Journal of Digital Forensic Practice, 3:64–66, 2010

ISSN: 1556-7281 print / 1556-7346 online
DOI: 10.1080/15567280903463819

Taylor & Francis
Taylor & Francis Group

BOOK REVIEW

Windows Forensic Analysis DVD Toolkit, 2nd edition. By Harlan Carvey

2009, Burlington, MA: Syngress. xxiv + 482 pp. ISBN 13: 978-1-59749-422-9. $69.95.

The first edition of Harlan Carvey's text on Windows forensics quickly became a standard as an example of both a quality professional reference and a source of a font of practical information on the subject. The second edition promises to continue in that tradition. The quality contributions that Carvey makes on many professional listservs is but a harbinger of what can be found in his book, and a valuable text is all but guaranteed given the technical editor (Eoghan Casey) and technical reviewers (Troy Larson, Rob Lee, and Lance Mueller).

The book targets a broad audience of practitioners who might need to examine Windows systems for purposes ranging from intelligence gathering and forensics examination to security administration and incident response. This in no way dilutes the book's effectiveness; this is not a text about the digital forensics process per se but one about methods and tools with which to examine a particular computing platform; indeed, the procedures are pretty much the same regardless of the intended use of the extracted information. To this end, the book is about the process of examining Windows boxes and contains explanations, background information, product examples, and a lot of Perl scripts.

The book contains nine chapters. Each chapter indicates the major topics right at the beginning and contains a summary, high-level overview, and frequently asked questions (FAQ) section at the end. An excellent table of contents and index supplement the book's content.

The first chapter is titled, "Live Response: Collecting Volatile Data." We are no longer in an age where pulling the plug from the back of the machine is the automatic first step of every computer acquisition. This chapter provides a starting point to understand when a live acquisition is warranted and what volatile and nonvolatile information needs to be gathered. Carvey also describes the meaning and relevance of these items so that the reader knows why this information is being collected in the first place. Acquisition tools are introduced at each step of the way, culminating in a section about how to select the proper tool for the task. The chapter concludes with a review of local, remote, and hybrid live system response methodologies (including Carvey's own Forensic Server Project).

The next chapter covers "Live Response: Data Analysis." The collection of information and its subsequent analysis are different processes using different tools–indeed, they may be performed by different people–so it makes sense that they warrant different chapters. Data analysis–or the correlation of the acquired data to actual system events–really requires that the analyst understand the target operating system and processes so that *abnormal* can be distinguished from *normal*. The chapter leads the reader through several example scenarios in order to teach the reader a process of analysis. Regardless of the purpose of the exam, of course, the bottom line is to determine what happened and why.

Chapter 3 moves into "Windows Memory Analysis" and addresses the acquisition and analysis of RAM (one could argue that this topic, like that of live response, could also have been divided into two chapters, but that is a quibble). The first half of the chapter provides a description of tools and methods for acquiring process memory (i.e., all of the physical and virtual memory associated with running processes) or physical memory (i.e., just the contents of RAM). Both software and hardware methods are explored as well as alternative methods for dumping RAM. The

last half of the chapter addresses memory dump analysis. As with live system analysis, memory analysis is an art that requires a good working knowledge of computer science, operating systems, and the basis of how processes are loaded into memory and execute. Tools and methods for analysis are presented, as well as areas of research that are refining this still-evolving field.

Chapter 4, titled "Registry Analysis," is the longest chapter, comprising nearly 20% of the book. The chapter starts with a brief overview of the purpose of the registry, the structure and format of the database, and tools with which to manage and examine the registry contents. The rest of the chapter steps through some of the more important registry keys–those dealing with system information; network applications and connections; user and system activity; removable, mounted, and portable devices; and CD burning–describing their format, contents, examination tools, and interpretation.

"File Analysis" is the title of chapter 5, the primary focus of which is about the many log files that Windows maintains. Detailed coverage is provided about the event logs and log files of various services, as well as tools with which to parse and interpret these files. A slew of additional log files containing many useful timestamps, Recycle Bins, and restore points are also described. File metadata for Word, PDF, and image files; file signature analysis; and Alternate Data Streams are the next major topics. Finally, additional tools are presented detailing how to mount images, detect malware, and perform timeline analysis.

Chapter 6 addresses "Executable File Analysis." This chapter covers both static analysis (i.e., analyzing the file without running the program) and dynamic analysis (i.e., analyzing the file by running the program in a controlled environment). The goal of this chapter is for the reader to understand the characteristics of executable programs in order to properly analyze a suspicious file. The chapter presents tools and methods so that the examiner can gather information about an executable file in order to obtain clues about the file's purpose as a first step in identifying possible malware or other suspicious programs.

The next chapter is titled, "Rootkits and Rootkit Detection." Rootkits are a growing threat and are a particularly pernicious form of malware because they hide themselves and their function from the operating system. The chapter starts with an explanation of how rootkits work in a Windows environment but spends the bulk of the pages on tools for rootkit detection.

"Tying It All Together" is the title of chapter 8. While the first seven chapters step through a logical series of procedural steps, this chapter pulls it all together with seven case studies that help the reader recognize what methods and processes apply in which situations. The case studies are followed by a section that helps the reader organize the examination of Windows systems, including documentation, goals, and a checklist.

The last chapter is titled "Performing Analysis on a Budget" and will resonate with almost all examiners who face real-world financial constraints. The point of this chapter is not really about cost, per se, but about the fact that digital forensics–for any purpose–is about process rather than tools. The fact is that most organizations cannot afford to give all examiners all of the available commercial software that they might like to have. Carvey argues here that maybe such access is not necessary; indeed, a combination of commercial, open source, and homegrown tools–all validated, of course–is the right answer. The chapter discusses many options for documentation, acquisition, searching, and image, file, and network analysis.

Unlike most professional texts, this book is written in a casual, first-person style, as if the author were speaking directly to the reader. This style seems artificial and stilted in some books but it does seem to work with this text because you can almost hear Carvey's voice as you read the book–in fact, if you watch any of the videos on the DVD you really will hear his voice (which makes reading the text even more personal). The DVD contains videos demonstrating the use of some of the tools in addition to source code for the book's Perl scripts, executable Perl files, sample data files, and a lot more goodies.

Indeed, one of the most valuable aspects of the book is the choice of tools. In addition to his own Perl scripts, Carvey's analysis tools of choice are Technology Pathways' ProDiscover and Matthew Shannon's F-Response. It is nice to see a computer forensics book that showcases tools other than EnCase and FTK!

This second edition is a welcome update since the subject platform–Windows–has changed in the few years since the first edition was written. This edition is noticeably different from the first–some chapters, particularly the ones on Windows memory and registry analysis, are significantly longer and more detailed than

before, and the last two chapters in this edition are totally new. The coverage of the subject matter is definitely more up-to-date, describing current operating system issues and current analysis and examination tools. More forensic artifacts are identified. The DVD has been minimally updated; the movies and most of the tools have the same dates as those in the first edition, although there are some new pointers to additional readings and other resources. There is no question that this update provides significant value for the reader.

Like the first edition, this book will be an essential reference for digital forensics examiners and information security incident responders needing to look at Windows systems, written by a true professional in our field. The information, methods, and tools presented in this book will help all of us do our jobs better.

Reviewed by
Gary C. Kessler