Analysis of *Forensic Discovery*

Chris Williams

October 22, 2010

1 Introduction

Despite being a little dated, which happens very quickly in this industry, "Forensic Discovery", by Dan Farmer and Wietse Venema, is an excellent introduction to both the art and science of forensic analysis. It should be considered a high-level conceptual overview, and one should not expect detailed explanations of specific tools or techniques. While it does occasionally delve into specifics for an example, the examples can be considered light at best. Thus, this book should not be considered a one-stop-shopping experience, but simply the first step of building a solid foundation.

2 Important Sections

The most important concept, which the authors stress very often, is that establishing a timeline of an attack is crucial. The system that they recommend looking at for this is "MACtimes" – referring specifically to a file's *mtime*, *atime* and *ctime* (or the Windows equivalent). There are two big problems with this idea, which the authors point out early on. The first is that such measurements do not provide history data or granularity (and therefore "fade quickly"). The second problem is that MACtimes can be forged very easily. For example, a backdoor might be placed in a system directory and then have its times modified so that it looks like it has been there since the operating system was installed. As a result of these problems, adequate logging remains very important. Now that bulk storage is cheap, it may be advisable to log everything for an extended period of time, at least on high-risk systems.

There is also a strong emphasis on understanding the filesystem, because most attacks will affect non-volatile storage in some way. The focus is on *ext2*, which seems to be an odd choice, given that the book was published in 2005. This was possibly a deliberate choice due to *ext2*'s simplicity, but if that is the case then they should have mentioned this. The authors seem to put way too much stock in the long-outdated technique of hiding data under mount points. It is probably best to read the filesystem chapters in this book and then move on to a more comprehensive text on filesystem forensics.

The next section is on malware and subversion (not the version control system). Again, the book provides a broad overview of malware and rootkits, and another, more comprehensive text should follow. When it comes to technologies like rootkits, techniques become obsolete very quickly, so this high-level, conceptual section is useful for understanding the absolute essentials of rootkit technology.

The final section is on deleted data, recovery, and how long it remains on magnetic storage systems. With an analysis of the magnetic surface of a disk, it is possible to extract previous values of each bit that have been overwritten. Apparently it is very difficult to destroy a magnetic disk such that the data cannot be recovered by "data recovery experts."

3 Conclusion

"Forensic Discovery" is best used as an introductory book with a focus on the concepts. It is generally highly recommended by expert forensic investigators and malware analysts. Anyone interested in computer

forensics should read this book, preferably first. This is particularly true since the authors have made the full text freely available online[1].

[1] http://www.porcupine.org/forensics/forensic-discovery/