

```
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 337
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 192
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x3170
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
```

```
    337 9.946669    192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 337 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.944321000
    Time delta from previous packet: 0.006147000 seconds
    Time since reference or first frame: 9.946669000 seconds
    Frame Number: 337
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d29 (40233)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x194d [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19855, Ack: 72746, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19855    (relative sequence number)
    Next sequence number: 19894    (relative sequence number)
    Acknowledgement number: 72746    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x93b4 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 336
        Time from request: 0.006147000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
```

```
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 192
    Close Response (0x04)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    338 9.946758    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=72746 Ack=19894 Win=65535 Len=0 TSV=636883964
TSER=1545526522

Frame 338 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.944410000
    Time delta from previous packet: 0.000089000 seconds
    Time since reference or first frame: 9.946758000 seconds
    Frame Number: 338
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a26 (23078)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
```

```
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c77 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 72746, Ack: 19894, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 72746    (relative sequence number)
    Acknowledgement number: 19894    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x07b0 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    339 9.947215    192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \._Audio.mov

Frame 339 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.944867000
    Time delta from previous packet: 0.000546000 seconds
    Time since reference or first frame: 9.947215000 seconds
    Frame Number: 339
    Packet Length: 180 bytes
    Capture Length: 180 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
```

```
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x5a27 (23079)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c04 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 72746, Ack: 19894, Len: 114
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 72746    (relative sequence number)
    Next sequence number: 72860    (relative sequence number)
    Acknowledgement number: 19894    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xd048 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
```

```
        Server Component: SMB
        Response in: 340
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 193
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Reserved: 00
        File Name Len: 24
        Create Flags: 0x00000000
        Root FID: 0x00000000
        Access Mask: 0x00020007
        Allocation Size: 0
```

```
        File Attributes: 0x00000080
        Share Access: 0x00000007
        Disposition: Open (if file exists open it, else fail) (1)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 27
        File Name: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    340 9.953043    192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x3171

Frame 340 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.950695000
    Time delta from previous packet: 0.005828000 seconds
    Time since reference or first frame: 9.953043000 seconds
    Frame Number: 340
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9d2a (40234)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1908 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 19894, Ack: 72860, Len: 107
```

```
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 19894    (relative sequence number)
    Next sequence number: 20001    (relative sequence number)
    Acknowledgement number: 72860    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x13ce [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 103
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 339
        Time from request: 0.005828000 seconds
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
```

```
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 193
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
        FID: 0x3171
        Create action: The file existed and was opened (1)
        Created: Dec 11, 2006 15:23:30.000000000
        Last Access: Dec 11, 2006 15:23:30.000000000
        Last Write: Dec 11, 2006 15:23:30.000000000
        Change: Dec 11, 2006 15:23:30.000000000
        File Attributes: 0x00000022
        Allocation Size: 1048576
        End Of File: 82
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    341 9.953110    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=72860 Ack=20001 Win=65535 Len=0 TSV=636883964
TSER=1545526522

Frame 341 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.950762000
    Time delta from previous packet: 0.000067000 seconds
```

```
    Time since reference or first frame: 9.953110000 seconds
    Frame Number: 341
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a28 (23080)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c75 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 72860, Ack: 20001, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 72860    (relative sequence number)
    Acknowledgement number: 20001    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x06d3 [correct]
```

```
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    342 9.953255    192.168.1.106         192.168.1.108         SMB      Read
AndX Request, FID: 0x3171, 82 bytes at offset 0

Frame 342 (129 bytes on wire, 129 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.950907000
    Time delta from previous packet: 0.000212000 seconds
    Time since reference or first frame: 9.953255000 seconds
    Frame Number: 342
    Packet Length: 129 bytes
    Capture Length: 129 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 115
    Identification: 0x5a29 (23081)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c35 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 72860, Ack: 20001, Len: 63
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 72860    (relative sequence number)
```

```
    Next sequence number: 72923    (relative sequence number)
    Acknowledgement number: 20001    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x228b [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 59
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 343
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
```

```
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 194
    Read AndX Request (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3171
        Offset: 0
        Max Count Low: 82
        Min Count: 82
        Max Count High (multiply with 64K): 0
        Remaining: 82
        High Offset: 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    343 9.958901    192.168.1.108         192.168.1.106         SMB      Read
AndX Response, FID: 0x3171, 82 bytes

Frame 343 (211 bytes on wire, 211 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.956553000
    Time delta from previous packet: 0.005646000 seconds
    Time since reference or first frame: 9.958901000 seconds
    Frame Number: 343
    Packet Length: 211 bytes
    Capture Length: 211 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
```

```
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 197
    Identification: 0x9d2b (40235)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18e1 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 20001, Ack: 72923, Len: 145
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 20001    (relative sequence number)
    Next sequence number: 20146    (relative sequence number)
    Acknowledgement number: 72923    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x2646 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 141
SMB (Server Message Block Protocol)
```

```
    SMB Header
        Server Component: SMB
        Response to: 342
        Time from request: 0.005646000 seconds
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 194
    Read AndX Response (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3171
        Remaining: 65535
        Data Compaction Mode: 0
```

```
        Reserved: 0000
        Data Length Low: 82
        Data Offset: 59
        Data Length High (multiply with 64K): 0
        Reserved: 000000000000
        Byte Count (BCC): 82
        File Data: 000516070002000000000000000000000000000000000000...

No.     Time        Source                Destination           Protocol Info
    344 9.958993    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=72923 Ack=20146 Win=65535 Len=0 TSV=636883964
TSER=1545526522

Frame 344 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.956645000
    Time delta from previous packet: 0.000092000 seconds
    Time since reference or first frame: 9.958993000 seconds
    Frame Number: 344
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a2a (23082)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c73 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 72923, Ack: 20146, Len: 0
```

```
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 72923    (relative sequence number)
    Acknowledgement number: 20146    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x0603 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    345 9.959208    192.168.1.106         192.168.1.108         SMB      Write
AndX Request, FID: 0x3171, 32 bytes at offset 50

Frame 345 (166 bytes on wire, 166 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.956860000
    Time delta from previous packet: 0.000307000 seconds
    Time since reference or first frame: 9.959208000 seconds
    Frame Number: 345
    Packet Length: 166 bytes
    Capture Length: 166 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 152
```

```
    Identification: 0x5a2b (23083)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c0e [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 72923, Ack: 20146, Len: 100
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 72923    (relative sequence number)
    Next sequence number: 73023    (relative sequence number)
    Acknowledgement number: 20146    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xbc65 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 96
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 346
        SMB Command: Write AndX (0x2f)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
```

```
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 195
    Write AndX Request (0x2f)
        Word Count (WCT): 14
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3171
        Offset: 50
        Reserved: 00000000
        Write Mode: 0x0000
        Remaining: 0
        Data Length High (multiply with 64K): 0
        Data Length Low: 32
        Data Offset: 64
        High Offset: 0
        Byte Count (BCC): 33
        Padding: EE
        File Data: 4D6F6F5654564F44000000000000000000000000000000...
```

```
No.     Time        Source                Destination           Protocol Info
    346 9.964337    192.168.1.108         192.168.1.106         SMB      Write
AndX Response, FID: 0x3171, 32 bytes

Frame 346 (117 bytes on wire, 117 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.961989000
    Time delta from previous packet: 0.005129000 seconds
    Time since reference or first frame: 9.964337000 seconds
    Frame Number: 346
    Packet Length: 117 bytes
    Capture Length: 117 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 103
    Identification: 0x9d2c (40236)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x193e [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 20146, Ack: 73023, Len: 51
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 20146    (relative sequence number)
    Next sequence number: 20197    (relative sequence number)
    Acknowledgement number: 73023    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
```

```
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x5c45 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 47
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 345
        Time from request: 0.005129000 seconds
        SMB Command: Write AndX (0x2f)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
```

```
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 195
    Write AndX Response (0x2f)
        Word Count (WCT): 6
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3171
        Count Low: 32
        Remaining: 0
        Count High (multiply with 64K): 0
        Reserved: 0000
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    347 9.964436    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=73023 Ack=20197 Win=65535 Len=0 TSV=636883964
TSER=1545526522

Frame 347 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.962088000
    Time delta from previous packet: 0.000099000 seconds
    Time since reference or first frame: 9.964436000 seconds
    Frame Number: 347
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
```

```
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a2c (23084)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c71 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73023, Ack: 20197, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 73023    (relative sequence number)
    Acknowledgement number: 20197    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x056c [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    348 9.964643    192.168.1.106         192.168.1.108         SMB      Flush
Request, FID: 0x3171

Frame 348 (107 bytes on wire, 107 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.962295000
    Time delta from previous packet: 0.000306000 seconds
    Time since reference or first frame: 9.964643000 seconds
    Frame Number: 348
    Packet Length: 107 bytes
    Capture Length: 107 bytes
```

```
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 93
    Identification: 0x5a2d (23085)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c47 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73023, Ack: 20197, Len: 41
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 73023    (relative sequence number)
    Next sequence number: 73064    (relative sequence number)
    Acknowledgement number: 20197    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5545 [correct]
    Options: (12 bytes)
        NOP
        NOP
```

```
        Time stamp: tsval 636883964, tsecr 1545526522
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 37
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 350
        SMB Command: Flush (0x05)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 196
    Flush Request (0x05)
        Word Count (WCT): 1
        FID: 0x3171
```

```
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    349 9.964715    192.168.1.106         192.168.1.108         SMB      Trans2
Request, QUERY_FS_INFO, Info Allocation

Frame 349 (140 bytes on wire, 140 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.962367000
    Time delta from previous packet: 0.000072000 seconds
    Time since reference or first frame: 9.964715000 seconds
    Frame Number: 349
    Packet Length: 140 bytes
    Capture Length: 140 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 126
    Identification: 0x5a2e (23086)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c25 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73064, Ack: 20197, Len: 74
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 73064    (relative sequence number)
    Next sequence number: 73138    (relative sequence number)
    Acknowledgement number: 20197    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
```

```
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x48e4 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 70
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 353
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
```

```
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 197
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 2
        Total Data Count: 0
        Max Parameter Count: 4
        Max Data Count: 18
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 2
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: QUERY_FS_INFO (0x0003)
        Byte Count (BCC): 5
        Padding: 000000
        QUERY_FS_INFO Parameters
            Level of Interest: Info Allocation (0x0001)

No.     Time        Source                Destination           Protocol Info
    350 9.970299    192.168.1.108         192.168.1.106         SMB      Flush
Response

Frame 350 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.967951000
    Time delta from previous packet: 0.005584000 seconds
    Time since reference or first frame: 9.970299000 seconds
    Frame Number: 350
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
```

```
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d2d (40237)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1949 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 20197, Ack: 73064, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 20197    (relative sequence number)
    Next sequence number: 20236    (relative sequence number)
    Acknowledgement number: 73064    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x8c20 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
```

```
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 348
        Time from request: 0.005656000 seconds
        SMB Command: Flush (0x05)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 196
    Flush Response (0x05)
```

```
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    351 9.970373    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=73138 Ack=20236 Win=65535 Len=0 TSV=636883964
TSER=1545526522

Frame 351 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.968025000
    Time delta from previous packet: 0.000074000 seconds
    Time since reference or first frame: 9.970373000 seconds
    Frame Number: 351
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a2f (23087)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c6e [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73138, Ack: 20236, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 73138    (relative sequence number)
    Acknowledgement number: 20236    (relative ack number)
    Header length: 32 bytes
```

```
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x04d2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    352 9.970467    192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x3171

Frame 352 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.968119000
    Time delta from previous packet: 0.000168000 seconds
    Time since reference or first frame: 9.970467000 seconds
    Frame Number: 352
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
    Identification: 0x5a30 (23088)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
```

```
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c40 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73138, Ack: 20236, Len: 45
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 73138    (relative sequence number)
    Next sequence number: 73183    (relative sequence number)
    Acknowledgement number: 20236    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x51a3 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 355
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
```

```
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 198
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x3171
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    353 9.972212    192.168.1.108         192.168.1.106         SMB      Trans2
Response, QUERY_FS_INFO

Frame 353 (144 bytes on wire, 144 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.969864000
    Time delta from previous packet: 0.001745000 seconds
    Time since reference or first frame: 9.972212000 seconds
    Frame Number: 353
    Packet Length: 144 bytes
    Capture Length: 144 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 130
    Identification: 0x9d2e (40238)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1921 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 20236, Ack: 73138, Len: 78
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 20236    (relative sequence number)
    Next sequence number: 20314    (relative sequence number)
    Acknowledgement number: 73138    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x2312 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
```

```
    Length: 74
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 349
        Time from request: 0.007497000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 197
    Trans2 Response (0x32)
        Subcommand: QUERY_FS_INFO (0x0003)
        Word Count (WCT): 10
        Total Parameter Count: 0
        Total Data Count: 18
        Reserved: 0000
```

```
        Parameter Count: 0
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 18
        Data Offset: 56
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 19
        Padding: 00
        QUERY_FS_INFO Data

No.     Time        Source                Destination           Protocol Info
    354 9.972286    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=73183 Ack=20314 Win=65535 Len=0 TSV=636883964
TSER=1545526522

Frame 354 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.969938000
    Time delta from previous packet: 0.000074000 seconds
    Time since reference or first frame: 9.972286000 seconds
    Frame Number: 354
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a31 (23089)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c6c [correct]
```

```
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73183, Ack: 20314, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 73183    (relative sequence number)
    Acknowledgement number: 20314    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x0457 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    355 9.978481    192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 355 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.976133000
    Time delta from previous packet: 0.006269000 seconds
    Time since reference or first frame: 9.978481000 seconds
    Frame Number: 355
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
```

```
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d2f (40239)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1947 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 20314, Ack: 73183, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 20314    (relative sequence number)
    Next sequence number: 20353    (relative sequence number)
    Acknowledgement number: 73183    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x8a34 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 352
```

```
        Time from request: 0.008014000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 198
    Close Response (0x04)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    356 9.978564    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=73183 Ack=20353 Win=65535 Len=0 TSV=636883964
TSER=1545526522

Frame 356 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.976216000
```

```
    Time delta from previous packet: 0.000083000 seconds
    Time since reference or first frame: 9.978564000 seconds
    Frame Number: 356
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a32 (23090)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c6b [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73183, Ack: 20353, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 73183    (relative sequence number)
    Acknowledgement number: 20353    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
```

```
    Checksum: 0x0430 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    357 9.978741    192.168.1.106         192.168.1.108         SMB      Trans2
Request, SET_PATH_INFO, Path: \Audio.mov

Frame 357 (206 bytes on wire, 206 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.976393000
    Time delta from previous packet: 0.000260000 seconds
    Time since reference or first frame: 9.978741000 seconds
    Frame Number: 357
    Packet Length: 206 bytes
    Capture Length: 206 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 192
    Identification: 0x5a33 (23091)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bde [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73183, Ack: 20353, Len: 140
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
```

```
    Sequence number: 73183    (relative sequence number)
    Next sequence number: 73323    (relative sequence number)
    Acknowledgement number: 20353    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5a2a [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 136
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 358
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
```

```
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 199
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 28
        Total Data Count: 40
        Max Parameter Count: 24
        Max Data Count: 56
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 28
        Parameter Offset: 68
        Data Count: 40
        Data Offset: 96
        Setup Count: 1
        Reserved: 00
        Subcommand: SET_PATH_INFO (0x0006)
        Byte Count (BCC): 71
        Padding: 000000
        SET_PATH_INFO Parameters
            Level of Interest: Set File Basic Info (1004)
            Reserved: 00000000
            File Name: \Audio.mov
        SET_PATH_INFO Data

No.     Time        Source                Destination           Protocol Info
    358 9.986153    192.168.1.108         192.168.1.106         SMB      Trans2
Response, SET_PATH_INFO

Frame 358 (128 bytes on wire, 128 bytes captured)
```

```
    Arrival Time: Dec 11, 2006 15:21:01.983805000
    Time delta from previous packet: 0.007412000 seconds
    Time since reference or first frame: 9.986153000 seconds
    Frame Number: 358
    Packet Length: 128 bytes
    Capture Length: 128 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 114
    Identification: 0x9d30 (40240)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x192f [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 20353, Ack: 73323, Len: 62
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 20353    (relative sequence number)
    Next sequence number: 20415    (relative sequence number)
    Acknowledgement number: 73323    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
```

```
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x1014 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 58
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 357
        Time from request: 0.007412000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
```

```
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 199
    Trans2 Response (0x32)
        Subcommand: SET_PATH_INFO (0x0006)
        Word Count (WCT): 10
        Total Parameter Count: 2
        Total Data Count: 0
        Reserved: 0000
        Parameter Count: 2
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 0
        Data Offset: 0
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 3
        Padding: 00
        SET_PATH_INFO Parameters
            EA Error offset: 0

No.     Time        Source                Destination           Protocol Info
    359 9.986251    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=73323 Ack=20415 Win=65535 Len=0 TSV=636883964
TSER=1545526522

Frame 359 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.983903000
    Time delta from previous packet: 0.000098000 seconds
    Time since reference or first frame: 9.986251000 seconds
    Frame Number: 359
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
```

```
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a34 (23092)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c69 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73323, Ack: 20415, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 73323    (relative sequence number)
    Acknowledgement number: 20415    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x0366 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    360 9.986404    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Audio.mov

Frame 360 (172 bytes on wire, 172 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.984056000
    Time delta from previous packet: 0.000251000 seconds
    Time since reference or first frame: 9.986404000 seconds
    Frame Number: 360
```

```
    Packet Length: 172 bytes
    Capture Length: 172 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 158
    Identification: 0x5a35 (23093)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bfe [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73323, Ack: 20415, Len: 106
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 73323    (relative sequence number)
    Next sequence number: 73429    (relative sequence number)
    Acknowledgement number: 20415    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x106c [correct]
    Options: (12 bytes)
```

```
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 102
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 361
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 200
    Trans2 Request (0x32)
```

```
        Word Count (WCT): 15
        Total Parameter Count: 34
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 34
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 37
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Audio.mov

No.     Time        Source                Destination           Protocol Info
    361 9.993380    192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Audio.mov

Frame 361 (250 bytes on wire, 250 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.991032000
    Time delta from previous packet: 0.006976000 seconds
    Time since reference or first frame: 9.993380000 seconds
    Frame Number: 361
    Packet Length: 250 bytes
    Capture Length: 250 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
```

```
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 236
    Identification: 0x9d31 (40241)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18b4 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 20415, Ack: 73429, Len: 184
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 20415    (relative sequence number)
    Next sequence number: 20599    (relative sequence number)
    Acknowledgement number: 73429    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xaf96 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 180
SMB (Server Message Block Protocol)
```

```
    SMB Header
        Server Component: SMB
        Response to: 360
        Time from request: 0.006976000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 200
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 112
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
```

```
        Parameter Displacement: 0
        Data Count: 112
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 125
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    362 9.993472    192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=73429 Ack=20599 Win=65535 Len=0 TSV=636883964
TSER=1545526522

Frame 362 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.991124000
    Time delta from previous packet: 0.000092000 seconds
    Time since reference or first frame: 9.993472000 seconds
    Frame Number: 362
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a36 (23094)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
```

```
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c67 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73429, Ack: 20599, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 73429    (relative sequence number)
    Acknowledgement number: 20599    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x0244 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    363 9.993731    192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \._Audio.mov

Frame 363 (176 bytes on wire, 176 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.991383000
    Time delta from previous packet: 0.000351000 seconds
    Time since reference or first frame: 9.993731000 seconds
    Frame Number: 363
    Packet Length: 176 bytes
    Capture Length: 176 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
```

```
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 162
    Identification: 0x5a37 (23095)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bf8 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73429, Ack: 20599, Len: 110
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 73429    (relative sequence number)
    Next sequence number: 73539    (relative sequence number)
    Acknowledgement number: 20599    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x8135 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
```

```
    Length: 106
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 364
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 201
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 38
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
```

```
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 38
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 41
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    364 10.000201   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: ._Audio.mov

Frame 364 (254 bytes on wire, 254 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.997853000
    Time delta from previous packet: 0.006470000 seconds
    Time since reference or first frame: 10.000201000 seconds
    Frame Number: 364
    Packet Length: 254 bytes
    Capture Length: 254 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 240
```

```
    Identification: 0x9d32 (40242)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18af [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 20599, Ack: 73539, Len: 188
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 20599    (relative sequence number)
    Next sequence number: 20787    (relative sequence number)
    Acknowledgement number: 73539    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x412e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 184
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 363
        Time from request: 0.006470000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
```

```
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 201
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 116
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 116
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 129
```

```
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    365 10.000293   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=73539 Ack=20787 Win=65535 Len=0 TSV=636883964
TSER=1545526522

Frame 365 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.997945000
    Time delta from previous packet: 0.000092000 seconds
    Time since reference or first frame: 10.000293000 seconds
    Frame Number: 365
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a38 (23096)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c65 [correct]
    Source: 192.168.1.106 (192.168.1.106)
```

```
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73539, Ack: 20787, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 73539    (relative sequence number)
    Acknowledgement number: 20787    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x011a [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    366 10.000629   192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \._Audio.mov

Frame 366 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:01.998281000
    Time delta from previous packet: 0.000428000 seconds
    Time since reference or first frame: 10.000629000 seconds
    Frame Number: 366
    Packet Length: 180 bytes
    Capture Length: 180 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
```

```
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x5a39 (23097)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bf2 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73539, Ack: 20787, Len: 114
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 73539    (relative sequence number)
    Next sequence number: 73653    (relative sequence number)
    Acknowledgement number: 20787    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xc6b2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 367
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
```

```
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 202
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Reserved: 00
        File Name Len: 24
        Create Flags: 0x00000000
        Root FID: 0x00000000
        Access Mask: 0x00020001
        Allocation Size: 0
        File Attributes: 0x00000080
        Share Access: 0x00000007
        Disposition: Open (if file exists open it, else fail) (1)
        Create Options: 0x00000000
```

```
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 27
        File Name: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    367 10.006393   192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x3172

Frame 367 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.004045000
    Time delta from previous packet: 0.005764000 seconds
    Time since reference or first frame: 10.006393000 seconds
    Frame Number: 367
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9d33 (40243)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18ff [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 20787, Ack: 73653, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 20787    (relative sequence number)
    Next sequence number: 20894    (relative sequence number)
```

```
    Acknowledgement number: 73653    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xb972 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 103
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 366
        Time from request: 0.005764000 seconds
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
```

```
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 202
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
        FID: 0x3172
        Create action: The file existed and was opened (1)
        Created: Dec 11, 2006 15:23:30.000000000
        Last Access: Dec 11, 2006 15:23:31.000000000
        Last Write: Dec 11, 2006 15:23:31.000000000
        Change: Dec 11, 2006 15:23:31.000000000
        File Attributes: 0x00000022
        Allocation Size: 1048576
        End Of File: 82
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    368 10.006459   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=73653 Ack=20894 Win=65535 Len=0 TSV=636883964
TSER=1545526522

Frame 368 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.004111000
    Time delta from previous packet: 0.000066000 seconds
    Time since reference or first frame: 10.006459000 seconds
    Frame Number: 368
    Packet Length: 66 bytes
```

```
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a3a (23098)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c63 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73653, Ack: 20894, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 73653    (relative sequence number)
    Acknowledgement number: 20894    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x003d [correct]
    Options: (12 bytes)
        NOP
        NOP
```

```
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    369 10.006583   192.168.1.106         192.168.1.108         SMB      Read
AndX Request, FID: 0x3172, 82 bytes at offset 0

Frame 369 (129 bytes on wire, 129 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.004235000
    Time delta from previous packet: 0.000190000 seconds
    Time since reference or first frame: 10.006583000 seconds
    Frame Number: 369
    Packet Length: 129 bytes
    Capture Length: 129 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 115
    Identification: 0x5a3b (23099)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c23 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73653, Ack: 20894, Len: 63
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 73653    (relative sequence number)
    Next sequence number: 73716    (relative sequence number)
    Acknowledgement number: 20894    (relative ack number)
    Header length: 32 bytes
```

```
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x12f4 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 59
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 370
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
```

```
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 203
    Read AndX Request (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3172
        Offset: 0
        Max Count Low: 82
        Min Count: 82
        Max Count High (multiply with 64K): 0
        Remaining: 82
        High Offset: 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    370 10.011783   192.168.1.108         192.168.1.106         SMB      Read
AndX Response, FID: 0x3172, 82 bytes

Frame 370 (211 bytes on wire, 211 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.009435000
    Time delta from previous packet: 0.005200000 seconds
    Time since reference or first frame: 10.011783000 seconds
    Frame Number: 370
    Packet Length: 211 bytes
    Capture Length: 211 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
```

```
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 197
    Identification: 0x9d34 (40244)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18d8 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 20894, Ack: 73716, Len: 145
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 20894    (relative sequence number)
    Next sequence number: 21039    (relative sequence number)
    Acknowledgement number: 73716    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x28b2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 141
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 369
        Time from request: 0.005200000 seconds
```

```
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 203
    Read AndX Response (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3172
        Remaining: 65535
        Data Compaction Mode: 0
        Reserved: 0000
        Data Length Low: 82
        Data Offset: 59
        Data Length High (multiply with 64K): 0
```

```
        Reserved: 000000000000
        Byte Count (BCC): 82
        File Data: 000516070002000000000000000000000000000000000000...

No.     Time        Source                Destination           Protocol Info
    371 10.011974   192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x3172

Frame 371 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.009626000
    Time delta from previous packet: 0.000191000 seconds
    Time since reference or first frame: 10.011974000 seconds
    Frame Number: 371
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
    Identification: 0x5a3c (23100)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c34 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73716, Ack: 21039, Len: 45
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 73716    (relative sequence number)
    Next sequence number: 73761    (relative sequence number)
    Acknowledgement number: 21039    (relative ack number)
```

```
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x463d [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 372
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
```

```
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 204
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x3172
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    372 10.015456   192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 372 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.013108000
    Time delta from previous packet: 0.003482000 seconds
    Time since reference or first frame: 10.015456000 seconds
    Frame Number: 372
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d35 (40245)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
```

```
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1941 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 21039, Ack: 73761, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 21039    (relative sequence number)
    Next sequence number: 21078    (relative sequence number)
    Acknowledgement number: 73761    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x7f1d [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 371
        Time from request: 0.003482000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
```

```
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 204
    Close Response (0x04)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    373 10.015942   192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \._Audio.mov

Frame 373 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.013594000
    Time delta from previous packet: 0.000486000 seconds
    Time since reference or first frame: 10.015942000 seconds
    Frame Number: 373
    Packet Length: 180 bytes
    Capture Length: 180 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
```

```
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x5a3d (23101)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bee [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73761, Ack: 21078, Len: 114
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 73761    (relative sequence number)
    Next sequence number: 73875    (relative sequence number)
    Acknowledgement number: 21078    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xc1b1 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
```

```
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 374
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 205
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
```

```
        Reserved: 00
        File Name Len: 24
        Create Flags: 0x00000000
        Root FID: 0x00000000
        Access Mask: 0x00020001
        Allocation Size: 0
        File Attributes: 0x00000080
        Share Access: 0x00000007
        Disposition: Open (if file exists open it, else fail) (1)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 27
        File Name: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    374 10.019981   192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x3173

Frame 374 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.017633000
    Time delta from previous packet: 0.004039000 seconds
    Time since reference or first frame: 10.019981000 seconds
    Frame Number: 374
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9d36 (40246)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x18fc [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 21078, Ack: 73875, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 21078    (relative sequence number)
    Next sequence number: 21185    (relative sequence number)
    Acknowledgement number: 73875    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xb371 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 103
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 373
        Time from request: 0.004039000 seconds
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
```

```
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 205
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
        FID: 0x3173
        Create action: The file existed and was opened (1)
        Created: Dec 11, 2006 15:23:30.000000000
        Last Access: Dec 11, 2006 15:23:31.000000000
        Last Write: Dec 11, 2006 15:23:31.000000000
        Change: Dec 11, 2006 15:23:31.000000000
        File Attributes: 0x00000022
        Allocation Size: 1048576
        End Of File: 82
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
```

```
    375 10.020182   192.168.1.106         192.168.1.108         SMB      Read
AndX Request, FID: 0x3173, 82 bytes at offset 0

Frame 375 (129 bytes on wire, 129 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.017834000
    Time delta from previous packet: 0.000201000 seconds
    Time since reference or first frame: 10.020182000 seconds
    Frame Number: 375
    Packet Length: 129 bytes
    Capture Length: 129 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 115
    Identification: 0x5a3e (23102)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c20 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73875, Ack: 21185, Len: 63
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 73875    (relative sequence number)
    Next sequence number: 73938    (relative sequence number)
    Acknowledgement number: 21185    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x0df2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 59
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 376
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
```

```
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 206
    Read AndX Request (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3173
        Offset: 0
        Max Count Low: 82
        Min Count: 82
        Max Count High (multiply with 64K): 0
        Remaining: 82
        High Offset: 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    376 10.024045   192.168.1.108         192.168.1.106         SMB      Read
AndX Response, FID: 0x3173, 82 bytes

Frame 376 (211 bytes on wire, 211 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.021697000
    Time delta from previous packet: 0.003863000 seconds
    Time since reference or first frame: 10.024045000 seconds
    Frame Number: 376
    Packet Length: 211 bytes
    Capture Length: 211 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
```

```
    Total Length: 197
    Identification: 0x9d37 (40247)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18d5 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 21185, Ack: 73938, Len: 145
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 21185    (relative sequence number)
    Next sequence number: 21330    (relative sequence number)
    Acknowledgement number: 73938    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x23b1 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 141
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 375
        Time from request: 0.003863000 seconds
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
```

```
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 206
    Read AndX Response (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3173
        Remaining: 65535
        Data Compaction Mode: 0
        Reserved: 0000
        Data Length Low: 82
        Data Offset: 59
        Data Length High (multiply with 64K): 0
        Reserved: 000000000000
        Byte Count (BCC): 82
```

```
        File Data: 000516070002000000000000000000000000000000000000...

No.     Time        Source                Destination           Protocol Info
    377 10.024258   192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x3173

Frame 377 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.021910000
    Time delta from previous packet: 0.000213000 seconds
    Time since reference or first frame: 10.024258000 seconds
    Frame Number: 377
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
    Identification: 0x5a3f (23103)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c31 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73938, Ack: 21330, Len: 45
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 73938    (relative sequence number)
    Next sequence number: 73983    (relative sequence number)
    Acknowledgement number: 21330    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
```

```
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x413b [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 378
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
```

```
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 207
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x3173
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    378 10.027476   192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 378 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.025128000
    Time delta from previous packet: 0.003218000 seconds
    Time since reference or first frame: 10.027476000 seconds
    Frame Number: 378
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d38 (40248)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
```

```
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x193e [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 21330, Ack: 73983, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 21330    (relative sequence number)
    Next sequence number: 21369    (relative sequence number)
    Acknowledgement number: 73983    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x7a1c [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 377
        Time from request: 0.003218000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
```

```
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 207
    Close Response (0x04)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    379 10.028105   192.168.1.106         192.168.1.108         SMB      Trans2
Request, QUERY_FS_INFO, Info Allocation

Frame 379 (140 bytes on wire, 140 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.025757000
    Time delta from previous packet: 0.000629000 seconds
    Time since reference or first frame: 10.028105000 seconds
    Frame Number: 379
    Packet Length: 140 bytes
    Capture Length: 140 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
```

```
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 126
    Identification: 0x5a40 (23104)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c13 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 73983, Ack: 21369, Len: 74
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 73983    (relative sequence number)
    Next sequence number: 74057    (relative sequence number)
    Acknowledgement number: 21369    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x35b9 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
```

```
        .... ...0 = Add 0 to length
    Length: 70
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 380
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 208
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 2
        Total Data Count: 0
        Max Parameter Count: 4
        Max Data Count: 18
        Max Setup Count: 0
```

```
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 2
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: QUERY_FS_INFO (0x0003)
        Byte Count (BCC): 5
        Padding: 000000
        QUERY_FS_INFO Parameters
            Level of Interest: Info Allocation (0x0001)

No.     Time        Source                Destination           Protocol Info
    380 10.031825   192.168.1.108         192.168.1.106         SMB      Trans2
Response, QUERY_FS_INFO

Frame 380 (144 bytes on wire, 144 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.029477000
    Time delta from previous packet: 0.003720000 seconds
    Time since reference or first frame: 10.031825000 seconds
    Frame Number: 380
    Packet Length: 144 bytes
    Capture Length: 144 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 130
    Identification: 0x9d39 (40249)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
```

```
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1916 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 21369, Ack: 74057, Len: 78
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 21369    (relative sequence number)
    Next sequence number: 21447    (relative sequence number)
    Acknowledgement number: 74057    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x100e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 74
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 379
        Time from request: 0.003720000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
```

```
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 208
    Trans2 Response (0x32)
        Subcommand: QUERY_FS_INFO (0x0003)
        Word Count (WCT): 10
        Total Parameter Count: 0
        Total Data Count: 18
        Reserved: 0000
        Parameter Count: 0
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 18
        Data Offset: 56
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 19
        Padding: 00
        QUERY_FS_INFO Data

No.     Time        Source                Destination           Protocol Info
```

```
    381 10.032109   192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \._Audio.mov

Frame 381 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.029761000
    Time delta from previous packet: 0.000284000 seconds
    Time since reference or first frame: 10.032109000 seconds
    Frame Number: 381
    Packet Length: 180 bytes
    Capture Length: 180 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x5a41 (23105)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bea [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 74057, Ack: 21447, Len: 114
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 74057    (relative sequence number)
    Next sequence number: 74171    (relative sequence number)
    Acknowledgement number: 21447    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xbb18 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 382
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
```

```
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 209
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Reserved: 00
        File Name Len: 24
        Create Flags: 0x00000000
        Root FID: 0x00000000
        Access Mask: 0x00020001
        Allocation Size: 0
        File Attributes: 0x00000080
        Share Access: 0x00000007
        Disposition: Open (if file exists open it, else fail) (1)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 27
        File Name: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    382 10.036463   192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x3174

Frame 382 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.034115000
    Time delta from previous packet: 0.004354000 seconds
    Time since reference or first frame: 10.036463000 seconds
    Frame Number: 382
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
```

```
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9d3a (40250)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18f8 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 21447, Ack: 74171, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 21447    (relative sequence number)
    Next sequence number: 21554    (relative sequence number)
    Acknowledgement number: 74171    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xabd8 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 103
SMB (Server Message Block Protocol)
```

```
    SMB Header
        Server Component: SMB
        Response to: 381
        Time from request: 0.004354000 seconds
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 209
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
        FID: 0x3174
        Create action: The file existed and was opened (1)
```

```
        Created: Dec 11, 2006 15:23:30.000000000
        Last Access: Dec 11, 2006 15:23:31.000000000
        Last Write: Dec 11, 2006 15:23:31.000000000
        Change: Dec 11, 2006 15:23:31.000000000
        File Attributes: 0x00000022
        Allocation Size: 1048576
        End Of File: 82
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    383 10.036613   192.168.1.106         192.168.1.108         SMB      Read
AndX Request, FID: 0x3174, 82 bytes at offset 0

Frame 383 (129 bytes on wire, 129 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.034265000
    Time delta from previous packet: 0.000150000 seconds
    Time since reference or first frame: 10.036613000 seconds
    Frame Number: 383
    Packet Length: 129 bytes
    Capture Length: 129 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 115
    Identification: 0x5a42 (23106)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c1c [correct]
    Source: 192.168.1.106 (192.168.1.106)
```

```
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 74171, Ack: 21554, Len: 63
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 74171    (relative sequence number)
    Next sequence number: 74234    (relative sequence number)
    Acknowledgement number: 21554    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x0758 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 59
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 384
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
```

```
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 210
    Read AndX Request (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3174
        Offset: 0
        Max Count Low: 82
        Min Count: 82
        Max Count High (multiply with 64K): 0
        Remaining: 82
        High Offset: 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    384 10.040380   192.168.1.108         192.168.1.106         SMB      Read
AndX Response, FID: 0x3174, 82 bytes

Frame 384 (211 bytes on wire, 211 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.038032000
    Time delta from previous packet: 0.003767000 seconds
    Time since reference or first frame: 10.040380000 seconds
    Frame Number: 384
    Packet Length: 211 bytes
    Capture Length: 211 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
```

```
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 197
    Identification: 0x9d3b (40251)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18d1 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 21554, Ack: 74234, Len: 145
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 21554    (relative sequence number)
    Next sequence number: 21699    (relative sequence number)
    Acknowledgement number: 74234    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x1d18 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
```

```
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 141
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 383
        Time from request: 0.003767000 seconds
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 210
    Read AndX Response (0x2e)
```

```
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3174
        Remaining: 65535
        Data Compaction Mode: 0
        Reserved: 0000
        Data Length Low: 82
        Data Offset: 59
        Data Length High (multiply with 64K): 0
        Reserved: 000000000000
        Byte Count (BCC): 82
        File Data: 000516070002000000000000000000000000000000000000...

No.     Time        Source                Destination           Protocol Info
    385 10.040602   192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x3174

Frame 385 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.038254000
    Time delta from previous packet: 0.000222000 seconds
    Time since reference or first frame: 10.040602000 seconds
    Frame Number: 385
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
    Identification: 0x5a43 (23107)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x5c2d [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 74234, Ack: 21699, Len: 45
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 74234    (relative sequence number)
    Next sequence number: 74279    (relative sequence number)
    Acknowledgement number: 21699    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x3aa1 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 386
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
```

```
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 211
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x3174
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    386 10.045163   192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 386 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.042815000
    Time delta from previous packet: 0.004561000 seconds
    Time since reference or first frame: 10.045163000 seconds
    Frame Number: 386
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d3c (40252)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x193a [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 21699, Ack: 74279, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 21699    (relative sequence number)
    Next sequence number: 21738    (relative sequence number)
    Acknowledgement number: 74279    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x7383 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
```

```
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 385
        Time from request: 0.004561000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 211
    Close Response (0x04)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
```

```
    387 10.045520   192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \._Audio.mov

Frame 387 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.043172000
    Time delta from previous packet: 0.000357000 seconds
    Time since reference or first frame: 10.045520000 seconds
    Frame Number: 387
    Packet Length: 180 bytes
    Capture Length: 180 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x5a44 (23108)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5be7 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 74279, Ack: 21738, Len: 114
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 74279    (relative sequence number)
    Next sequence number: 74393    (relative sequence number)
    Acknowledgement number: 21738    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xb617 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 388
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
```

```
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 212
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Reserved: 00
        File Name Len: 24
        Create Flags: 0x00000000
        Root FID: 0x00000000
        Access Mask: 0x00020001
        Allocation Size: 0
        File Attributes: 0x00000080
        Share Access: 0x00000007
        Disposition: Open (if file exists open it, else fail) (1)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 27
        File Name: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    388 10.049895   192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x3175

Frame 388 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.047547000
    Time delta from previous packet: 0.004375000 seconds
    Time since reference or first frame: 10.049895000 seconds
    Frame Number: 388
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
```

```
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9d3d (40253)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18f5 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 21738, Ack: 74393, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 21738    (relative sequence number)
    Next sequence number: 21845    (relative sequence number)
    Acknowledgement number: 74393    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xa5d7 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 103
SMB (Server Message Block Protocol)
```

```
    SMB Header
        Server Component: SMB
        Response to: 387
        Time from request: 0.004375000 seconds
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 212
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
        FID: 0x3175
        Create action: The file existed and was opened (1)
```

```
        Created: Dec 11, 2006 15:23:30.000000000
        Last Access: Dec 11, 2006 15:23:31.000000000
        Last Write: Dec 11, 2006 15:23:31.000000000
        Change: Dec 11, 2006 15:23:31.000000000
        File Attributes: 0x00000022
        Allocation Size: 1048576
        End Of File: 82
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    389 10.050103   192.168.1.106         192.168.1.108         SMB      Read
AndX Request, FID: 0x3175, 82 bytes at offset 0

Frame 389 (129 bytes on wire, 129 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.047755000
    Time delta from previous packet: 0.000208000 seconds
    Time since reference or first frame: 10.050103000 seconds
    Frame Number: 389
    Packet Length: 129 bytes
    Capture Length: 129 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 115
    Identification: 0x5a45 (23109)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c19 [correct]
    Source: 192.168.1.106 (192.168.1.106)
```

```
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 74393, Ack: 21845, Len: 63
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 74393    (relative sequence number)
    Next sequence number: 74456    (relative sequence number)
    Acknowledgement number: 21845    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x0256 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 59
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 390
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
```

```
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 213
    Read AndX Request (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3175
        Offset: 0
        Max Count Low: 82
        Min Count: 82
        Max Count High (multiply with 64K): 0
        Remaining: 82
        High Offset: 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    390 10.054368   192.168.1.108         192.168.1.106         SMB      Read
AndX Response, FID: 0x3175, 82 bytes

Frame 390 (211 bytes on wire, 211 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.052020000
    Time delta from previous packet: 0.004265000 seconds
    Time since reference or first frame: 10.054368000 seconds
    Frame Number: 390
    Packet Length: 211 bytes
    Capture Length: 211 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
```

```
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 197
    Identification: 0x9d3e (40254)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18ce [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 21845, Ack: 74456, Len: 145
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 21845    (relative sequence number)
    Next sequence number: 21990    (relative sequence number)
    Acknowledgement number: 74456    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x1817 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
```

```
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 141
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 389
        Time from request: 0.004265000 seconds
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 213
    Read AndX Response (0x2e)
```

```
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3175
        Remaining: 65535
        Data Compaction Mode: 0
        Reserved: 0000
        Data Length Low: 82
        Data Offset: 59
        Data Length High (multiply with 64K): 0
        Reserved: 000000000000
        Byte Count (BCC): 82
        File Data: 000516070002000000000000000000000000000000000000...

No.     Time        Source                Destination           Protocol Info
    391 10.054640   192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x3175

Frame 391 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.052292000
    Time delta from previous packet: 0.000272000 seconds
    Time since reference or first frame: 10.054640000 seconds
    Frame Number: 391
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
    Identification: 0x5a46 (23110)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x5c2a [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 74456, Ack: 21990, Len: 45
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 74456    (relative sequence number)
    Next sequence number: 74501    (relative sequence number)
    Acknowledgement number: 21990    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x359f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 392
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
```

```
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 214
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x3175
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    392 10.058289   192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 392 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.055941000
    Time delta from previous packet: 0.003649000 seconds
    Time since reference or first frame: 10.058289000 seconds
    Frame Number: 392
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d3f (40255)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1937 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 21990, Ack: 74501, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 21990    (relative sequence number)
    Next sequence number: 22029    (relative sequence number)
    Acknowledgement number: 74501    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x6e82 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
```

```
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 391
        Time from request: 0.003649000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 214
    Close Response (0x04)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
```

```
    393 10.059096   192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \._Audio.mov

Frame 393 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.056748000
    Time delta from previous packet: 0.000807000 seconds
    Time since reference or first frame: 10.059096000 seconds
    Frame Number: 393
    Packet Length: 180 bytes
    Capture Length: 180 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x5a47 (23111)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5be4 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 74501, Ack: 22029, Len: 114
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 74501    (relative sequence number)
    Next sequence number: 74615    (relative sequence number)
    Acknowledgement number: 22029    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xb116 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 394
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
```

```
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 215
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Reserved: 00
        File Name Len: 24
        Create Flags: 0x00000000
        Root FID: 0x00000000
        Access Mask: 0x00020001
        Allocation Size: 0
        File Attributes: 0x00000080
        Share Access: 0x00000007
        Disposition: Open (if file exists open it, else fail) (1)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 27
        File Name: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    394 10.063530   192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x3176

Frame 394 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.061182000
    Time delta from previous packet: 0.004434000 seconds
    Time since reference or first frame: 10.063530000 seconds
    Frame Number: 394
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
```

```
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9d40 (40256)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18f2 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 22029, Ack: 74615, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 22029    (relative sequence number)
    Next sequence number: 22136    (relative sequence number)
    Acknowledgement number: 74615    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x9fd6 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 103
SMB (Server Message Block Protocol)
```

```
    SMB Header
        Server Component: SMB
        Response to: 393
        Time from request: 0.004434000 seconds
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 215
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
        FID: 0x3176
        Create action: The file existed and was opened (1)
```

```
        Created: Dec 11, 2006 15:23:30.000000000
        Last Access: Dec 11, 2006 15:23:31.000000000
        Last Write: Dec 11, 2006 15:23:31.000000000
        Change: Dec 11, 2006 15:23:31.000000000
        File Attributes: 0x00000022
        Allocation Size: 1048576
        End Of File: 82
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    395 10.063795   192.168.1.106         192.168.1.108         SMB      Read
AndX Request, FID: 0x3176, 82 bytes at offset 0

Frame 395 (129 bytes on wire, 129 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.061447000
    Time delta from previous packet: 0.000265000 seconds
    Time since reference or first frame: 10.063795000 seconds
    Frame Number: 395
    Packet Length: 129 bytes
    Capture Length: 129 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 115
    Identification: 0x5a48 (23112)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c16 [correct]
    Source: 192.168.1.106 (192.168.1.106)
```

```
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 74615, Ack: 22136, Len: 63
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 74615    (relative sequence number)
    Next sequence number: 74678    (relative sequence number)
    Acknowledgement number: 22136    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xfd53 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 59
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 396
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
```

```
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 216
    Read AndX Request (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3176
        Offset: 0
        Max Count Low: 82
        Min Count: 82
        Max Count High (multiply with 64K): 0
        Remaining: 82
        High Offset: 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    396 10.068391   192.168.1.108         192.168.1.106         SMB      Read
AndX Response, FID: 0x3176, 82 bytes

Frame 396 (211 bytes on wire, 211 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.066043000
    Time delta from previous packet: 0.004596000 seconds
    Time since reference or first frame: 10.068391000 seconds
    Frame Number: 396
    Packet Length: 211 bytes
    Capture Length: 211 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
```

```
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 197
    Identification: 0x9d41 (40257)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18cb [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 22136, Ack: 74678, Len: 145
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 22136    (relative sequence number)
    Next sequence number: 22281    (relative sequence number)
    Acknowledgement number: 74678    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x1316 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
```

```
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 141
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 395
        Time from request: 0.004596000 seconds
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 216
    Read AndX Response (0x2e)
```

```
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3176
        Remaining: 65535
        Data Compaction Mode: 0
        Reserved: 0000
        Data Length Low: 82
        Data Offset: 59
        Data Length High (multiply with 64K): 0
        Reserved: 000000000000
        Byte Count (BCC): 82
        File Data: 000516070002000000000000000000000000000000000000...

No.     Time        Source                Destination           Protocol Info
    397 10.068659   192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x3176

Frame 397 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.066311000
    Time delta from previous packet: 0.000268000 seconds
    Time since reference or first frame: 10.068659000 seconds
    Frame Number: 397
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
    Identification: 0x5a49 (23113)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x5c27 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 74678, Ack: 22281, Len: 45
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 74678    (relative sequence number)
    Next sequence number: 74723    (relative sequence number)
    Acknowledgement number: 22281    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x309d [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 398
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
```

```
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 217
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x3176
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    398 10.072521   192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 398 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.070173000
    Time delta from previous packet: 0.003862000 seconds
    Time since reference or first frame: 10.072521000 seconds
    Frame Number: 398
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d42 (40258)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1934 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 22281, Ack: 74723, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 22281    (relative sequence number)
    Next sequence number: 22320    (relative sequence number)
    Acknowledgement number: 74723    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x6981 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
```

```
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 397
        Time from request: 0.003862000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 217
    Close Response (0x04)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
```

```
    399 10.110704   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=74723 Ack=22320 Win=65535 Len=0 TSV=636883964
TSER=1545526522

Frame 399 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.108356000
    Time delta from previous packet: 0.038183000 seconds
    Time since reference or first frame: 10.110704000 seconds
    Frame Number: 399
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a4a (23114)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c53 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 74723, Ack: 22320, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 74723    (relative sequence number)
    Acknowledgement number: 22320    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xf67c [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    400 10.154263   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \*

Frame 400 (156 bytes on wire, 156 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.151915000
    Time delta from previous packet: 0.081742000 seconds
    Time since reference or first frame: 10.154263000 seconds
    Frame Number: 400
    Packet Length: 156 bytes
    Capture Length: 156 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 142
    Identification: 0x5a4b (23115)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bf8 [correct]
```

```
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 74723, Ack: 22320, Len: 90
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 74723    (relative sequence number)
    Next sequence number: 74813    (relative sequence number)
    Acknowledgement number: 22320    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1ed6 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 86
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 401
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
```

```
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 218
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 18
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 18
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 21
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 32
            Flags: 0x0006
```

```
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \*

No.     Time        Source                Destination           Protocol Info
    401 10.168679   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: . .. ._Audio.mov .bash_history .CFUserTextEncoding
.DS_Store .emacs.d .lpoptions .mysql_history .ssh .TemporaryItems .Trash

Frame 401 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.166331000
    Time delta from previous packet: 0.014416000 seconds
    Time since reference or first frame: 10.168679000 seconds
    Frame Number: 401
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x9d43 (40259)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x13b2 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 22320, Ack: 74813, Len: 1448
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 22320    (relative sequence number)
    Next sequence number: 23768    (relative sequence number)
```

```
    Acknowledgement number: 74813    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xb01e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    Last frame of this PDU: 402
    Time until the last segment of this PDU: 0.008591000 seconds
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 2852
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 400
        Time from request: 0.014416000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
```

```
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 218
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 2784
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 2784
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 2797
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 25
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 2680
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    402 10.177270   192.168.1.108         192.168.1.106         TCP
[Continuation to #401] netbios-ssn > 51751 [PSH, ACK] Seq=23768 Ack=74813
Win=64240 Len=1408 TSV=1545526522 TSER=636883964
```

```
Frame 402 (1474 bytes on wire, 1474 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.174922000
    Time delta from previous packet: 0.008591000 seconds
    Time since reference or first frame: 10.177270000 seconds
    Frame Number: 402
    Packet Length: 1474 bytes
    Capture Length: 1474 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1460
    Identification: 0x9d44 (40260)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x13d9 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 23768, Ack: 74813, Len: 1408
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 23768    (relative sequence number)
    Next sequence number: 25176    (relative sequence number)
    Acknowledgement number: 74813    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
```

```
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x3b8f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    This is a continuation to the PDU in frame: 401

No.     Time        Source                Destination           Protocol Info
    403 10.178253   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.bash_history

Frame 403 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.175905000
    Time delta from previous packet: 0.009574000 seconds
    Time since reference or first frame: 10.178253000 seconds
    Frame Number: 403
    Packet Length: 180 bytes
    Capture Length: 180 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x5a4c (23116)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bdf [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
```

```
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 74813, Ack: 25176, Len: 114
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 74813    (relative sequence number)
    Next sequence number: 74927    (relative sequence number)
    Acknowledgement number: 25176    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x19d7 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 404
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
```

```
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 219
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 42
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 42
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 45
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
```

```
            Search Pattern: \.bash_history

No.     Time        Source                Destination           Protocol Info
    404 10.184278   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: .bash_history

Frame 404 (258 bytes on wire, 258 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.181930000
    Time delta from previous packet: 0.006025000 seconds
    Time since reference or first frame: 10.184278000 seconds
    Frame Number: 404
    Packet Length: 258 bytes
    Capture Length: 258 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 244
    Identification: 0x9d45 (40261)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1898 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 25176, Ack: 74927, Len: 192
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 25176    (relative sequence number)
    Next sequence number: 25368    (relative sequence number)
    Acknowledgement number: 74927    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
```

```
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x0ac0 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 188
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 403
        Time from request: 0.006025000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
```

```
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 219
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 120
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 120
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 133
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    405 10.184600   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.CFUserTextEncoding

Frame 405 (192 bytes on wire, 192 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.182252000
    Time delta from previous packet: 0.000322000 seconds
    Time since reference or first frame: 10.184600000 seconds
    Frame Number: 405
```

```
    Packet Length: 192 bytes
    Capture Length: 192 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 178
    Identification: 0x5a4d (23117)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bd2 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 74927, Ack: 25368, Len: 126
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 74927    (relative sequence number)
    Next sequence number: 75053    (relative sequence number)
    Acknowledgement number: 25368    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x3267 [correct]
    Options: (12 bytes)
```

```
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 122
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 406
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 220
```

```
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 54
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 54
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 57
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.CFUserTextEncoding

No.     Time        Source                Destination           Protocol Info
    406 10.190192   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: .CFUserTextEncoding

Frame 406 (270 bytes on wire, 270 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.187844000
    Time delta from previous packet: 0.005592000 seconds
    Time since reference or first frame: 10.190192000 seconds
    Frame Number: 406
    Packet Length: 270 bytes
    Capture Length: 270 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 256
    Identification: 0x9d46 (40262)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x188b [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 25368, Ack: 75053, Len: 204
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 25368    (relative sequence number)
    Next sequence number: 25572    (relative sequence number)
    Acknowledgement number: 75053    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xb8f4 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
```

```
    Length: 200
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 405
        Time from request: 0.005592000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 220
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 132
        Reserved: 0000
```

```
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 132
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 145
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    407 10.190458   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.DS_Store

Frame 407 (172 bytes on wire, 172 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.188110000
    Time delta from previous packet: 0.000266000 seconds
    Time since reference or first frame: 10.190458000 seconds
    Frame Number: 407
    Packet Length: 172 bytes
    Capture Length: 172 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 158
    Identification: 0x5a4e (23118)
    Flags: 0x04 (Don't Fragment)
```

```
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5be5 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 75053, Ack: 25572, Len: 106
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 75053    (relative sequence number)
    Next sequence number: 75159    (relative sequence number)
    Acknowledgement number: 25572    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x2185 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 102
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 408
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
```

```
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 221
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 34
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 34
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
```

```
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 37
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.DS_Store

No.     Time        Source                Destination           Protocol Info
    408 10.197728   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: .DS_Store

Frame 408 (250 bytes on wire, 250 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.195380000
    Time delta from previous packet: 0.007270000 seconds
    Time since reference or first frame: 10.197728000 seconds
    Frame Number: 408
    Packet Length: 250 bytes
    Capture Length: 250 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 236
    Identification: 0x9d47 (40263)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x189e [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
```

```
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 25572, Ack: 75159, Len: 184
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 25572    (relative sequence number)
    Next sequence number: 25756    (relative sequence number)
    Acknowledgement number: 75159    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xf827 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 180
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 407
        Time from request: 0.007270000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
```

```
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 221
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 112
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 112
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 125
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data
```

```
No.     Time        Source                Destination           Protocol Info
    409 10.198095   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.emacs.d

Frame 409 (170 bytes on wire, 170 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.195747000
    Time delta from previous packet: 0.000367000 seconds
    Time since reference or first frame: 10.198095000 seconds
    Frame Number: 409
    Packet Length: 170 bytes
    Capture Length: 170 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 156
    Identification: 0x5a4f (23119)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5be6 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 75159, Ack: 25756, Len: 104
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 75159    (relative sequence number)
    Next sequence number: 75263    (relative sequence number)
    Acknowledgement number: 25756    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
```

```
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x876d [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 100
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 410
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
```

```
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 222
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 32
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 32
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 35
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.emacs.d

No.     Time        Source                Destination           Protocol Info
    410 10.203652   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: .emacs.d

Frame 410 (250 bytes on wire, 250 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.201304000
    Time delta from previous packet: 0.005557000 seconds
    Time since reference or first frame: 10.203652000 seconds
    Frame Number: 410
```

```
    Packet Length: 250 bytes
    Capture Length: 250 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 236
    Identification: 0x9d48 (40264)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x189d [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 25756, Ack: 75263, Len: 184
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 25756    (relative sequence number)
    Next sequence number: 25940    (relative sequence number)
    Acknowledgement number: 75263    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xba1d [correct]
    Options: (12 bytes)
```

```
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 180
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 409
        Time from request: 0.005557000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
```

```
        User ID: 100
        Multiplex ID: 222
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 112
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 112
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 125
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    411 10.204127   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.lpoptions

Frame 411 (174 bytes on wire, 174 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.201779000
    Time delta from previous packet: 0.000475000 seconds
    Time since reference or first frame: 10.204127000 seconds
    Frame Number: 411
    Packet Length: 174 bytes
    Capture Length: 174 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
```

```
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 160
    Identification: 0x5a50 (23120)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5be1 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 75263, Ack: 25940, Len: 108
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 75263    (relative sequence number)
    Next sequence number: 75371    (relative sequence number)
    Acknowledgement number: 25940    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x3838 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 104
SMB (Server Message Block Protocol)
    SMB Header
```

```
        Server Component: SMB
        Response in: 412
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 223
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 36
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
```

```
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 36
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 39
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.lpoptions

No.     Time        Source                Destination           Protocol Info
    412 10.209787   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: .lpoptions

Frame 412 (254 bytes on wire, 254 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.207439000
    Time delta from previous packet: 0.005660000 seconds
    Time since reference or first frame: 10.209787000 seconds
    Frame Number: 412
    Packet Length: 254 bytes
    Capture Length: 254 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 240
    Identification: 0x9d49 (40265)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
```

```
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1898 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 25940, Ack: 75371, Len: 188
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 25940    (relative sequence number)
    Next sequence number: 26128    (relative sequence number)
    Acknowledgement number: 75371    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x455d [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 184
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 411
        Time from request: 0.005660000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
```

```
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 223
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 116
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 116
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 129
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
```

```
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    413 10.210113   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.mysql_history

Frame 413 (182 bytes on wire, 182 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.207765000
    Time delta from previous packet: 0.000326000 seconds
    Time since reference or first frame: 10.210113000 seconds
    Frame Number: 413
    Packet Length: 182 bytes
    Capture Length: 182 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 168
    Identification: 0x5a51 (23121)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bd8 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 75371, Ack: 26128, Len: 116
    Source port: 51751 (51751)
```

```
    Destination port: netbios-ssn (139)
    Sequence number: 75371    (relative sequence number)
    Next sequence number: 75487    (relative sequence number)
    Acknowledgement number: 26128    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x76e6 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 112
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 414
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
```

```
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 224
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 44
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 44
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 47
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.mysql_history

No.     Time        Source                Destination           Protocol Info
```

```
    414 10.216237   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: .mysql_history

Frame 414 (262 bytes on wire, 262 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.213889000
    Time delta from previous packet: 0.006124000 seconds
    Time since reference or first frame: 10.216237000 seconds
    Frame Number: 414
    Packet Length: 262 bytes
    Capture Length: 262 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 248
    Identification: 0x9d4a (40266)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x188f [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 26128, Ack: 75487, Len: 196
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 26128    (relative sequence number)
    Next sequence number: 26324    (relative sequence number)
    Acknowledgement number: 75487    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x4d1c [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 192
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 413
        Time from request: 0.006124000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
```

```
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 224
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 124
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 124
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 137
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    415 10.216593   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.ssh

Frame 415 (162 bytes on wire, 162 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.214245000
    Time delta from previous packet: 0.000356000 seconds
    Time since reference or first frame: 10.216593000 seconds
    Frame Number: 415
    Packet Length: 162 bytes
    Capture Length: 162 bytes
```

```
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 148
    Identification: 0x5a52 (23122)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5beb [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 75487, Ack: 26324, Len: 96
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 75487    (relative sequence number)
    Next sequence number: 75583    (relative sequence number)
    Acknowledgement number: 26324    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xce16 [correct]
    Options: (12 bytes)
        NOP
        NOP
```

```
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 92
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 416
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 225
    Trans2 Request (0x32)
        Word Count (WCT): 15
```

```
        Total Parameter Count: 24
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 24
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 27
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.ssh

No.     Time        Source                Destination           Protocol Info
    416 10.222031   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: .ssh

Frame 416 (242 bytes on wire, 242 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.219683000
    Time delta from previous packet: 0.005438000 seconds
    Time since reference or first frame: 10.222031000 seconds
    Frame Number: 416
    Packet Length: 242 bytes
    Capture Length: 242 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
```

```
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 228
    Identification: 0x9d4b (40267)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18a2 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 26324, Ack: 75583, Len: 176
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 26324    (relative sequence number)
    Next sequence number: 26500    (relative sequence number)
    Acknowledgement number: 75583    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xba59 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 172
SMB (Server Message Block Protocol)
    SMB Header
```

```
        Server Component: SMB
        Response to: 415
        Time from request: 0.005438000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 225
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 104
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
```

```
        Data Count: 104
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 117
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    417 10.222756   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.TemporaryItems

Frame 417 (184 bytes on wire, 184 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.220408000
    Time delta from previous packet: 0.000725000 seconds
    Time since reference or first frame: 10.222756000 seconds
    Frame Number: 417
    Packet Length: 184 bytes
    Capture Length: 184 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 170
    Identification: 0x5a53 (23123)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
```

```
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bd4 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 75583, Ack: 26500, Len: 118
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 75583    (relative sequence number)
    Next sequence number: 75701    (relative sequence number)
    Acknowledgement number: 26500    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5494 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 114
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 418
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
```

```
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 226
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 46
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 46
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 49
```

```
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.TemporaryItems

No.     Time        Source                Destination           Protocol Info
    418 10.228656   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: .TemporaryItems

Frame 418 (262 bytes on wire, 262 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.226308000
    Time delta from previous packet: 0.005900000 seconds
    Time since reference or first frame: 10.228656000 seconds
    Frame Number: 418
    Packet Length: 262 bytes
    Capture Length: 262 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 248
    Identification: 0x9d4c (40268)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x188d [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 26500, Ack: 75701, Len: 196
```

```
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 26500    (relative sequence number)
    Next sequence number: 26696    (relative sequence number)
    Acknowledgement number: 75701    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x5b5b [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 192
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 417
        Time from request: 0.005900000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
```

```
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 226
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 124
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 124
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 137
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
```

```
    419 10.229182   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.Trash

Frame 419 (166 bytes on wire, 166 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.226834000
    Time delta from previous packet: 0.000526000 seconds
    Time since reference or first frame: 10.229182000 seconds
    Frame Number: 419
    Packet Length: 166 bytes
    Capture Length: 166 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 152
    Identification: 0x5a54 (23124)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5be5 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 75701, Ack: 26696, Len: 100
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 75701    (relative sequence number)
    Next sequence number: 75801    (relative sequence number)
    Acknowledgement number: 26696    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x15b8 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 96
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 420
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
```

```
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 227
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 28
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 28
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 31
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.Trash

No.     Time        Source                Destination           Protocol Info
    420 10.234479   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: .Trash

Frame 420 (246 bytes on wire, 246 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.232131000
    Time delta from previous packet: 0.005297000 seconds
    Time since reference or first frame: 10.234479000 seconds
    Frame Number: 420
```

```
    Packet Length: 246 bytes
    Capture Length: 246 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 232
    Identification: 0x9d4d (40269)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x189c [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 26696, Ack: 75801, Len: 180
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 26696    (relative sequence number)
    Next sequence number: 26876    (relative sequence number)
    Acknowledgement number: 75801    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x982f [correct]
    Options: (12 bytes)
```

```
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 176
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 419
        Time from request: 0.005297000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
```

```
        User ID: 100
        Multiplex ID: 227
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 108
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 108
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 121
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    421 10.234992   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.viminfo

Frame 421 (170 bytes on wire, 170 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.232644000
    Time delta from previous packet: 0.000513000 seconds
    Time since reference or first frame: 10.234992000 seconds
    Frame Number: 421
    Packet Length: 170 bytes
    Capture Length: 170 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
```

```
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 156
    Identification: 0x5a55 (23125)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5be0 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 75801, Ack: 26876, Len: 104
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 75801    (relative sequence number)
    Next sequence number: 75905    (relative sequence number)
    Acknowledgement number: 26876    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1d8b [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 100
SMB (Server Message Block Protocol)
    SMB Header
```

```
        Server Component: SMB
        Response in: 423
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 228
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 32
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
```

```
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 32
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 35
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.viminfo

No.     Time        Source                Destination           Protocol Info
    422 10.238779   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=26876 Ack=75905 Win=64240 Len=0 TSV=1545526522
TSER=636883964

Frame 422 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.236431000
    Time delta from previous packet: 0.003787000 seconds
    Time since reference or first frame: 10.238779000 seconds
    Frame Number: 422
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d4e (40270)
    Flags: 0x04 (Don't Fragment)
```

```
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x194f [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 26876, Ack: 75905, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 26876    (relative sequence number)
    Acknowledgement number: 75905    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xe521 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    423 10.241437   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: .viminfo

Frame 423 (250 bytes on wire, 250 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.239089000
    Time delta from previous packet: 0.006445000 seconds
    Time since reference or first frame: 10.241437000 seconds
    Frame Number: 423
    Packet Length: 250 bytes
    Capture Length: 250 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
```

```
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 236
    Identification: 0x9d4f (40271)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1896 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 26876, Ack: 75905, Len: 184
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 26876    (relative sequence number)
    Next sequence number: 27060    (relative sequence number)
    Acknowledgement number: 75905    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xbf5b [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
```

```
        .... ...0 = Add 0 to length
    Length: 180
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 421
        Time from request: 0.006445000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 228
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 112
```

```
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 112
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 125
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    424 10.241678   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Audio.mov

Frame 424 (172 bytes on wire, 172 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.239330000
    Time delta from previous packet: 0.000241000 seconds
    Time since reference or first frame: 10.241678000 seconds
    Frame Number: 424
    Packet Length: 172 bytes
    Capture Length: 172 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 158
    Identification: 0x5a56 (23126)
```

```
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bdd [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 75905, Ack: 27060, Len: 106
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 75905    (relative sequence number)
    Next sequence number: 76011    (relative sequence number)
    Acknowledgement number: 27060    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xcf60 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 102
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 425
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
```

```
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 229
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 34
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 34
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
```

```
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 37
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Audio.mov

No.     Time        Source                Destination           Protocol Info
    425 10.247163   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Audio.mov

Frame 425 (250 bytes on wire, 250 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.244815000
    Time delta from previous packet: 0.005485000 seconds
    Time since reference or first frame: 10.247163000 seconds
    Frame Number: 425
    Packet Length: 250 bytes
    Capture Length: 250 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 236
    Identification: 0x9d50 (40272)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1895 [correct]
    Source: 192.168.1.108 (192.168.1.108)
```

```
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 27060, Ack: 76011, Len: 184
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 27060    (relative sequence number)
    Next sequence number: 27244    (relative sequence number)
    Acknowledgement number: 76011    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x6e8b [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 180
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 424
        Time from request: 0.005485000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
```

```
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 229
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 112
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 112
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 125
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data
```

```
No.     Time        Source                Destination           Protocol Info
    426 10.247462   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \._Audio.mov

Frame 426 (176 bytes on wire, 176 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.245114000
    Time delta from previous packet: 0.000299000 seconds
    Time since reference or first frame: 10.247462000 seconds
    Frame Number: 426
    Packet Length: 176 bytes
    Capture Length: 176 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 162
    Identification: 0x5a57 (23127)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bd8 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 76011, Ack: 27244, Len: 110
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 76011    (relative sequence number)
    Next sequence number: 76121    (relative sequence number)
    Acknowledgement number: 27244    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
```

```
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x402a [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 106
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 427
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
```

```
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 230
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 38
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 38
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 41
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    427 10.252450   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: ._Audio.mov

Frame 427 (254 bytes on wire, 254 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.250102000
    Time delta from previous packet: 0.004988000 seconds
```

```
    Time since reference or first frame: 10.252450000 seconds
    Frame Number: 427
    Packet Length: 254 bytes
    Capture Length: 254 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 240
    Identification: 0x9d51 (40273)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1890 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 27244, Ack: 76121, Len: 188
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 27244    (relative sequence number)
    Next sequence number: 27432    (relative sequence number)
    Acknowledgement number: 76121    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
```

```
    Checksum: 0x0023 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 184
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 426
        Time from request: 0.004988000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
```

```
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 230
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 116
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 116
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 129
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    428 10.252627   192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \._Audio.mov

Frame 428 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.250279000
    Time delta from previous packet: 0.000177000 seconds
    Time since reference or first frame: 10.252627000 seconds
    Frame Number: 428
    Packet Length: 180 bytes
    Capture Length: 180 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x5a58 (23128)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bd3 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 76121, Ack: 27432, Len: 114
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 76121    (relative sequence number)
    Next sequence number: 76235    (relative sequence number)
    Acknowledgement number: 27432    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x85a7 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
```

```
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 429
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 231
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Reserved: 00
        File Name Len: 24
        Create Flags: 0x00000000
```

```
        Root FID: 0x00000000
        Access Mask: 0x00020001
        Allocation Size: 0
        File Attributes: 0x00000080
        Share Access: 0x00000007
        Disposition: Open (if file exists open it, else fail) (1)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 27
        File Name: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    429 10.257338   192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x3177

Frame 429 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.254990000
    Time delta from previous packet: 0.004711000 seconds
    Time since reference or first frame: 10.257338000 seconds
    Frame Number: 429
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9d52 (40274)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18e0 [correct]
    Source: 192.168.1.108 (192.168.1.108)
```

```
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 27432, Ack: 76235, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 27432    (relative sequence number)
    Next sequence number: 27539    (relative sequence number)
    Acknowledgement number: 76235    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x7367 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 103
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 428
        Time from request: 0.004711000 seconds
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
```

```
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 231
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
        FID: 0x3177
        Create action: The file existed and was opened (1)
        Created: Dec 11, 2006 15:23:30.000000000
        Last Access: Dec 11, 2006 15:23:31.000000000
        Last Write: Dec 11, 2006 15:23:31.000000000
        Change: Dec 11, 2006 15:23:31.000000000
        File Attributes: 0x00000022
        Allocation Size: 1048576
        End Of File: 82
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    430 10.257594   192.168.1.106         192.168.1.108         SMB      Read
AndX Request, FID: 0x3177, 82 bytes at offset 0

Frame 430 (129 bytes on wire, 129 bytes captured)
```

```
    Arrival Time: Dec 11, 2006 15:21:02.255246000
    Time delta from previous packet: 0.000256000 seconds
    Time since reference or first frame: 10.257594000 seconds
    Frame Number: 430
    Packet Length: 129 bytes
    Capture Length: 129 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 115
    Identification: 0x5a59 (23129)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c05 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 76235, Ack: 27539, Len: 63
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 76235    (relative sequence number)
    Next sequence number: 76298    (relative sequence number)
    Acknowledgement number: 27539    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
```

```
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xd1e3 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 59
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 431
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
```

```
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 232
    Read AndX Request (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3177
        Offset: 0
        Max Count Low: 82
        Min Count: 82
        Max Count High (multiply with 64K): 0
        Remaining: 82
        High Offset: 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    431 10.262102   192.168.1.108         192.168.1.106         SMB      Read
AndX Response, FID: 0x3177, 82 bytes

Frame 431 (211 bytes on wire, 211 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.259754000
    Time delta from previous packet: 0.004508000 seconds
    Time since reference or first frame: 10.262102000 seconds
    Frame Number: 431
    Packet Length: 211 bytes
    Capture Length: 211 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 197
    Identification: 0x9d53 (40275)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
```

```
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18b9 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 27539, Ack: 76298, Len: 145
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 27539    (relative sequence number)
    Next sequence number: 27684    (relative sequence number)
    Acknowledgement number: 76298    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xe7a6 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 141
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 430
        Time from request: 0.004508000 seconds
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
```

```
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 232
    Read AndX Response (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3177
        Remaining: 65535
        Data Compaction Mode: 0
        Reserved: 0000
        Data Length Low: 82
        Data Offset: 59
        Data Length High (multiply with 64K): 0
        Reserved: 000000000000
        Byte Count (BCC): 82
        File Data: 000516070002000000000000000000000000000000000000...

No.     Time        Source                Destination           Protocol Info
    432 10.262346   192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x3177
```

```
Frame 432 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.259998000
    Time delta from previous packet: 0.000244000 seconds
    Time since reference or first frame: 10.262346000 seconds
    Frame Number: 432
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
    Identification: 0x5a5a (23130)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c16 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 76298, Ack: 27684, Len: 45
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 76298    (relative sequence number)
    Next sequence number: 76343    (relative sequence number)
    Acknowledgement number: 27684    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
```

```
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x052d [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 433
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
```

```
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 233
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x3177
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    433 10.266579   192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 433 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.264231000
    Time delta from previous packet: 0.004233000 seconds
    Time since reference or first frame: 10.266579000 seconds
    Frame Number: 433
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d54 (40276)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1922 [correct]
    Source: 192.168.1.108 (192.168.1.108)
```

```
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 27684, Ack: 76343, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 27684    (relative sequence number)
    Next sequence number: 27723    (relative sequence number)
    Acknowledgement number: 76343    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x3e12 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 432
        Time from request: 0.004233000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
```

```
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 233
    Close Response (0x04)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    434 10.266849   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Backups

Frame 434 (168 bytes on wire, 168 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.264501000
    Time delta from previous packet: 0.000270000 seconds
    Time since reference or first frame: 10.266849000 seconds
    Frame Number: 434
    Packet Length: 168 bytes
    Capture Length: 168 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
```

```
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 154
    Identification: 0x5a5b (23131)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bdc [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 76343, Ack: 27723, Len: 102
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 76343    (relative sequence number)
    Next sequence number: 76445    (relative sequence number)
    Acknowledgement number: 27723    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x6f28 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 98
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
```

```
        Response in: 435
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 234
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 30
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
```

```
        Reserved: 0000
        Parameter Count: 30
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 33
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Backups

No.     Time        Source                Destination           Protocol Info
    435 10.272731   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Backups

Frame 435 (246 bytes on wire, 246 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.270383000
    Time delta from previous packet: 0.005882000 seconds
    Time since reference or first frame: 10.272731000 seconds
    Frame Number: 435
    Packet Length: 246 bytes
    Capture Length: 246 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 232
    Identification: 0x9d55 (40277)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
```

```
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1894 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 27723, Ack: 76445, Len: 180
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 27723    (relative sequence number)
    Next sequence number: 27903    (relative sequence number)
    Acknowledgement number: 76445    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x1bf2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 176
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 434
        Time from request: 0.005882000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
```

```
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 234
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 108
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 108
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 121
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
```

```
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    436 10.273196   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Desktop

Frame 436 (168 bytes on wire, 168 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.270848000
    Time delta from previous packet: 0.000465000 seconds
    Time since reference or first frame: 10.273196000 seconds
    Frame Number: 436
    Packet Length: 168 bytes
    Capture Length: 168 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 154
    Identification: 0x5a5c (23132)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bdb [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 76445, Ack: 27903, Len: 102
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
```

```
    Sequence number: 76445    (relative sequence number)
    Next sequence number: 76547    (relative sequence number)
    Acknowledgement number: 27903    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5c0e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 98
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 437
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
```

```
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 235
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 30
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 30
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 33
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Desktop

No.     Time        Source                Destination           Protocol Info
```

```
    437 10.278428   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Desktop

Frame 437 (246 bytes on wire, 246 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.276080000
    Time delta from previous packet: 0.005232000 seconds
    Time since reference or first frame: 10.278428000 seconds
    Frame Number: 437
    Packet Length: 246 bytes
    Capture Length: 246 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 232
    Identification: 0x9d56 (40278)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1893 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 27903, Ack: 76547, Len: 180
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 27903    (relative sequence number)
    Next sequence number: 28083    (relative sequence number)
    Acknowledgement number: 76547    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x86c3 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 176
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 436
        Time from request: 0.005232000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
```

```
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 235
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 108
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 108
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 121
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    438 10.278929   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Documents

Frame 438 (172 bytes on wire, 172 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.276581000
    Time delta from previous packet: 0.000501000 seconds
    Time since reference or first frame: 10.278929000 seconds
    Frame Number: 438
    Packet Length: 172 bytes
    Capture Length: 172 bytes
```

```
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 158
    Identification: 0x5a5d (23133)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bd6 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 76547, Ack: 28083, Len: 106
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 76547    (relative sequence number)
    Next sequence number: 76653    (relative sequence number)
    Acknowledgement number: 28083    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x81df [correct]
    Options: (12 bytes)
        NOP
        NOP
```

```
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 102
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 439
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 236
    Trans2 Request (0x32)
        Word Count (WCT): 15
```

```
        Total Parameter Count: 34
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 34
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 37
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Documents

No.     Time        Source                Destination           Protocol Info
    439 10.284500   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Documents

Frame 439 (250 bytes on wire, 250 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.282152000
    Time delta from previous packet: 0.005571000 seconds
    Time since reference or first frame: 10.284500000 seconds
    Frame Number: 439
    Packet Length: 250 bytes
    Capture Length: 250 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
```

```
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 236
    Identification: 0x9d57 (40279)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x188e [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 28083, Ack: 76653, Len: 184
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 28083    (relative sequence number)
    Next sequence number: 28267    (relative sequence number)
    Acknowledgement number: 76653    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xde12 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 180
SMB (Server Message Block Protocol)
    SMB Header
```

```
        Server Component: SMB
        Response to: 438
        Time from request: 0.005571000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 236
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 112
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
```

```
        Data Count: 112
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 125
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    440 10.285018   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Library

Frame 440 (168 bytes on wire, 168 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.282670000
    Time delta from previous packet: 0.000518000 seconds
    Time since reference or first frame: 10.285018000 seconds
    Frame Number: 440
    Packet Length: 168 bytes
    Capture Length: 168 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 154
    Identification: 0x5a5e (23134)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
```

```
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bd9 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 76653, Ack: 28267, Len: 102
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 76653    (relative sequence number)
    Next sequence number: 76755    (relative sequence number)
    Acknowledgement number: 28267    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5cd2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 98
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 441
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
```

```
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 237
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 30
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 30
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 33
```

```
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Library

No.     Time        Source                Destination           Protocol Info
    441 10.290638   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Library

Frame 441 (246 bytes on wire, 246 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.288290000
    Time delta from previous packet: 0.005620000 seconds
    Time since reference or first frame: 10.290638000 seconds
    Frame Number: 441
    Packet Length: 246 bytes
    Capture Length: 246 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 232
    Identification: 0x9d58 (40280)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1891 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 28267, Ack: 76755, Len: 180
```

```
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 28267    (relative sequence number)
    Next sequence number: 28447    (relative sequence number)
    Acknowledgement number: 76755    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x8d5e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 176
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 440
        Time from request: 0.005620000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
```

```
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 237
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 108
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 108
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 121
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
```

```
    442 10.291142   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Movies

Frame 442 (166 bytes on wire, 166 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.288794000
    Time delta from previous packet: 0.000504000 seconds
    Time since reference or first frame: 10.291142000 seconds
    Frame Number: 442
    Packet Length: 166 bytes
    Capture Length: 166 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 152
    Identification: 0x5a5f (23135)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bda [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 76755, Ack: 28447, Len: 100
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 76755    (relative sequence number)
    Next sequence number: 76855    (relative sequence number)
    Acknowledgement number: 28447    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xbcc2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 96
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 443
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
```

```
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 238
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 28
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 28
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 31
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Movies

No.     Time        Source                Destination           Protocol Info
    443 10.296933   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Movies

Frame 443 (246 bytes on wire, 246 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.294585000
    Time delta from previous packet: 0.005791000 seconds
    Time since reference or first frame: 10.296933000 seconds
    Frame Number: 443
```

```
    Packet Length: 246 bytes
    Capture Length: 246 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 232
    Identification: 0x9d59 (40281)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1890 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 28447, Ack: 76855, Len: 180
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 28447    (relative sequence number)
    Next sequence number: 28627    (relative sequence number)
    Acknowledgement number: 76855    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xfc16 [correct]
    Options: (12 bytes)
```

```
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 176
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 442
        Time from request: 0.005791000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
```

```
        User ID: 100
        Multiplex ID: 238
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 108
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 108
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 121
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    444 10.297444   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Music

Frame 444 (164 bytes on wire, 164 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.295096000
    Time delta from previous packet: 0.000511000 seconds
    Time since reference or first frame: 10.297444000 seconds
    Frame Number: 444
    Packet Length: 164 bytes
    Capture Length: 164 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
```

```
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 150
    Identification: 0x5a60 (23136)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bdb [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 76855, Ack: 28627, Len: 98
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 76855    (relative sequence number)
    Next sequence number: 76953    (relative sequence number)
    Acknowledgement number: 28627    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x2cb5 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 94
SMB (Server Message Block Protocol)
    SMB Header
```

```
        Server Component: SMB
        Response in: 445
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 239
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 26
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
```

```
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 26
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 29
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Music

No.     Time        Source                Destination           Protocol Info
    445 10.303863   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Music

Frame 445 (242 bytes on wire, 242 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.301515000
    Time delta from previous packet: 0.006419000 seconds
    Time since reference or first frame: 10.303863000 seconds
    Frame Number: 445
    Packet Length: 242 bytes
    Capture Length: 242 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 228
    Identification: 0x9d5a (40282)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
```

```
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1893 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 28627, Ack: 76953, Len: 176
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 28627    (relative sequence number)
    Next sequence number: 28803    (relative sequence number)
    Acknowledgement number: 76953    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x6545 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 172
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 444
        Time from request: 0.006419000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
```

```
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 239
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 104
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 104
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 117
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
```

```
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    446 10.304405   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \mysql

Frame 446 (164 bytes on wire, 164 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.302057000
    Time delta from previous packet: 0.000542000 seconds
    Time since reference or first frame: 10.304405000 seconds
    Frame Number: 446
    Packet Length: 164 bytes
    Capture Length: 164 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 150
    Identification: 0x5a61 (23137)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bda [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 76953, Ack: 28803, Len: 98
    Source port: 51751 (51751)
```

```
    Destination port: netbios-ssn (139)
    Sequence number: 76953    (relative sequence number)
    Next sequence number: 77051    (relative sequence number)
    Acknowledgement number: 28803    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xf5a2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 94
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 447
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
```

```
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 240
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 26
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 26
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 29
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \mysql

No.     Time        Source                Destination           Protocol Info
```

```
    447 10.309936   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: mysql

Frame 447 (242 bytes on wire, 242 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.307588000
    Time delta from previous packet: 0.005531000 seconds
    Time since reference or first frame: 10.309936000 seconds
    Frame Number: 447
    Packet Length: 242 bytes
    Capture Length: 242 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 228
    Identification: 0x9d5b (40283)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1892 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 28803, Ack: 77051, Len: 176
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 28803    (relative sequence number)
    Next sequence number: 28979    (relative sequence number)
    Acknowledgement number: 77051    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xdf77 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 172
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 446
        Time from request: 0.005531000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
```

```
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 240
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 104
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 104
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 117
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    448 10.310378   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Picture 1.png

Frame 448 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.308030000
    Time delta from previous packet: 0.000442000 seconds
    Time since reference or first frame: 10.310378000 seconds
    Frame Number: 448
    Packet Length: 180 bytes
    Capture Length: 180 bytes
```

```
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x5a62 (23138)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bc9 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 77051, Ack: 28979, Len: 114
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 77051    (relative sequence number)
    Next sequence number: 77165    (relative sequence number)
    Acknowledgement number: 28979    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x893e [correct]
    Options: (12 bytes)
        NOP
        NOP
```

```
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 449
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 241
    Trans2 Request (0x32)
        Word Count (WCT): 15
```

```
        Total Parameter Count: 42
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 42
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 45
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Picture 1.png

No.     Time        Source                Destination           Protocol Info
    449 10.315763   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Picture 1.png

Frame 449 (258 bytes on wire, 258 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.313415000
    Time delta from previous packet: 0.005385000 seconds
    Time since reference or first frame: 10.315763000 seconds
    Frame Number: 449
    Packet Length: 258 bytes
    Capture Length: 258 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
```

```
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 244
    Identification: 0x9d5c (40284)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1881 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 28979, Ack: 77165, Len: 192
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 28979    (relative sequence number)
    Next sequence number: 29171    (relative sequence number)
    Acknowledgement number: 77165    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x454f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 188
SMB (Server Message Block Protocol)
    SMB Header
```

```
        Server Component: SMB
        Response to: 448
        Time from request: 0.005385000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 241
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 120
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
```

```
        Data Count: 120
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 133
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    450 10.316064   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Pictures

Frame 450 (170 bytes on wire, 170 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.313716000
    Time delta from previous packet: 0.000301000 seconds
    Time since reference or first frame: 10.316064000 seconds
    Frame Number: 450
    Packet Length: 170 bytes
    Capture Length: 170 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 156
    Identification: 0x5a63 (23139)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
```

```
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bd2 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 77165, Ack: 29171, Len: 104
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 77165    (relative sequence number)
    Next sequence number: 77269    (relative sequence number)
    Acknowledgement number: 29171    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xd83f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 100
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 451
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
```

```
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 242
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 32
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 32
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 35
```

```
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Pictures

No.     Time        Source                Destination           Protocol Info
    451 10.322462   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Pictures

Frame 451 (250 bytes on wire, 250 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.320114000
    Time delta from previous packet: 0.006398000 seconds
    Time since reference or first frame: 10.322462000 seconds
    Frame Number: 451
    Packet Length: 250 bytes
    Capture Length: 250 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 236
    Identification: 0x9d5d (40285)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1888 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 29171, Ack: 77269, Len: 184
```

```
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 29171    (relative sequence number)
    Next sequence number: 29355    (relative sequence number)
    Acknowledgement number: 77269    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x0f90 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 180
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 450
        Time from request: 0.006398000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
```

```
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 242
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 112
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 112
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 125
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
```

```
    452 10.323365   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.emacs.d\Contents

Frame 452 (188 bytes on wire, 188 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.321017000
    Time delta from previous packet: 0.000903000 seconds
    Time since reference or first frame: 10.323365000 seconds
    Frame Number: 452
    Packet Length: 188 bytes
    Capture Length: 188 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 174
    Identification: 0x5a64 (23140)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bbf [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 77269, Ack: 29355, Len: 122
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 77269    (relative sequence number)
    Next sequence number: 77391    (relative sequence number)
    Acknowledgement number: 29355    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xb1c2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 118
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 453
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
```

```
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 243
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 50
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 50
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 53
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.emacs.d\Contents

No.     Time        Source                Destination           Protocol Info
    453 10.328639   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Error: STATUS_NO_SUCH_FILE

Frame 453 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.326291000
    Time delta from previous packet: 0.005274000 seconds
    Time since reference or first frame: 10.328639000 seconds
    Frame Number: 453
```

```
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d5e (40286)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1918 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 29355, Ack: 77391, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 29355    (relative sequence number)
    Next sequence number: 29394    (relative sequence number)
    Acknowledgement number: 77391    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xfb62 [correct]
    Options: (12 bytes)
```

```
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 452
        Time from request: 0.005274000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_NO_SUCH_FILE (0xc000000f)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
```

```
        User ID: 100
        Multiplex ID: 243
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    454 10.328890   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.emacs.d\Contents

Frame 454 (188 bytes on wire, 188 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.326542000
    Time delta from previous packet: 0.000251000 seconds
    Time since reference or first frame: 10.328890000 seconds
    Frame Number: 454
    Packet Length: 188 bytes
    Capture Length: 188 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 174
    Identification: 0x5a65 (23141)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bbe [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 77391, Ack: 29394, Len: 122
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
```

```
    Sequence number: 77391    (relative sequence number)
    Next sequence number: 77513    (relative sequence number)
    Acknowledgement number: 29394    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xb021 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 118
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 455
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
```

```
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 244
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 50
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 50
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 53
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.emacs.d\Contents

No.     Time        Source                Destination           Protocol Info
```

```
    455 10.333370   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Error: STATUS_NO_SUCH_FILE

Frame 455 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.331022000
    Time delta from previous packet: 0.004480000 seconds
    Time since reference or first frame: 10.333370000 seconds
    Frame Number: 455
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d5f (40287)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1917 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 29394, Ack: 77513, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 29394    (relative sequence number)
    Next sequence number: 29433    (relative sequence number)
    Acknowledgement number: 77513    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
```

```
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xf9c1 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 454
        Time from request: 0.004480000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_NO_SUCH_FILE (0xc000000f)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
```

```
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 244
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    456 10.334644   192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \._Audio.mov

Frame 456 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.332296000
    Time delta from previous packet: 0.001274000 seconds
    Time since reference or first frame: 10.334644000 seconds
    Frame Number: 456
    Packet Length: 180 bytes
    Capture Length: 180 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x5a66 (23142)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
```

```
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bc5 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 77513, Ack: 29433, Len: 114
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 77513    (relative sequence number)
    Next sequence number: 77627    (relative sequence number)
    Acknowledgement number: 29433    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x6a66 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 457
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
```

```
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 245
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Reserved: 00
        File Name Len: 24
        Create Flags: 0x00000000
        Root FID: 0x00000000
        Access Mask: 0x00020001
        Allocation Size: 0
        File Attributes: 0x00000080
        Share Access: 0x00000007
        Disposition: Open (if file exists open it, else fail) (1)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 27
        File Name: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    457 10.338778   192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x3178
```

```
Frame 457 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.336430000
    Time delta from previous packet: 0.004134000 seconds
    Time since reference or first frame: 10.338778000 seconds
    Frame Number: 457
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9d60 (40288)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18d2 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 29433, Ack: 77627, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 29433    (relative sequence number)
    Next sequence number: 29540    (relative sequence number)
    Acknowledgement number: 77627    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
```

```
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x5726 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 103
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 456
        Time from request: 0.004134000 seconds
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
```

```
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 245
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
        FID: 0x3178
        Create action: The file existed and was opened (1)
        Created: Dec 11, 2006 15:23:30.000000000
        Last Access: Dec 11, 2006 15:23:31.000000000
        Last Write: Dec 11, 2006 15:23:31.000000000
        Change: Dec 11, 2006 15:23:31.000000000
        File Attributes: 0x00000022
        Allocation Size: 1048576
        End Of File: 82
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    458 10.339015   192.168.1.106         192.168.1.108         SMB      Read
AndX Request, FID: 0x3178, 82 bytes at offset 0

Frame 458 (129 bytes on wire, 129 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.336667000
    Time delta from previous packet: 0.000237000 seconds
    Time since reference or first frame: 10.339015000 seconds
    Frame Number: 458
    Packet Length: 129 bytes
    Capture Length: 129 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
```

```
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 115
    Identification: 0x5a67 (23143)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bf7 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 77627, Ack: 29540, Len: 63
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 77627    (relative sequence number)
    Next sequence number: 77690    (relative sequence number)
    Acknowledgement number: 29540    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xb6a1 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883964, tsecr 1545526522
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 59
SMB (Server Message Block Protocol)
```

```
    SMB Header
        Server Component: SMB
        Response in: 459
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 246
    Read AndX Request (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3178
        Offset: 0
        Max Count Low: 82
        Min Count: 82
        Max Count High (multiply with 64K): 0
```

```
        Remaining: 82
        High Offset: 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    459 10.343026   192.168.1.108         192.168.1.106         SMB      Read
AndX Response, FID: 0x3178, 82 bytes

Frame 459 (211 bytes on wire, 211 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.340678000
    Time delta from previous packet: 0.004011000 seconds
    Time since reference or first frame: 10.343026000 seconds
    Frame Number: 459
    Packet Length: 211 bytes
    Capture Length: 211 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 197
    Identification: 0x9d61 (40289)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18ab [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 29540, Ack: 77690, Len: 145
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 29540    (relative sequence number)
    Next sequence number: 29685    (relative sequence number)
    Acknowledgement number: 77690    (relative ack number)
```

```
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xcc65 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883964
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 141
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 458
        Time from request: 0.004011000 seconds
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
```

```
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 246
    Read AndX Response (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3178
        Remaining: 65535
        Data Compaction Mode: 0
        Reserved: 0000
        Data Length Low: 82
        Data Offset: 59
        Data Length High (multiply with 64K): 0
        Reserved: 000000000000
        Byte Count (BCC): 82
        File Data: 000516070002000000000000000000000000000000000000...

No.     Time        Source                Destination           Protocol Info
    460 10.343090   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=77690 Ack=29685 Win=65535 Len=0 TSV=636883965
TSER=1545526522

Frame 460 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.340742000
    Time delta from previous packet: 0.000064000 seconds
    Time since reference or first frame: 10.343090000 seconds
    Frame Number: 460
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
```

```
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a68 (23144)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c35 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 77690, Ack: 29685, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 77690    (relative sequence number)
    Acknowledgement number: 29685    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xce1f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    461 10.343265   192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x3178
```

```
Frame 461 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.340917000
    Time delta from previous packet: 0.000239000 seconds
    Time since reference or first frame: 10.343265000 seconds
    Frame Number: 461
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
    Identification: 0x5a69 (23145)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c07 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 77690, Ack: 29685, Len: 45
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 77690    (relative sequence number)
    Next sequence number: 77735    (relative sequence number)
    Acknowledgement number: 29685    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
```

```
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xe9e9 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526522
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 462
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
```

```
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 247
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x3178
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    462 10.349047   192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 462 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.346699000
    Time delta from previous packet: 0.005782000 seconds
    Time since reference or first frame: 10.349047000 seconds
    Frame Number: 462
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d62 (40290)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1914 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
```

```
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 29685, Ack: 77735, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 29685    (relative sequence number)
    Next sequence number: 29724    (relative sequence number)
    Acknowledgement number: 77735    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x22d0 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883965
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 461
        Time from request: 0.005782000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
```

```
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 247
    Close Response (0x04)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    463 10.349117   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=77735 Ack=29724 Win=65535 Len=0 TSV=636883965
TSER=1545526522

Frame 463 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.346769000
    Time delta from previous packet: 0.000070000 seconds
    Time since reference or first frame: 10.349117000 seconds
    Frame Number: 463
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
```

```
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a6a (23146)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c33 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 77735, Ack: 29724, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 77735    (relative sequence number)
    Acknowledgement number: 29724    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xcdcb [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    464 10.351706   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Public

Frame 464 (166 bytes on wire, 166 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.349358000
    Time delta from previous packet: 0.002659000 seconds
    Time since reference or first frame: 10.351706000 seconds
```

```
    Frame Number: 464
    Packet Length: 166 bytes
    Capture Length: 166 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 152
    Identification: 0x5a6b (23147)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bce [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 77735, Ack: 29724, Len: 100
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 77735    (relative sequence number)
    Next sequence number: 77835    (relative sequence number)
    Acknowledgement number: 29724    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xbdf0 [correct]
```

```
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526522
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 96
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 465
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 248
```

```
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 28
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 28
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 31
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Public

No.     Time        Source                Destination           Protocol Info
    465 10.356840   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Public

Frame 465 (246 bytes on wire, 246 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.354492000
    Time delta from previous packet: 0.005134000 seconds
    Time since reference or first frame: 10.356840000 seconds
    Frame Number: 465
    Packet Length: 246 bytes
    Capture Length: 246 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 232
    Identification: 0x9d63 (40291)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1886 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 29724, Ack: 77835, Len: 180
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 29724    (relative sequence number)
    Next sequence number: 29904    (relative sequence number)
    Acknowledgement number: 77835    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x4b33 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883965
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
```

```
    Length: 176
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 464
        Time from request: 0.005134000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 248
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 108
        Reserved: 0000
```

```
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 108
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 121
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    466 10.356943   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=77835 Ack=29904 Win=65535 Len=0 TSV=636883965
TSER=1545526522

Frame 466 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.354595000
    Time delta from previous packet: 0.000103000 seconds
    Time since reference or first frame: 10.356943000 seconds
    Frame Number: 466
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a6c (23148)
```

```
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c31 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 77835, Ack: 29904, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 77835    (relative sequence number)
    Acknowledgement number: 29904    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xccb3 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    467 10.357459   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \Sites

Frame 467 (164 bytes on wire, 164 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.355111000
    Time delta from previous packet: 0.000619000 seconds
    Time since reference or first frame: 10.357459000 seconds
    Frame Number: 467
    Packet Length: 164 bytes
    Capture Length: 164 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
```

```
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 150
    Identification: 0x5a6d (23149)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bce [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 77835, Ack: 29904, Len: 98
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 77835    (relative sequence number)
    Next sequence number: 77933    (relative sequence number)
    Acknowledgement number: 29904    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x12e3 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526522
NetBIOS Session Service
    Message Type: Session message
```

```
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 94
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 468
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 249
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 26
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
```

```
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 26
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 29
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \Sites

No.     Time        Source                Destination           Protocol Info
    468 10.363845   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Files: Sites

Frame 468 (242 bytes on wire, 242 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.361497000
    Time delta from previous packet: 0.006386000 seconds
    Time since reference or first frame: 10.363845000 seconds
    Frame Number: 468
    Packet Length: 242 bytes
    Capture Length: 242 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
```

```
        .... ...0 = ECN-CE: 0
    Total Length: 228
    Identification: 0x9d64 (40292)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1889 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 29904, Ack: 77933, Len: 176
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 29904    (relative sequence number)
    Next sequence number: 30080    (relative sequence number)
    Acknowledgement number: 77933    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xf0a5 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526522, tsecr 636883965
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 172
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 467
        Time from request: 0.006386000 seconds
        SMB Command: Trans2 (0x32)
```

```
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 249
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 10
        Total Parameter Count: 10
        Total Data Count: 104
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 104
        Data Offset: 68
        Data Displacement: 0
        Setup Count: 0
```

```
        Reserved: 00
        Byte Count (BCC): 117
        Padding: 00
        FIND_FIRST2 Parameters
            Level of Interest: Find File Both Directory Info (260)
            Search ID: 0xfffd
            Search Count: 1
            End Of Search: 1
            EA Error offset: 0
            Last Name Offset: 0
        Padding: 0000
        FIND_FIRST2 Data

No.     Time        Source                Destination           Protocol Info
    469 10.363938   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=77933 Ack=30080 Win=65535 Len=0 TSV=636883965
TSER=1545526522

Frame 469 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.361590000
    Time delta from previous packet: 0.000093000 seconds
    Time since reference or first frame: 10.363938000 seconds
    Frame Number: 469
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a6e (23150)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
```

```
    Header checksum: 0x5c2f [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 77933, Ack: 30080, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 77933    (relative sequence number)
    Acknowledgement number: 30080    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xcba1 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526522
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    470 10.365546   192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \.DS_Store

Frame 470 (176 bytes on wire, 176 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.363198000
    Time delta from previous packet: 0.001701000 seconds
    Time since reference or first frame: 10.365546000 seconds
    Frame Number: 470
    Packet Length: 176 bytes
    Capture Length: 176 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
```

```
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 162
    Identification: 0x5a6f (23151)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bc0 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 77933, Ack: 30080, Len: 110
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 77933    (relative sequence number)
    Next sequence number: 78043    (relative sequence number)
    Acknowledgement number: 30080    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x3347 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526522
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 106
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 472
```

```
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 250
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Reserved: 00
        File Name Len: 20
        Create Flags: 0x00000000
        Root FID: 0x00000000
        Access Mask: 0x00020001
        Allocation Size: 0
        File Attributes: 0x00000080
        Share Access: 0x00000007
```

```
        Disposition: Open (if file exists open it, else fail) (1)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 23
        File Name: \.DS_Store

No.     Time        Source                Destination           Protocol Info
    471 10.369091   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=30080 Ack=78043 Win=64130 Len=0 TSV=1545526523
TSER=636883965

Frame 471 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.366743000
    Time delta from previous packet: 0.003545000 seconds
    Time since reference or first frame: 10.369091000 seconds
    Frame Number: 471
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d65 (40293)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1938 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 30080, Ack: 78043, Len: 0
    Source port: netbios-ssn (139)
```

```
    Destination port: 51751 (51751)
    Sequence number: 30080    (relative sequence number)
    Acknowledgement number: 78043    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64130
    Checksum: 0xd0af [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    472 10.371462   192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x3179

Frame 472 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.369114000
    Time delta from previous packet: 0.005916000 seconds
    Time since reference or first frame: 10.371462000 seconds
    Frame Number: 472
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9d66 (40294)
```

```
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18cc [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 30080, Ack: 78043, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 30080    (relative sequence number)
    Next sequence number: 30187    (relative sequence number)
    Acknowledgement number: 78043    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x40a2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 103
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 470
        Time from request: 0.005916000 seconds
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
```

```
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 250
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
        FID: 0x3179
        Create action: The file existed and was opened (1)
        Created: Sep 22, 2006 18:40:31.000000000
        Last Access: Dec 11, 2006 15:23:26.000000000
        Last Write: Dec 10, 2006 01:50:09.000000000
        Change: Dec 10, 2006 01:50:09.000000000
        File Attributes: 0x00000002
        Allocation Size: 1048576
        End Of File: 12292
        File Type: Disk file or directory (0)
        IPC State: 0x0000
```

```
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    473 10.371532   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=78043 Ack=30187 Win=65535 Len=0 TSV=636883965
TSER=1545526523

Frame 473 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.369184000
    Time delta from previous packet: 0.000070000 seconds
    Time since reference or first frame: 10.371532000 seconds
    Frame Number: 473
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a70 (23152)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c2d [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78043, Ack: 30187, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 78043    (relative sequence number)
    Acknowledgement number: 30187    (relative ack number)
    Header length: 32 bytes
```

```
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xcac7 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526523
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    474 10.371705   192.168.1.106         192.168.1.108         SMB      Read
AndX Request, FID: 0x3179, 12292 bytes at offset 0

Frame 474 (129 bytes on wire, 129 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.369357000
    Time delta from previous packet: 0.000243000 seconds
    Time since reference or first frame: 10.371705000 seconds
    Frame Number: 474
    Packet Length: 129 bytes
    Capture Length: 129 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 115
    Identification: 0x5a71 (23153)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
```

```
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bed [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78043, Ack: 30187, Len: 63
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 78043    (relative sequence number)
    Next sequence number: 78106    (relative sequence number)
    Acknowledgement number: 30187    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1e61 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526523
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 59
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 476
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
```

```
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 251
    Read AndX Request (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3179
        Offset: 0
        Max Count Low: 12292
        Min Count: 12292
        Max Count High (multiply with 64K): 0
        Remaining: 12292
        High Offset: 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    475 10.377408   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=30187 Ack=78106 Win=64177 Len=0 TSV=1545526523
TSER=636883965

Frame 475 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.375060000
    Time delta from previous packet: 0.005703000 seconds
    Time since reference or first frame: 10.377408000 seconds
```

```
    Frame Number: 475
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d67 (40295)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1936 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 30187, Ack: 78106, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 30187    (relative sequence number)
    Acknowledgement number: 78106    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64177
    Checksum: 0xcfd6 [correct]
    Options: (12 bytes)
```

```
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    476 10.385812   192.168.1.108         192.168.1.106         SMB      Read
AndX Response, FID: 0x3179, 12292 bytes

Frame 476 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.383464000
    Time delta from previous packet: 0.014107000 seconds
    Time since reference or first frame: 10.385812000 seconds
    Frame Number: 476
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x9d68 (40296)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x138d [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 30187, Ack: 78106, Len: 1448
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 30187    (relative sequence number)
    Next sequence number: 31635    (relative sequence number)
```

```
    Acknowledgement number: 78106    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xb60c [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
    Last frame of this PDU: 486
    Time until the last segment of this PDU: 0.069281000 seconds
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 12351
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 474
        Time from request: 0.014107000 seconds
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
```

```
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 251
    Read AndX Response (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x3179
        Remaining: 65535
        Data Compaction Mode: 0
        Reserved: 0000
        Data Length Low: 12292
        Data Offset: 59
        Data Length High (multiply with 64K): 0
        Reserved: 000000000000
        Byte Count (BCC): 12292
        File Data: Incomplete. Only 1385 of 12292 bytes

No.     Time        Source                Destination           Protocol Info
    477 10.394525   192.168.1.108         192.168.1.106         TCP
[Continuation to #476] netbios-ssn > 51751 [ACK] Seq=31635 Ack=78106 Win=64240
Len=1448 TSV=1545526523 TSER=636883965

Frame 477 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.392177000
    Time delta from previous packet: 0.008713000 seconds
    Time since reference or first frame: 10.394525000 seconds
    Frame Number: 477
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
```

```
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x9d69 (40297)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x138c [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 31635, Ack: 78106, Len: 1448
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 31635    (relative sequence number)
    Next sequence number: 33083    (relative sequence number)
    Acknowledgement number: 78106    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xb83f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
    This is a continuation to the PDU in frame: 476
```

```
No.     Time        Source                Destination           Protocol Info
    478 10.394620   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=78106 Ack=33083 Win=63716 Len=0 TSV=636883965
TSER=1545526523

Frame 478 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.392272000
    Time delta from previous packet: 0.008808000 seconds
    Time since reference or first frame: 10.394620000 seconds
    Frame Number: 478
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a72 (23154)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c2b [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78106, Ack: 33083, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 78106    (relative sequence number)
    Acknowledgement number: 33083    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
```

```
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 63716
    Checksum: 0xc653 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526523
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    479 10.404386   192.168.1.108         192.168.1.106         TCP
[Continuation to #476] netbios-ssn > 51751 [ACK] Seq=33083 Ack=78106 Win=64240
Len=1448 TSV=1545526523 TSER=636883965

Frame 479 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.402038000
    Time delta from previous packet: 0.018574000 seconds
    Time since reference or first frame: 10.404386000 seconds
    Frame Number: 479
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x9d6a (40298)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x138b [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 33083, Ack: 78106, Len: 1448
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 33083    (relative sequence number)
    Next sequence number: 34531    (relative sequence number)
    Acknowledgement number: 78106    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x774f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
    This is a continuation to the PDU in frame: 476

No.     Time        Source                Destination           Protocol Info
    480 10.413939   192.168.1.108         192.168.1.106         TCP
[Continuation to #476] netbios-ssn > 51751 [ACK] Seq=34531 Ack=78106 Win=64240
Len=1448 TSV=1545526523 TSER=636883965

Frame 480 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.411591000
    Time delta from previous packet: 0.028127000 seconds
    Time since reference or first frame: 10.413939000 seconds
    Frame Number: 480
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x9d6b (40299)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x138a [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 34531, Ack: 78106, Len: 1448
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 34531    (relative sequence number)
    Next sequence number: 35979    (relative sequence number)
    Acknowledgement number: 78106    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x643e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
    This is a continuation to the PDU in frame: 476

No.     Time        Source                Destination           Protocol Info
```

```
    481 10.422694   192.168.1.108         192.168.1.106         TCP
[Continuation to #476] netbios-ssn > 51751 [ACK] Seq=35979 Ack=78106 Win=64240
Len=1448 TSV=1545526523 TSER=636883965

Frame 481 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.420346000
    Time delta from previous packet: 0.036882000 seconds
    Time since reference or first frame: 10.422694000 seconds
    Frame Number: 481
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x9d6c (40300)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1389 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 35979, Ack: 78106, Len: 1448
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 35979    (relative sequence number)
    Next sequence number: 37427    (relative sequence number)
    Acknowledgement number: 78106    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
```

```
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x5527 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
    This is a continuation to the PDU in frame: 476

No.     Time        Source                Destination           Protocol Info
    482 10.431572   192.168.1.108         192.168.1.106         TCP
[Continuation to #476] netbios-ssn > 51751 [ACK] Seq=37427 Ack=78106 Win=64240
Len=1448 TSV=1545526523 TSER=636883965

Frame 482 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.429224000
    Time delta from previous packet: 0.045760000 seconds
    Time since reference or first frame: 10.431572000 seconds
    Frame Number: 482
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x9d6d (40301)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x1388 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 37427, Ack: 78106, Len: 1448
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 37427    (relative sequence number)
    Next sequence number: 38875    (relative sequence number)
    Acknowledgement number: 78106    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xb3f3 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
    This is a continuation to the PDU in frame: 476

No.     Time        Source                Destination           Protocol Info
    483 10.431686   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=78106 Ack=38875 Win=65535 Len=0 TSV=636883965
TSER=1545526523

Frame 483 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.429338000
    Time delta from previous packet: 0.045874000 seconds
    Time since reference or first frame: 10.431686000 seconds
    Frame Number: 483
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a73 (23155)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c2a [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78106, Ack: 38875, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 78106    (relative sequence number)
    Acknowledgement number: 38875    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xa898 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526523
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    484 10.441257   192.168.1.108         192.168.1.106         TCP
[Continuation to #476] netbios-ssn > 51751 [ACK] Seq=38875 Ack=78106 Win=64240
Len=1448 TSV=1545526523 TSER=636883965
```

```
Frame 484 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.438909000
    Time delta from previous packet: 0.055445000 seconds
    Time since reference or first frame: 10.441257000 seconds
    Frame Number: 484
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x9d6e (40302)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1387 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 38875, Ack: 78106, Len: 1448
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 38875    (relative sequence number)
    Next sequence number: 40323    (relative sequence number)
    Acknowledgement number: 78106    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
```

```
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xa7ff [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
    This is a continuation to the PDU in frame: 476

No.     Time        Source                Destination           Protocol Info
    485 10.449912   192.168.1.108         192.168.1.106         TCP
[Continuation to #476] netbios-ssn > 51751 [ACK] Seq=40323 Ack=78106 Win=64240
Len=1448 TSV=1545526523 TSER=636883965

Frame 485 (1514 bytes on wire, 1514 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.447564000
    Time delta from previous packet: 0.064100000 seconds
    Time since reference or first frame: 10.449912000 seconds
    Frame Number: 485
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x9d6f (40303)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1386 [correct]
    Source: 192.168.1.108 (192.168.1.108)
```

```
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 40323, Ack: 78106, Len: 1448
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 40323    (relative sequence number)
    Next sequence number: 41771    (relative sequence number)
    Acknowledgement number: 78106    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xa257 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
    This is a continuation to the PDU in frame: 476

No.     Time        Source                Destination           Protocol Info
    486 10.455093   192.168.1.108         192.168.1.106         TCP
[Continuation to #476] netbios-ssn > 51751 [PSH, ACK] Seq=41771 Ack=78106
Win=64240 Len=771 TSV=1545526523 TSER=636883965

Frame 486 (837 bytes on wire, 837 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.452745000
    Time delta from previous packet: 0.069281000 seconds
    Time since reference or first frame: 10.455093000 seconds
    Frame Number: 486
    Packet Length: 837 bytes
    Capture Length: 837 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
```

```
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 823
    Identification: 0x9d70 (40304)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x162a [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 41771, Ack: 78106, Len: 771
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 41771    (relative sequence number)
    Next sequence number: 42542    (relative sequence number)
    Acknowledgement number: 78106    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x9f4c [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
    This is a continuation to the PDU in frame: 476

No.     Time        Source                Destination           Protocol Info
    487 10.455166   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=78106 Ack=42542 Win=65535 Len=0 TSV=636883965
TSER=1545526523

Frame 487 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.452818000
```

```
    Time delta from previous packet: 0.069354000 seconds
    Time since reference or first frame: 10.455166000 seconds
    Frame Number: 487
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a74 (23156)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c29 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78106, Ack: 42542, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 78106    (relative sequence number)
    Acknowledgement number: 42542    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
```

```
    Checksum: 0x9a45 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526523
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    488 10.455334   192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x3179

Frame 488 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.452986000
    Time delta from previous packet: 0.069522000 seconds
    Time since reference or first frame: 10.455334000 seconds
    Frame Number: 488
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
    Identification: 0x5a75 (23157)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bfb [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78106, Ack: 42542, Len: 45
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
```

```
    Sequence number: 78106    (relative sequence number)
    Next sequence number: 78151    (relative sequence number)
    Acknowledgement number: 42542    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xb10e [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526523
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 490
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
```

```
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 252
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x3179
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    489 10.459713   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=42542 Ack=78151 Win=64195 Len=0 TSV=1545526523
TSER=636883965

Frame 489 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.457365000
    Time delta from previous packet: 0.004379000 seconds
    Time since reference or first frame: 10.459713000 seconds
    Frame Number: 489
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
```

```
    Identification: 0x9d71 (40305)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x192c [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 42542, Ack: 78151, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 42542    (relative sequence number)
    Acknowledgement number: 78151    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64195
    Checksum: 0x9f54 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    490 10.461871   192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 490 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.459523000
    Time delta from previous packet: 0.006537000 seconds
    Time since reference or first frame: 10.461871000 seconds
    Frame Number: 490
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
```

```
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d72 (40306)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1904 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 42542, Ack: 78151, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 42542    (relative sequence number)
    Next sequence number: 42581    (relative sequence number)
    Acknowledgement number: 78151    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xe9f5 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
```

```
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 488
        Time from request: 0.006537000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 252
    Close Response (0x04)
        Word Count (WCT): 0
```

```
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    491 10.462486   192.168.1.106         192.168.1.108         SMB      Trans2
Request, QUERY_FS_INFO, Info Allocation

Frame 491 (140 bytes on wire, 140 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.460138000
    Time delta from previous packet: 0.000615000 seconds
    Time since reference or first frame: 10.462486000 seconds
    Frame Number: 491
    Packet Length: 140 bytes
    Capture Length: 140 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 126
    Identification: 0x5a76 (23158)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bdd [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78151, Ack: 42581, Len: 74
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 78151    (relative sequence number)
    Next sequence number: 78225    (relative sequence number)
    Acknowledgement number: 42581    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
```

```
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xa592 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526523
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 70
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 493
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
```

```
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 253
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 2
        Total Data Count: 0
        Max Parameter Count: 4
        Max Data Count: 18
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 2
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: QUERY_FS_INFO (0x0003)
        Byte Count (BCC): 5
        Padding: 000000
        QUERY_FS_INFO Parameters
            Level of Interest: Info Allocation (0x0001)

No.     Time        Source                Destination           Protocol Info
    492 10.466099   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=42581 Ack=78225 Win=64166 Len=0 TSV=1545526523
TSER=636883965

Frame 492 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.463751000
    Time delta from previous packet: 0.003613000 seconds
    Time since reference or first frame: 10.466099000 seconds
    Frame Number: 492
    Packet Length: 66 bytes
    Capture Length: 66 bytes
```

```
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d73 (40307)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x192a [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 42581, Ack: 78225, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 42581    (relative sequence number)
    Acknowledgement number: 78225    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64166
    Checksum: 0x9f00 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
```

```
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    493 10.468414   192.168.1.108         192.168.1.106         SMB      Trans2
Response, QUERY_FS_INFO

Frame 493 (144 bytes on wire, 144 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.466066000
    Time delta from previous packet: 0.005928000 seconds
    Time since reference or first frame: 10.468414000 seconds
    Frame Number: 493
    Packet Length: 144 bytes
    Capture Length: 144 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 130
    Identification: 0x9d74 (40308)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18db [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 42581, Ack: 78225, Len: 78
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 42581    (relative sequence number)
    Next sequence number: 42659    (relative sequence number)
    Acknowledgement number: 78225    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
```

```
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x7fe7 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 74
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 491
        Time from request: 0.005928000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
```

```
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 253
    Trans2 Response (0x32)
        Subcommand: QUERY_FS_INFO (0x0003)
        Word Count (WCT): 10
        Total Parameter Count: 0
        Total Data Count: 18
        Reserved: 0000
        Parameter Count: 0
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 18
        Data Offset: 56
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 19
        Padding: 00
        QUERY_FS_INFO Data

No.     Time        Source                Destination           Protocol Info
    494 10.468789   192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \._Audio.mov

Frame 494 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.466441000
    Time delta from previous packet: 0.000375000 seconds
    Time since reference or first frame: 10.468789000 seconds
    Frame Number: 494
    Packet Length: 180 bytes
    Capture Length: 180 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x5a77 (23159)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bb4 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78225, Ack: 42659, Len: 114
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 78225    (relative sequence number)
    Next sequence number: 78339    (relative sequence number)
    Acknowledgement number: 42659    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x2af2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526523
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
```

```
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 496
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 254
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Reserved: 00
        File Name Len: 24
        Create Flags: 0x00000000
```

```
        Root FID: 0x00000000
        Access Mask: 0x00020001
        Allocation Size: 0
        File Attributes: 0x00000080
        Share Access: 0x00000007
        Disposition: Open (if file exists open it, else fail) (1)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 27
        File Name: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    495 10.472202   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=42659 Ack=78339 Win=64126 Len=0 TSV=1545526523
TSER=636883965

Frame 495 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.469854000
    Time delta from previous packet: 0.003413000 seconds
    Time since reference or first frame: 10.472202000 seconds
    Frame Number: 495
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d75 (40309)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1928 [correct]
```

```
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 42659, Ack: 78339, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 42659    (relative sequence number)
    Acknowledgement number: 78339    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64126
    Checksum: 0x9e68 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    496 10.474225   192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x317a

Frame 496 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.471877000
    Time delta from previous packet: 0.005436000 seconds
    Time since reference or first frame: 10.474225000 seconds
    Frame Number: 496
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
```

```
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9d76 (40310)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18bc [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 42659, Ack: 78339, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 42659    (relative sequence number)
    Next sequence number: 42766    (relative sequence number)
    Acknowledgement number: 78339    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x15b2 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 103
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 494
        Time from request: 0.005436000 seconds
```

```
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 254
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
        FID: 0x317a
        Create action: The file existed and was opened (1)
        Created: Dec 11, 2006 15:23:30.000000000
        Last Access: Dec 11, 2006 15:23:31.000000000
        Last Write: Dec 11, 2006 15:23:31.000000000
        Change: Dec 11, 2006 15:23:31.000000000
```

```
        File Attributes: 0x00000022
        Allocation Size: 1048576
        End Of File: 82
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    497 10.474427   192.168.1.106         192.168.1.108         SMB      Read
AndX Request, FID: 0x317a, 82 bytes at offset 0

Frame 497 (129 bytes on wire, 129 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.472079000
    Time delta from previous packet: 0.000202000 seconds
    Time since reference or first frame: 10.474427000 seconds
    Frame Number: 497
    Packet Length: 129 bytes
    Capture Length: 129 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 115
    Identification: 0x5a78 (23160)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5be6 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78339, Ack: 42766, Len: 63
    Source port: 51751 (51751)
```

```
    Destination port: netbios-ssn (139)
    Sequence number: 78339    (relative sequence number)
    Next sequence number: 78402    (relative sequence number)
    Acknowledgement number: 42766    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x772b [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526523
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 59
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 499
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
```

```
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 255
    Read AndX Request (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x317a
        Offset: 0
        Max Count Low: 82
        Min Count: 82
        Max Count High (multiply with 64K): 0
        Remaining: 82
        High Offset: 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    498 10.477522   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=42766 Ack=78402 Win=64177 Len=0 TSV=1545526523
TSER=636883965

Frame 498 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.475174000
    Time delta from previous packet: 0.003095000 seconds
    Time since reference or first frame: 10.477522000 seconds
    Frame Number: 498
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
```

```
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d77 (40311)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1926 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 42766, Ack: 78402, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 42766    (relative sequence number)
    Acknowledgement number: 78402    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64177
    Checksum: 0x9d8b [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    499 10.480223   192.168.1.108         192.168.1.106         SMB      Read
AndX Response, FID: 0x317a, 82 bytes
```

```
Frame 499 (211 bytes on wire, 211 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.477875000
    Time delta from previous packet: 0.005796000 seconds
    Time since reference or first frame: 10.480223000 seconds
    Frame Number: 499
    Packet Length: 211 bytes
    Capture Length: 211 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 197
    Identification: 0x9d78 (40312)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1894 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 42766, Ack: 78402, Len: 145
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 42766    (relative sequence number)
    Next sequence number: 42911    (relative sequence number)
    Acknowledgement number: 78402    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
```

```
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x8cf1 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 141
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 497
        Time from request: 0.005796000 seconds
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
```

```
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 255
    Read AndX Response (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x317a
        Remaining: 65535
        Data Compaction Mode: 0
        Reserved: 0000
        Data Length Low: 82
        Data Offset: 59
        Data Length High (multiply with 64K): 0
        Reserved: 000000000000
        Byte Count (BCC): 82
        File Data: 000516070002000000000000000000000000000000000000...

No.     Time        Source                Destination           Protocol Info
    500 10.480406   192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x317a

Frame 500 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.478058000
    Time delta from previous packet: 0.000183000 seconds
    Time since reference or first frame: 10.480406000 seconds
    Frame Number: 500
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
```

```
    Total Length: 97
    Identification: 0x5a79 (23161)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bf7 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78402, Ack: 42911, Len: 45
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 78402    (relative sequence number)
    Next sequence number: 78447    (relative sequence number)
    Acknowledgement number: 42911    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xaa74 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526523
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 502
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
```

```
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 256
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x317a
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    501 10.483553   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=42911 Ack=78447 Win=64195 Len=0 TSV=1545526523
TSER=636883965

Frame 501 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.481205000
    Time delta from previous packet: 0.003147000 seconds
    Time since reference or first frame: 10.483553000 seconds
    Frame Number: 501
```

```
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d79 (40313)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1924 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 42911, Ack: 78447, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 42911    (relative sequence number)
    Acknowledgement number: 78447    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64195
    Checksum: 0x9cbb [correct]
    Options: (12 bytes)
        NOP
```

```
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    502 10.485758   192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 502 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.483410000
    Time delta from previous packet: 0.005352000 seconds
    Time since reference or first frame: 10.485758000 seconds
    Frame Number: 502
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d7a (40314)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18fc [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 42911, Ack: 78447, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 42911    (relative sequence number)
    Next sequence number: 42950    (relative sequence number)
    Acknowledgement number: 78447    (relative ack number)
```

```
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xe35c [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 500
        Time from request: 0.005352000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
```

```
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 256
    Close Response (0x04)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    503 10.486182   192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \._Audio.mov

Frame 503 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.483834000
    Time delta from previous packet: 0.000424000 seconds
    Time since reference or first frame: 10.486182000 seconds
    Frame Number: 503
    Packet Length: 180 bytes
    Capture Length: 180 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x5a7a (23162)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
```

```
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bb1 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78447, Ack: 42950, Len: 114
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 78447    (relative sequence number)
    Next sequence number: 78561    (relative sequence number)
    Acknowledgement number: 42950    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x25f1 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526523
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 505
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
```

```
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 257
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Reserved: 00
        File Name Len: 24
        Create Flags: 0x00000000
        Root FID: 0x00000000
        Access Mask: 0x00020001
        Allocation Size: 0
        File Attributes: 0x00000080
        Share Access: 0x00000007
        Disposition: Open (if file exists open it, else fail) (1)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 27
        File Name: \._Audio.mov
```

```
No.     Time        Source                Destination           Protocol Info
    504 10.489669   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=42950 Ack=78561 Win=64126 Len=0 TSV=1545526523
TSER=636883965

Frame 504 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.487321000
    Time delta from previous packet: 0.003487000 seconds
    Time since reference or first frame: 10.489669000 seconds
    Frame Number: 504
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d7b (40315)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1922 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 42950, Ack: 78561, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 42950    (relative sequence number)
    Acknowledgement number: 78561    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
```

```
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64126
    Checksum: 0x9c67 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    505 10.491901   192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x317b

Frame 505 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.489553000
    Time delta from previous packet: 0.005719000 seconds
    Time since reference or first frame: 10.491901000 seconds
    Frame Number: 505
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9d7c (40316)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
```

```
    Header checksum: 0x18b6 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 42950, Ack: 78561, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 42950    (relative sequence number)
    Next sequence number: 43057    (relative sequence number)
    Acknowledgement number: 78561    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x0fb1 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 103
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 503
        Time from request: 0.005719000 seconds
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
```

```
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 257
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
        FID: 0x317b
        Create action: The file existed and was opened (1)
        Created: Dec 11, 2006 15:23:30.000000000
        Last Access: Dec 11, 2006 15:23:31.000000000
        Last Write: Dec 11, 2006 15:23:31.000000000
        Change: Dec 11, 2006 15:23:31.000000000
        File Attributes: 0x00000022
        Allocation Size: 1048576
        End Of File: 82
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    506 10.492131   192.168.1.106         192.168.1.108         SMB      Read
AndX Request, FID: 0x317b, 82 bytes at offset 0
```

```
Frame 506 (129 bytes on wire, 129 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.489783000
    Time delta from previous packet: 0.000230000 seconds
    Time since reference or first frame: 10.492131000 seconds
    Frame Number: 506
    Packet Length: 129 bytes
    Capture Length: 129 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 115
    Identification: 0x5a7b (23163)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5be3 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78561, Ack: 43057, Len: 63
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 78561    (relative sequence number)
    Next sequence number: 78624    (relative sequence number)
    Acknowledgement number: 43057    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
```

```
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x7229 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526523
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 59
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 508
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
```

```
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 258
    Read AndX Request (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x317b
        Offset: 0
        Max Count Low: 82
        Min Count: 82
        Max Count High (multiply with 64K): 0
        Remaining: 82
        High Offset: 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    507 10.495195   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=43057 Ack=78624 Win=64177 Len=0 TSV=1545526523
TSER=636883965

Frame 507 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.492847000
    Time delta from previous packet: 0.003064000 seconds
    Time since reference or first frame: 10.495195000 seconds
    Frame Number: 507
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d7d (40317)
    Flags: 0x04 (Don't Fragment)
```

```
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1920 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43057, Ack: 78624, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 43057    (relative sequence number)
    Acknowledgement number: 78624    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64177
    Checksum: 0x9b8a [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    508 10.497655   192.168.1.108         192.168.1.106         SMB      Read
AndX Response, FID: 0x317b, 82 bytes

Frame 508 (211 bytes on wire, 211 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.495307000
    Time delta from previous packet: 0.005524000 seconds
    Time since reference or first frame: 10.497655000 seconds
    Frame Number: 508
    Packet Length: 211 bytes
    Capture Length: 211 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
```

```
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 197
    Identification: 0x9d7e (40318)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x188e [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43057, Ack: 78624, Len: 145
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 43057    (relative sequence number)
    Next sequence number: 43202    (relative sequence number)
    Acknowledgement number: 78624    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x87f0 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
```

```
        .... ...0 = Add 0 to length
    Length: 141
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 506
        Time from request: 0.005524000 seconds
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 258
    Read AndX Response (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
```

```
        FID: 0x317b
        Remaining: 65535
        Data Compaction Mode: 0
        Reserved: 0000
        Data Length Low: 82
        Data Offset: 59
        Data Length High (multiply with 64K): 0
        Reserved: 000000000000
        Byte Count (BCC): 82
        File Data: 000516070002000000000000000000000000000000000000...

No.     Time        Source                Destination           Protocol Info
    509 10.497858   192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x317b

Frame 509 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.495510000
    Time delta from previous packet: 0.000203000 seconds
    Time since reference or first frame: 10.497858000 seconds
    Frame Number: 509
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
    Identification: 0x5a7c (23164)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bf4 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
```

```
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78624, Ack: 43202, Len: 45
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 78624    (relative sequence number)
    Next sequence number: 78669    (relative sequence number)
    Acknowledgement number: 43202    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xa572 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526523
    SEQ/ACK analysis
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 511
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
```

```
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 259
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x317b
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    510 10.500896   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=43202 Ack=78669 Win=64195 Len=0 TSV=1545526523
TSER=636883965

Frame 510 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.498548000
    Time delta from previous packet: 0.003038000 seconds
    Time since reference or first frame: 10.500896000 seconds
    Frame Number: 510
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
```

```
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d7f (40319)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x191e [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43202, Ack: 78669, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 43202    (relative sequence number)
    Acknowledgement number: 78669    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64195
    Checksum: 0x9aba [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    511 10.503682   192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 511 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.501334000
    Time delta from previous packet: 0.005824000 seconds
    Time since reference or first frame: 10.503682000 seconds
```

```
    Frame Number: 511
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d80 (40320)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18f6 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43202, Ack: 78669, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 43202    (relative sequence number)
    Next sequence number: 43241    (relative sequence number)
    Acknowledgement number: 78669    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xde5b [correct]
```

```
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526523, tsecr 636883965
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 509
        Time from request: 0.005824000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
```

```
        User ID: 100
        Multiplex ID: 259
    Close Response (0x04)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    512 10.510835   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=78669 Ack=43241 Win=65535 Len=0 TSV=636883965
TSER=1545526523

Frame 512 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:02.508487000
    Time delta from previous packet: 0.007153000 seconds
    Time since reference or first frame: 10.510835000 seconds
    Frame Number: 512
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a7d (23165)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c20 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78669, Ack: 43241, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
```

```
    Sequence number: 78669    (relative sequence number)
    Acknowledgement number: 43241    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x9557 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883965, tsecr 1545526523
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    513 11.629943   00:17:ab:43:fd:35     Broadcast             ARP      Who has
192.168.1.105?  Gratuitous ARP

Frame 513 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:03.627595000
    Time delta from previous packet: 1.126261000 seconds
    Time since reference or first frame: 11.629943000 seconds
    Frame Number: 513
    Packet Length: 60 bytes
    Capture Length: 60 bytes
    Protocols in frame: eth:arp
Ethernet II, Src: 00:17:ab:43:fd:35 (00:17:ab:43:fd:35), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: 00:17:ab:43:fd:35 (00:17:ab:43:fd:35)
    Type: ARP (0x0806)
    Trailer: 000000000000000000000000000000000000
Address Resolution Protocol (request/gratuitous ARP)

No.     Time        Source                Destination           Protocol Info
    514 12.264367   192.168.1.106         192.168.1.108         SMB      Trans2
Request, QUERY_PATH_INFO, Query File Basic Info, Path: \

Frame 514 (148 bytes on wire, 148 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.262019000
    Time delta from previous packet: 1.760685000 seconds
    Time since reference or first frame: 12.264367000 seconds
```

```
    Frame Number: 514
    Packet Length: 148 bytes
    Capture Length: 148 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 134
    Identification: 0x5a7e (23166)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bcd [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78669, Ack: 43241, Len: 82
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 78669    (relative sequence number)
    Next sequence number: 78751    (relative sequence number)
    Acknowledgement number: 43241    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0xfcd9 [correct]
```

```
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883968, tsecr 1545526523
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 78
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 516
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 260
```

```
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 10
        Total Data Count: 0
        Max Parameter Count: 2
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 10
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: QUERY_PATH_INFO (0x0005)
        Byte Count (BCC): 13
        Padding: 000000
        QUERY_PATH_INFO Parameters
            Level of Interest: Query File Basic Info (257)
            Reserved: 00000000
            File Name: \

No.     Time        Source                Destination           Protocol Info
    515 12.267787   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=43241 Ack=78751 Win=64158 Len=0 TSV=1545526526
TSER=636883968

Frame 515 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.265439000
    Time delta from previous packet: 0.003420000 seconds
    Time since reference or first frame: 12.267787000 seconds
    Frame Number: 515
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
```

```
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d81 (40321)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x191c [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43241, Ack: 78751, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 43241    (relative sequence number)
    Acknowledgement number: 78751    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64158
    Checksum: 0x9a60 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526526, tsecr 636883968
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    516 12.270265   192.168.1.108         192.168.1.106         SMB      Trans2
Response, QUERY_PATH_INFO

Frame 516 (166 bytes on wire, 166 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.267917000
    Time delta from previous packet: 0.005898000 seconds
```

```
    Time since reference or first frame: 12.270265000 seconds
    Frame Number: 516
    Packet Length: 166 bytes
    Capture Length: 166 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 152
    Identification: 0x9d82 (40322)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18b7 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43241, Ack: 78751, Len: 100
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 43241    (relative sequence number)
    Next sequence number: 43341    (relative sequence number)
    Acknowledgement number: 78751    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
```

```
    Checksum: 0x61c5 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526526, tsecr 636883968
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 96
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 514
        Time from request: 0.005898000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
```

```
        Process ID: 1
        User ID: 100
        Multiplex ID: 260
    Trans2 Response (0x32)
        Subcommand: QUERY_PATH_INFO (0x0005)
        Word Count (WCT): 10
        Total Parameter Count: 2
        Total Data Count: 36
        Reserved: 0000
        Parameter Count: 2
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 36
        Data Offset: 60
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 41
        Padding: 00
        QUERY_PATH_INFO Parameters
            EA Error offset: 0
        Padding: 0000
        QUERY_PATH_INFO Data

No.     Time        Source                Destination           Protocol Info
    517 12.270344   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=78751 Ack=43341 Win=65535 Len=0 TSV=636883968
TSER=1545526526

Frame 517 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.267996000
    Time delta from previous packet: 0.000079000 seconds
    Time since reference or first frame: 12.270344000 seconds
    Frame Number: 517
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
```

```
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a7f (23167)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c1e [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78751, Ack: 43341, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 78751    (relative sequence number)
    Acknowledgement number: 43341    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x949b [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883968, tsecr 1545526526
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    518 12.271924   192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \._Audio.mov

Frame 518 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.269576000
    Time delta from previous packet: 0.001659000 seconds
    Time since reference or first frame: 12.271924000 seconds
    Frame Number: 518
    Packet Length: 180 bytes
```

```
    Capture Length: 180 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x5a80 (23168)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bab [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78751, Ack: 43341, Len: 114
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 78751    (relative sequence number)
    Next sequence number: 78865    (relative sequence number)
    Acknowledgement number: 43341    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x1f34 [correct]
    Options: (12 bytes)
        NOP
```

```
        NOP
        Time stamp: tsval 636883968, tsecr 1545526526
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 520
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 261
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
```

```
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Reserved: 00
        File Name Len: 24
        Create Flags: 0x00000000
        Root FID: 0x00000000
        Access Mask: 0x00020001
        Allocation Size: 0
        File Attributes: 0x00000080
        Share Access: 0x00000007
        Disposition: Open (if file exists open it, else fail) (1)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 27
        File Name: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    519 12.275280   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=43341 Ack=78865 Win=64126 Len=0 TSV=1545526526
TSER=636883968

Frame 519 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.272932000
    Time delta from previous packet: 0.003356000 seconds
    Time since reference or first frame: 12.275280000 seconds
    Frame Number: 519
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d83 (40323)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
```

```
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x191a [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43341, Ack: 78865, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 43341    (relative sequence number)
    Acknowledgement number: 78865    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64126
    Checksum: 0x99aa [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526526, tsecr 636883968
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    520 12.277253   192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x317c

Frame 520 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.274905000
    Time delta from previous packet: 0.005329000 seconds
    Time since reference or first frame: 12.277253000 seconds
    Frame Number: 520
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
```

```
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9d84 (40324)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18ae [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43341, Ack: 78865, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 43341    (relative sequence number)
    Next sequence number: 43448    (relative sequence number)
    Acknowledgement number: 78865    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xd6c5 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526526, tsecr 636883968
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
```

```
    Length: 103
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 518
        Time from request: 0.005329000 seconds
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 261
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
```

```
        FID: 0x317c
        Create action: The file existed and was opened (1)
        Created: Dec 11, 2006 15:23:30.000000000
        Last Access: Dec 11, 2006 15:23:33.000000000
        Last Write: Dec 11, 2006 15:23:31.000000000
        Change: Dec 11, 2006 15:23:31.000000000
        File Attributes: 0x00000022
        Allocation Size: 1048576
        End Of File: 82
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    521 12.277305   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=78865 Ack=43448 Win=65535 Len=0 TSV=636883968
TSER=1545526526

Frame 521 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.274957000
    Time delta from previous packet: 0.000052000 seconds
    Time since reference or first frame: 12.277305000 seconds
    Frame Number: 521
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a81 (23169)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x5c1c [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78865, Ack: 43448, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 78865    (relative sequence number)
    Acknowledgement number: 43448    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x93be [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883968, tsecr 1545526526
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    522 12.277446   192.168.1.106         192.168.1.108         SMB      Read
AndX Request, FID: 0x317c, 82 bytes at offset 0

Frame 522 (129 bytes on wire, 129 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.275098000
    Time delta from previous packet: 0.000193000 seconds
    Time since reference or first frame: 12.277446000 seconds
    Frame Number: 522
    Packet Length: 129 bytes
    Capture Length: 129 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
```

```
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 115
    Identification: 0x5a82 (23170)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bdc [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78865, Ack: 43448, Len: 63
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 78865    (relative sequence number)
    Next sequence number: 78928    (relative sequence number)
    Acknowledgement number: 43448    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x6b6b [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883968, tsecr 1545526526
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 59
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
```

```
        Response in: 524
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 262
    Read AndX Request (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x317c
        Offset: 0
        Max Count Low: 82
        Min Count: 82
        Max Count High (multiply with 64K): 0
        Remaining: 82
        High Offset: 0
```

```
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    523 12.281871   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=43448 Ack=78928 Win=64177 Len=0 TSV=1545526526
TSER=636883968

Frame 523 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.279523000
    Time delta from previous packet: 0.004425000 seconds
    Time since reference or first frame: 12.281871000 seconds
    Frame Number: 523
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d85 (40325)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1918 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43448, Ack: 78928, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 43448    (relative sequence number)
    Acknowledgement number: 78928    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
```

```
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64177
    Checksum: 0x98cd [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526526, tsecr 636883968
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    524 12.284531   192.168.1.108         192.168.1.106         SMB      Read
AndX Response, FID: 0x317c, 82 bytes

Frame 524 (211 bytes on wire, 211 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.282183000
    Time delta from previous packet: 0.007085000 seconds
    Time since reference or first frame: 12.284531000 seconds
    Frame Number: 524
    Packet Length: 211 bytes
    Capture Length: 211 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 197
    Identification: 0x9d86 (40326)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
```

```
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1886 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43448, Ack: 78928, Len: 145
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 43448    (relative sequence number)
    Next sequence number: 43593    (relative sequence number)
    Acknowledgement number: 78928    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x8133 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526526, tsecr 636883968
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 141
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 522
        Time from request: 0.007085000 seconds
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
```

```
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 262
    Read AndX Response (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x317c
        Remaining: 65535
        Data Compaction Mode: 0
        Reserved: 0000
        Data Length Low: 82
        Data Offset: 59
        Data Length High (multiply with 64K): 0
        Reserved: 000000000000
        Byte Count (BCC): 82
        File Data: 000516070002000000000000000000000000000000000000...

No.     Time        Source                Destination           Protocol Info
    525 12.284619   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=78928 Ack=43593 Win=65535 Len=0 TSV=636883968
TSER=1545526526
```

```
Frame 525 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.282271000
    Time delta from previous packet: 0.000088000 seconds
    Time since reference or first frame: 12.284619000 seconds
    Frame Number: 525
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a83 (23171)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c1a [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78928, Ack: 43593, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 78928    (relative sequence number)
    Acknowledgement number: 43593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
```

```
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x92ee [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883968, tsecr 1545526526
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    526 12.284823   192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x317c

Frame 526 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.282475000
    Time delta from previous packet: 0.000292000 seconds
    Time since reference or first frame: 12.284823000 seconds
    Frame Number: 526
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
    Identification: 0x5a84 (23172)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bec [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78928, Ack: 43593, Len: 45
```

```
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 78928    (relative sequence number)
    Next sequence number: 78973    (relative sequence number)
    Acknowledgement number: 43593    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x9eb4 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883968, tsecr 1545526526
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 528
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
```

```
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 263
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x317c
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    527 12.289295   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=43593 Ack=78973 Win=64195 Len=0 TSV=1545526526
TSER=636883968

Frame 527 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.286947000
    Time delta from previous packet: 0.004472000 seconds
    Time since reference or first frame: 12.289295000 seconds
    Frame Number: 527
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
```

```
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d87 (40327)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1916 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43593, Ack: 78973, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 43593    (relative sequence number)
    Acknowledgement number: 78973    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64195
    Checksum: 0x97fd [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526526, tsecr 636883968
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    528 12.291021   192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 528 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.288673000
    Time delta from previous packet: 0.006198000 seconds
    Time since reference or first frame: 12.291021000 seconds
    Frame Number: 528
    Packet Length: 105 bytes
    Capture Length: 105 bytes
```

```
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d88 (40328)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18ee [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43593, Ack: 78973, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 43593    (relative sequence number)
    Next sequence number: 43632    (relative sequence number)
    Acknowledgement number: 78973    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xd79e [correct]
    Options: (12 bytes)
        NOP
        NOP
```

```
        Time stamp: tsval 1545526526, tsecr 636883968
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 526
        Time from request: 0.006198000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 263
    Close Response (0x04)
```

```
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    529 12.291077   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=78973 Ack=43632 Win=65535 Len=0 TSV=636883968
TSER=1545526526

Frame 529 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.288729000
    Time delta from previous packet: 0.000056000 seconds
    Time since reference or first frame: 12.291077000 seconds
    Frame Number: 529
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a85 (23173)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c18 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78973, Ack: 43632, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 78973    (relative sequence number)
    Acknowledgement number: 43632    (relative ack number)
    Header length: 32 bytes
```

```
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x929a [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883968, tsecr 1545526526
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    530 12.293186   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.emacs.d\Contents

Frame 530 (188 bytes on wire, 188 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.290838000
    Time delta from previous packet: 0.002165000 seconds
    Time since reference or first frame: 12.293186000 seconds
    Frame Number: 530
    Packet Length: 188 bytes
    Capture Length: 188 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 174
    Identification: 0x5a86 (23174)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
```

```
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5b9d [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 78973, Ack: 43632, Len: 122
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 78973    (relative sequence number)
    Next sequence number: 79095    (relative sequence number)
    Acknowledgement number: 43632    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5e4d [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883968, tsecr 1545526526
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 118
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 532
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
```

```
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 264
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 50
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 50
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 53
        Padding: 000000
        FIND_FIRST2 Parameters
```

```
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.emacs.d\Contents

No.     Time        Source                Destination           Protocol Info
    531 12.296194   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=43632 Ack=79095 Win=64118 Len=0 TSV=1545526526
TSER=636883968

Frame 531 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.293846000
    Time delta from previous packet: 0.003008000 seconds
    Time since reference or first frame: 12.296194000 seconds
    Frame Number: 531
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d89 (40329)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1914 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43632, Ack: 79095, Len: 0
    Source port: netbios-ssn (139)
```

```
    Destination port: 51751 (51751)
    Sequence number: 43632    (relative sequence number)
    Acknowledgement number: 79095    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64118
    Checksum: 0x97a9 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526526, tsecr 636883968
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    532 12.298506   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Error: STATUS_NO_SUCH_FILE

Frame 532 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.296158000
    Time delta from previous packet: 0.005320000 seconds
    Time since reference or first frame: 12.298506000 seconds
    Frame Number: 532
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d8a (40330)
```

```
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18ec [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43632, Ack: 79095, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 43632    (relative sequence number)
    Next sequence number: 43671    (relative sequence number)
    Acknowledgement number: 79095    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xa7ed [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526526, tsecr 636883968
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 530
        Time from request: 0.005320000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_NO_SUCH_FILE (0xc000000f)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
```

```
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 264
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    533 12.298572   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=79095 Ack=43671 Win=65535 Len=0 TSV=636883968
TSER=1545526526

Frame 533 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.296224000
    Time delta from previous packet: 0.000066000 seconds
    Time since reference or first frame: 12.298572000 seconds
    Frame Number: 533
    Packet Length: 66 bytes
    Capture Length: 66 bytes
```

```
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a87 (23175)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c16 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 79095, Ack: 43671, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 79095    (relative sequence number)
    Acknowledgement number: 43671    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x91f9 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883968, tsecr 1545526526
```

```
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    534 12.298822   192.168.1.106         192.168.1.108         SMB      Trans2
Request, FIND_FIRST2, Pattern: \.emacs.d\Contents

Frame 534 (188 bytes on wire, 188 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.296474000
    Time delta from previous packet: 0.000316000 seconds
    Time since reference or first frame: 12.298822000 seconds
    Frame Number: 534
    Packet Length: 188 bytes
    Capture Length: 188 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 174
    Identification: 0x5a88 (23176)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5b9b [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 79095, Ack: 43671, Len: 122
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 79095    (relative sequence number)
    Next sequence number: 79217    (relative sequence number)
    Acknowledgement number: 43671    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
```

```
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x5cac [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883968, tsecr 1545526526
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 118
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 536
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
```

```
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 265
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 50
        Total Data Count: 0
        Max Parameter Count: 10
        Max Data Count: 16644
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 50
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: FIND_FIRST2 (0x0001)
        Byte Count (BCC): 53
        Padding: 000000
        FIND_FIRST2 Parameters
            Search Attributes: 0x0016
            Search Count: 4
            Flags: 0x0007
            Level of Interest: Find File Both Directory Info (260)
            Storage Type: 0
            Search Pattern: \.emacs.d\Contents

No.     Time        Source                Destination           Protocol Info
    535 12.303076   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=43671 Ack=79217 Win=64118 Len=0 TSV=1545526526
TSER=636883968

Frame 535 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.300728000
```

```
    Time delta from previous packet: 0.004254000 seconds
    Time since reference or first frame: 12.303076000 seconds
    Frame Number: 535
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d8b (40331)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1912 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43671, Ack: 79217, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 43671    (relative sequence number)
    Acknowledgement number: 79217    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64118
```

```
    Checksum: 0x9708 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526526, tsecr 636883968
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    536 12.304800   192.168.1.108         192.168.1.106         SMB      Trans2
Response, FIND_FIRST2, Error: STATUS_NO_SUCH_FILE

Frame 536 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.302452000
    Time delta from previous packet: 0.005978000 seconds
    Time since reference or first frame: 12.304800000 seconds
    Frame Number: 536
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d8c (40332)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18ea [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43671, Ack: 79217, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
```

```
    Sequence number: 43671    (relative sequence number)
    Next sequence number: 43710    (relative sequence number)
    Acknowledgement number: 79217    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xa64c [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526526, tsecr 636883968
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 534
        Time from request: 0.005978000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_NO_SUCH_FILE (0xc000000f)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
```

```
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 265
    Trans2 Response (0x32)
        Subcommand: FIND_FIRST2 (0x0001)
        Word Count (WCT): 0
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    537 12.304840   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=79217 Ack=43710 Win=65535 Len=0 TSV=636883968
TSER=1545526526

Frame 537 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.302492000
    Time delta from previous packet: 0.000040000 seconds
    Time since reference or first frame: 12.304840000 seconds
    Frame Number: 537
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
```

```
    Total Length: 52
    Identification: 0x5a89 (23177)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c14 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 79217, Ack: 43710, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 79217    (relative sequence number)
    Acknowledgement number: 43710    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x9158 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883968, tsecr 1545526526
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    538 12.306096   192.168.1.106         192.168.1.108         SMB      NT
Create AndX Request, Path: \._Audio.mov

Frame 538 (180 bytes on wire, 180 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.303748000
    Time delta from previous packet: 0.001296000 seconds
    Time since reference or first frame: 12.306096000 seconds
    Frame Number: 538
    Packet Length: 180 bytes
    Capture Length: 180 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
```

```
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 166
    Identification: 0x5a8a (23178)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5ba1 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 79217, Ack: 43710, Len: 114
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 79217    (relative sequence number)
    Next sequence number: 79331    (relative sequence number)
    Acknowledgement number: 43710    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x16f1 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883968, tsecr 1545526526
```

```
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 110
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 540
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 266
    NT Create AndX Request (0xa2)
        Word Count (WCT): 24
        AndXCommand: No further commands (0xff)
        Reserved: 00
```

```
        AndXOffset: 0
        Reserved: 00
        File Name Len: 24
        Create Flags: 0x00000000
        Root FID: 0x00000000
        Access Mask: 0x00020001
        Allocation Size: 0
        File Attributes: 0x00000080
        Share Access: 0x00000007
        Disposition: Open (if file exists open it, else fail) (1)
        Create Options: 0x00000000
        Impersonation: Impersonation (2)
        Security Flags: 0x00
        Byte Count (BCC): 27
        File Name: \._Audio.mov

No.     Time        Source                Destination           Protocol Info
    539 12.309852   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=43710 Ack=79331 Win=64126 Len=0 TSV=1545526526
TSER=636883968

Frame 539 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.307504000
    Time delta from previous packet: 0.003756000 seconds
    Time since reference or first frame: 12.309852000 seconds
    Frame Number: 539
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d8d (40333)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
```

```
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1910 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43710, Ack: 79331, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 43710    (relative sequence number)
    Acknowledgement number: 79331    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64126
    Checksum: 0x9667 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526526, tsecr 636883968
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    540 12.312249   192.168.1.108         192.168.1.106         SMB      NT
Create AndX Response, FID: 0x317d

Frame 540 (173 bytes on wire, 173 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.309901000
    Time delta from previous packet: 0.006153000 seconds
    Time since reference or first frame: 12.312249000 seconds
    Frame Number: 540
    Packet Length: 173 bytes
    Capture Length: 173 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 159
    Identification: 0x9d8e (40334)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18a4 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43710, Ack: 79331, Len: 107
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 43710    (relative sequence number)
    Next sequence number: 43817    (relative sequence number)
    Acknowledgement number: 79331    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xcd82 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526526, tsecr 636883968
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 103
```

```
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 538
        Time from request: 0.006153000 seconds
        SMB Command: NT Create AndX (0xa2)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 266
    NT Create AndX Response (0xa2)
        Word Count (WCT): 34
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        Oplock level: No oplock granted (0)
        FID: 0x317d
```

```
        Create action: The file existed and was opened (1)
        Created: Dec 11, 2006 15:23:30.000000000
        Last Access: Dec 11, 2006 15:23:33.000000000
        Last Write: Dec 11, 2006 15:23:31.000000000
        Change: Dec 11, 2006 15:23:31.000000000
        File Attributes: 0x00000022
        Allocation Size: 1048576
        End Of File: 82
        File Type: Disk file or directory (0)
        IPC State: 0x0000
        Is Directory: This is NOT a directory (0)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    541 12.312295   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=79331 Ack=43817 Win=65535 Len=0 TSV=636883968
TSER=1545526526

Frame 541 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.309947000
    Time delta from previous packet: 0.000046000 seconds
    Time since reference or first frame: 12.312295000 seconds
    Frame Number: 541
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a8b (23179)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
```

```
    Header checksum: 0x5c12 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 79331, Ack: 43817, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 79331    (relative sequence number)
    Acknowledgement number: 43817    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x907b [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883968, tsecr 1545526526
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    542 12.312449   192.168.1.106         192.168.1.108         SMB      Read
AndX Request, FID: 0x317d, 82 bytes at offset 0

Frame 542 (129 bytes on wire, 129 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.310101000
    Time delta from previous packet: 0.000200000 seconds
    Time since reference or first frame: 12.312449000 seconds
    Frame Number: 542
    Packet Length: 129 bytes
    Capture Length: 129 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
```

```
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 115
    Identification: 0x5a8c (23180)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bd2 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 79331, Ack: 43817, Len: 63
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 79331    (relative sequence number)
    Next sequence number: 79394    (relative sequence number)
    Acknowledgement number: 43817    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x6327 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883968, tsecr 1545526526
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 59
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 544
```

```
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 267
    Read AndX Request (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x317d
        Offset: 0
        Max Count Low: 82
        Min Count: 82
        Max Count High (multiply with 64K): 0
        Remaining: 82
        High Offset: 0
        Byte Count (BCC): 0
```

```
No.     Time        Source                Destination           Protocol Info
    543 12.317702   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=43817 Ack=79394 Win=64177 Len=0 TSV=1545526526
TSER=636883968

Frame 543 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.315354000
    Time delta from previous packet: 0.005253000 seconds
    Time since reference or first frame: 12.317702000 seconds
    Frame Number: 543
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d8f (40335)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x190e [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43817, Ack: 79394, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 43817    (relative sequence number)
    Acknowledgement number: 79394    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
```

```
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64177
    Checksum: 0x958a [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526526, tsecr 636883968
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    544 12.319867   192.168.1.108         192.168.1.106         SMB      Read
AndX Response, FID: 0x317d, 82 bytes

Frame 544 (211 bytes on wire, 211 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.317519000
    Time delta from previous packet: 0.007418000 seconds
    Time since reference or first frame: 12.319867000 seconds
    Frame Number: 544
    Packet Length: 211 bytes
    Capture Length: 211 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 197
    Identification: 0x9d90 (40336)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x187c [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43817, Ack: 79394, Len: 145
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 43817    (relative sequence number)
    Next sequence number: 43962    (relative sequence number)
    Acknowledgement number: 79394    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x78f0 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526526, tsecr 636883968
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 141
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 542
        Time from request: 0.007418000 seconds
        SMB Command: Read AndX (0x2e)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
```

```
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 267
    Read AndX Response (0x2e)
        Word Count (WCT): 12
        AndXCommand: No further commands (0xff)
        Reserved: 00
        AndXOffset: 0
        FID: 0x317d
        Remaining: 65535
        Data Compaction Mode: 0
        Reserved: 0000
        Data Length Low: 82
        Data Offset: 59
        Data Length High (multiply with 64K): 0
        Reserved: 000000000000
        Byte Count (BCC): 82
        File Data: 000516070002000000000000000000000000000000000000...

No.     Time        Source                Destination           Protocol Info
    545 12.319908   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=79394 Ack=43962 Win=65535 Len=0 TSV=636883968
TSER=1545526526

Frame 545 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.317560000
```

```
    Time delta from previous packet: 0.000041000 seconds
    Time since reference or first frame: 12.319908000 seconds
    Frame Number: 545
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a8d (23181)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c10 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 79394, Ack: 43962, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 79394    (relative sequence number)
    Acknowledgement number: 43962    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
```

```
    Checksum: 0x8fab [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883968, tsecr 1545526526
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    546 12.320041   192.168.1.106         192.168.1.108         SMB      Close
Request, FID: 0x317d

Frame 546 (111 bytes on wire, 111 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.317693000
    Time delta from previous packet: 0.000174000 seconds
    Time since reference or first frame: 12.320041000 seconds
    Frame Number: 546
    Packet Length: 111 bytes
    Capture Length: 111 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 97
    Identification: 0x5a8e (23182)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5be2 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 79394, Ack: 43962, Len: 45
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
```

```
    Sequence number: 79394    (relative sequence number)
    Next sequence number: 79439    (relative sequence number)
    Acknowledgement number: 43962    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x9670 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883968, tsecr 1545526526
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 41
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 548
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
```

```
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 268
    Close Request (0x04)
        Word Count (WCT): 3
        FID: 0x317d
        Last Write: No time specified (0xffffffff)
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    547 12.324406   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=43962 Ack=79439 Win=64195 Len=0 TSV=1545526526
TSER=636883968

Frame 547 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.322058000
    Time delta from previous packet: 0.004365000 seconds
    Time since reference or first frame: 12.324406000 seconds
    Frame Number: 547
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
```

```
    Identification: 0x9d91 (40337)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x190c [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43962, Ack: 79439, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 43962    (relative sequence number)
    Acknowledgement number: 79439    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64195
    Checksum: 0x94ba [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526526, tsecr 636883968
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    548 12.326571   192.168.1.108         192.168.1.106         SMB      Close
Response

Frame 548 (105 bytes on wire, 105 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.324223000
    Time delta from previous packet: 0.006530000 seconds
    Time since reference or first frame: 12.326571000 seconds
    Frame Number: 548
    Packet Length: 105 bytes
    Capture Length: 105 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
```

```
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 91
    Identification: 0x9d92 (40338)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18e4 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 43962, Ack: 79439, Len: 39
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 43962    (relative sequence number)
    Next sequence number: 44001    (relative sequence number)
    Acknowledgement number: 79439    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0xcf5b [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526526, tsecr 636883968
```

```
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 35
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 546
        Time from request: 0.006530000 seconds
        SMB Command: Close (0x04)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 268
    Close Response (0x04)
        Word Count (WCT): 0
```

```
        Byte Count (BCC): 0

No.     Time        Source                Destination           Protocol Info
    549 12.326628   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=79439 Ack=44001 Win=65535 Len=0 TSV=636883968
TSER=1545526526

Frame 549 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.324280000
    Time delta from previous packet: 0.000057000 seconds
    Time since reference or first frame: 12.326628000 seconds
    Frame Number: 549
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a8f (23183)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c0e [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 79439, Ack: 44001, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 79439    (relative sequence number)
    Acknowledgement number: 44001    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
```

```
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x8f57 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883968, tsecr 1545526526
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    550 12.329771   192.168.1.106         192.168.1.108         SMB      Trans2
Request, QUERY_FS_INFO, Info Allocation

Frame 550 (140 bytes on wire, 140 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.327423000
    Time delta from previous packet: 0.003200000 seconds
    Time since reference or first frame: 12.329771000 seconds
    Frame Number: 550
    Packet Length: 140 bytes
    Capture Length: 140 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 126
    Identification: 0x5a90 (23184)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
```

```
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bc3 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 79439, Ack: 44001, Len: 74
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 79439    (relative sequence number)
    Next sequence number: 79513    (relative sequence number)
    Acknowledgement number: 44001    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x8af8 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883968, tsecr 1545526526
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 70
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response in: 552
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x08
            0... .... = Request/Response: Message is a request to the server
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
```

```
        Flags2: 0xc001
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .0.. .... = Long Names Used: Path names in request are not
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 269
    Trans2 Request (0x32)
        Word Count (WCT): 15
        Total Parameter Count: 2
        Total Data Count: 0
        Max Parameter Count: 4
        Max Data Count: 18
        Max Setup Count: 0
        Reserved: 00
        Flags: 0x0000
            .... .... .... ..0. = One Way Transaction: Two way transaction
            .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
        Timeout: Return immediately (0)
        Reserved: 0000
        Parameter Count: 2
        Parameter Offset: 68
        Data Count: 0
        Data Offset: 0
        Setup Count: 1
        Reserved: 00
        Subcommand: QUERY_FS_INFO (0x0003)
        Byte Count (BCC): 5
        Padding: 000000
        QUERY_FS_INFO Parameters
            Level of Interest: Info Allocation (0x0001)
```

```
No.     Time        Source                Destination           Protocol Info
    551 12.332663   192.168.1.108         192.168.1.106         TCP
netbios-ssn > 51751 [ACK] Seq=44001 Ack=79513 Win=64166 Len=0 TSV=1545526526
TSER=636883968

Frame 551 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.330315000
    Time delta from previous packet: 0.002892000 seconds
    Time since reference or first frame: 12.332663000 seconds
    Frame Number: 551
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d93 (40339)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x190a [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 44001, Ack: 79513, Len: 0
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 44001    (relative sequence number)
    Acknowledgement number: 79513    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
```

```
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64166
    Checksum: 0x9466 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526526, tsecr 636883968
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    552 12.334958   192.168.1.108         192.168.1.106         SMB      Trans2
Response, QUERY_FS_INFO

Frame 552 (144 bytes on wire, 144 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.332610000
    Time delta from previous packet: 0.005187000 seconds
    Time since reference or first frame: 12.334958000 seconds
    Frame Number: 552
    Packet Length: 144 bytes
    Capture Length: 144 bytes
    Protocols in frame: eth:ip:tcp:nbss:smb
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 130
    Identification: 0x9d94 (40340)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
```

```
    Protocol: TCP (0x06)
    Header checksum: 0x18bb [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: 51751
(51751), Seq: 44001, Ack: 79513, Len: 78
    Source port: netbios-ssn (139)
    Destination port: 51751 (51751)
    Sequence number: 44001    (relative sequence number)
    Next sequence number: 44079    (relative sequence number)
    Acknowledgement number: 79513    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64240
    Checksum: 0x654d [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526526, tsecr 636883968
NetBIOS Session Service
    Message Type: Session message
    Flags: 0x00
        .... ...0 = Add 0 to length
    Length: 74
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        Response to: 550
        Time from request: 0.005187000 seconds
        SMB Command: Trans2 (0x32)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x88
            1... .... = Request/Response: Message is a response to the
client/redirector
            .0.. .... = Notify: Notify client only on open
            ..0. .... = Oplocks: OpLock not requested/granted
            ...0 .... = Canonicalized Pathnames: Pathnames are not canonicalized
            .... 1... = Case Sensitivity: Path names are caseless
            .... ..0. = Receive Buffer Posted: Receive buffer has not been
posted
```

```
            .... ...0 = Lock and Read: Lock&Read, Write&Unlock are not supported
        Flags2: 0xc041
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error
codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if
execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 0... .... .... = Extended Security Negotiation: Extended
security negotiation is not supported
            .... .... .1.. .... = Long Names Used: Path names in request are
long file names
            .... .... .... .0.. = Security Signatures: Security signatures are
not supported
            .... .... .... ..0. = Extended Attributes: Extended attributes are
not supported
            .... .... .... ...1 = Long Names Allowed: Long file names are
allowed in the response
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 1
        Process ID: 1
        User ID: 100
        Multiplex ID: 269
    Trans2 Response (0x32)
        Subcommand: QUERY_FS_INFO (0x0003)
        Word Count (WCT): 10
        Total Parameter Count: 0
        Total Data Count: 18
        Reserved: 0000
        Parameter Count: 0
        Parameter Offset: 56
        Parameter Displacement: 0
        Data Count: 18
        Data Offset: 56
        Data Displacement: 0
        Setup Count: 0
        Reserved: 00
        Byte Count (BCC): 19
        Padding: 00
        QUERY_FS_INFO Data

No.     Time        Source                Destination           Protocol Info
    553 12.335006   192.168.1.106         192.168.1.108         TCP      51751 >
netbios-ssn [ACK] Seq=79513 Ack=44079 Win=65535 Len=0 TSV=636883968
TSER=1545526526
```

```
Frame 553 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:04.332658000
    Time delta from previous packet: 0.000048000 seconds
    Time since reference or first frame: 12.335006000 seconds
    Frame Number: 553
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a91 (23185)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c0c [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51751 (51751), Dst Port: netbios-ssn
(139), Seq: 79513, Ack: 44079, Len: 0
    Source port: 51751 (51751)
    Destination port: netbios-ssn (139)
    Sequence number: 79513    (relative sequence number)
    Acknowledgement number: 44079    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
```

```
        .... ...0 = Fin: Not set
    Window size: 65535
    Checksum: 0x8ebf [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883968, tsecr 1545526526
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    554 14.841870   192.168.1.106         192.168.1.108         DSI      Request
Tickle (70)

Frame 554 (82 bytes on wire, 82 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:06.839522000
    Time delta from previous packet: 2.506912000 seconds
    Time since reference or first frame: 14.841870000 seconds
    Frame Number: 554
    Packet Length: 82 bytes
    Capture Length: 82 bytes
    Protocols in frame: eth:ip:tcp:dsi:data
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 68
    Identification: 0x5a92 (23186)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bfb [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51762 (51762), Dst Port: afpovertcp
(548), Seq: 0, Ack: 0, Len: 16
```

```
    Source port: 51762 (51762)
    Destination port: afpovertcp (548)
    Sequence number: 0    (relative sequence number)
    Next sequence number: 16    (relative sequence number)
    Acknowledgement number: 0    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 49232
    Checksum: 0x0c42 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883973, tsecr 1545526495
Data Stream Interface

No.     Time        Source                Destination           Protocol Info
    555 14.845147   192.168.1.108         192.168.1.106         TCP
afpovertcp > 51762 [ACK] Seq=0 Ack=16 Win=32760 Len=0 TSV=1545526531
TSER=636883973

Frame 555 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:06.842799000
    Time delta from previous packet: 2.510189000 seconds
    Time since reference or first frame: 14.845147000 seconds
    Frame Number: 555
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
```

```
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d95 (40341)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1908 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: afpovertcp (548), Dst Port: 51762
(51762), Seq: 0, Ack: 16, Len: 0
    Source port: afpovertcp (548)
    Destination port: 51762 (51762)
    Sequence number: 0    (relative sequence number)
    Acknowledgement number: 16    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 32760
    Checksum: 0x4cc9 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526531, tsecr 636883973
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    556 16.399326   192.168.1.108         192.168.1.106         DSI      Request
Attention (11)

Frame 556 (84 bytes on wire, 84 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:08.396978000
    Time delta from previous packet: 4.064368000 seconds
    Time since reference or first frame: 16.399326000 seconds
    Frame Number: 556
    Packet Length: 84 bytes
    Capture Length: 84 bytes
```

```
    Protocols in frame: eth:ip:tcp:dsi
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 70
    Identification: 0x9d96 (40342)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x18f5 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: afpovertcp (548), Dst Port: 51762
(51762), Seq: 0, Ack: 16, Len: 18
    Source port: afpovertcp (548)
    Destination port: 51762 (51762)
    Sequence number: 0    (relative sequence number)
    Next sequence number: 18    (relative sequence number)
    Acknowledgement number: 16    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 32768
    Checksum: 0x1c8d [correct]
    Options: (12 bytes)
        NOP
        NOP
```

```
        Time stamp: tsval 1545526535, tsecr 636883973
Data Stream Interface

No.     Time        Source                Destination           Protocol Info
    557 16.399400   192.168.1.106         192.168.1.108         TCP      51762 >
afpovertcp [ACK] Seq=16 Ack=18 Win=49227 Len=0 TSV=636883977 TSER=1545526535

Frame 557 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:08.397052000
    Time delta from previous packet: 4.064442000 seconds
    Time since reference or first frame: 16.399400000 seconds
    Frame Number: 557
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x5a93 (23187)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5c0a [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51762 (51762), Dst Port: afpovertcp
(548), Seq: 16, Ack: 18, Len: 0
    Source port: 51762 (51762)
    Destination port: afpovertcp (548)
    Sequence number: 16    (relative sequence number)
    Acknowledgement number: 18    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
```

```
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 49227
    Checksum: 0x0c5c [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883977, tsecr 1545526535
    SEQ/ACK analysis

No.     Time        Source                Destination           Protocol Info
    558 16.399459   192.168.1.106         192.168.1.108         DSI      Reply
Attention (2816)

Frame 558 (82 bytes on wire, 82 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:08.397111000
    Time delta from previous packet: 4.064501000 seconds
    Time since reference or first frame: 16.399459000 seconds
    Frame Number: 558
    Packet Length: 82 bytes
    Capture Length: 82 bytes
    Protocols in frame: eth:ip:tcp:dsi
Ethernet II, Src: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce), Dst: AppleCom_20:81:e1
(00:30:65:20:81:e1)
    Destination: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Source: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.108
(192.168.1.108)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 68
    Identification: 0x5a94 (23188)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
```

```
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x5bf9 [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.108 (192.168.1.108)
Transmission Control Protocol, Src Port: 51762 (51762), Dst Port: afpovertcp
(548), Seq: 16, Ack: 18, Len: 16
    Source port: 51762 (51762)
    Destination port: afpovertcp (548)
    Sequence number: 16    (relative sequence number)
    Next sequence number: 32    (relative sequence number)
    Acknowledgement number: 18    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 49232
    Checksum: 0x0037 [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 636883977, tsecr 1545526535
Data Stream Interface

No.     Time        Source                Destination           Protocol Info
    559 16.404116   192.168.1.108         192.168.1.106         TCP
afpovertcp > 51762 [ACK] Seq=18 Ack=32 Win=32760 Len=0 TSV=1545526535
TSER=636883977

Frame 559 (66 bytes on wire, 66 bytes captured)
    Arrival Time: Dec 11, 2006 15:21:08.401768000
    Time delta from previous packet: 4.069158000 seconds
    Time since reference or first frame: 16.404116000 seconds
    Frame Number: 559
    Packet Length: 66 bytes
    Capture Length: 66 bytes
    Protocols in frame: eth:ip:tcp
Ethernet II, Src: AppleCom_20:81:e1 (00:30:65:20:81:e1), Dst: 00:17:f2:4b:6e:ce
(00:17:f2:4b:6e:ce)
    Destination: 00:17:f2:4b:6e:ce (00:17:f2:4b:6e:ce)
    Source: AppleCom_20:81:e1 (00:30:65:20:81:e1)
    Type: IP (0x0800)
```

```
Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 192.168.1.106
(192.168.1.106)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 52
    Identification: 0x9d97 (40343)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0x1906 [correct]
    Source: 192.168.1.108 (192.168.1.108)
    Destination: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: afpovertcp (548), Dst Port: 51762
(51762), Seq: 18, Ack: 32, Len: 0
    Source port: afpovertcp (548)
    Destination port: 51762 (51762)
    Sequence number: 18    (relative sequence number)
    Acknowledgement number: 32    (relative ack number)
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 32760
    Checksum: 0x4c9f [correct]
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1545526535, tsecr 636883977
    SEQ/ACK analysis
```