SYNGRESS

WINDOWS FORENSIC ANALYSIS

DVD Toolkit | 2E

HARLAN CARVEY

Windows Forensic Analysis DVD Toolkit 2E

Harlan Carvey
Eoghan Casey Technical Editor

PUBLISHED BY
Syngress Publishing, Inc.
Elsevier, Inc.
30 Corporate Drive
Burlington, MA 01803

Windows Forensic Analysis DVD Toolkit 2E

Printed in the United States of America
1 2 3 4 5 6 7 8 9 0

ISBN 13: 978-1-59749-422-9

Publisher: Laura Colantoni
Acquisitions Editor: Angelina Ward
Technical Editor: Eoghan Casey
Developmental Editor: Gary Byrne
Indexer: SPI

Project Manager: Heather Tighe
Page Layout and Art: SPI
Copy Editors: Audrey Doyle and Dan Hays
Cover Designer: Michael Kavish

For information on rights, translations, and bulk sales, contact Matt Pedersen, Director of Corporate Sales, at Syngress Publishing; email m.pedersen@elsevier.com.

Library of Congress Cataloging-in-Publication Data
Application submitted

To Terri and Kylie

Technical Editor

Eoghan Casey is founding partner of cmdLabs, author of the foundational book *Digital Evidence and Computer Crime*, and coauthor of *Malware Forensics*. For over a decade, he has dedicated himself to advancing the practice of incident handling and digital forensics. He helps client organizations handle security breaches and analyzes digital evidence in a wide range of investigations, including network intrusions with an international scope. He has testified in civil and criminal cases, and he has submitted expert reports and prepared trial exhibits for computer forensic and cyber-crime cases.

Eoghan has performed thousands of forensic acquisitions and examinations, including e-mail and file servers, mobile devices, backup tapes, database systems, and network logs. He has performed vulnerability assessments; deployed and maintained intrusion detection systems, firewalls, and public key infrastructures; and developed policies, procedures, and educational programs for a variety of organizations. In addition, he conducts research and teaches graduate students at Johns Hopkins University Information Security Institute, is editor of the *Handbook of Digital Forensics and Investigation*, and is Editor-in-Chief of Elsevier's *International Journal of Digital Investigation*.

Author

Harlan Carvey (CISSP), author of the acclaimed *Windows Forensics and Incident Recovery*, is a computer forensics and incident response consultant based out of the Northern VA/Metro DC area. He currently provides emergency incident response and computer forensic analysis services to clients throughout the U.S. His specialties include focusing specifically on the Windows 2000 and later platforms with regard to incident response, Registry and memory analysis, and post mortem computer forensic analysis. Harlan's background includes positions as a consultant performing vulnerability assessments and penetration tests and as a full-time security engineer. He also has supported federal government agencies with incident response and computer forensic services.

Technical Reviewers

Troy Larson is a Senior Forensic Engineer in Microsoft's Network Security team, where he enjoys analyzing Microsoft's newest technologies in a constant race to keep forensics practice current with Microsoft technology. Troy is a frequent speaker on forensics issues involving Windows and Office, and he is currently focused on developing forensic techniques for Vista and Office 2007. Prior to joining Microsoft's forensics team, Troy served tours of duty with Ernst & Young's national forensics practice and Attenex, Inc. Troy is a member of the Washington State Bar and received his undergraduate and law degrees from the University of California at Berkeley.

Rob Lee is an information security and forensic consultant providing services to Fortune 500 organizations and the U.S. government. Rob has over 13 years' experience in computer forensics, vulnerability discovery, intrusion detection, and incident response. Rob graduated the U.S. Air Force Academy and served in the U.S. Air Force as a founding member of the 609th Information Warfare Squadron, the first U.S. military operational unit focused on information operations. Later, he was a member of the Air Force Office of Special Investigations, where he conducted computer crime investigations and computer forensics. Prior to his current consultation job, he worked on contracts for a variety of government agencies, where he was the technical lead for a vulnerability discovery team, a contractor lead for a cyber forensics branch, and a leader of a security software development team. Rob is also a fellow and forensic curriculum chair for the SANS Institute. Rob has personally trained more than 8,000 forensic and incident response professionals over nine years. Rob also coauthored the bestselling book, *Know Your Enemy*, *2nd Edition*. In addition to working as a security consultant and at the SANS Institute, Rob has just finished his MBA at Georgetown University in Washington, D.C.

Lance Mueller (CISSP, GCIH, GREM, EnCE, CFCE, CCE) is the co-owner of BitSec Forensics, Inc., and he conducts computer forensic investigations worldwide. Additionally, Lance teaches computer forensics to local, state, and federal law enforcement officers worldwide. Lance's background includes 15 years in law enforcement, where he was

assigned to a computer forensic task force performing computer forensic examinations; he also conducted complex intrusion investigations. Lance continues to serve as a senior consultant to the U.S. Department of State, Bureau of Diplomatic Security Office of Africa, South America, and South East Asia consulting with international law enforcement agencies and government institutions so that they can acquire the skills needed to detect, prevent, and investigate incidents related to cyber terrorism and cyber crime.

Contents

Preface

The purpose of this book, as was with the first edition, is to address a need. An issue that many incident responders and computer forensic examiners have seen is that there is an overreliance on what forensic analysis tools purist procedures are telling us, without really understanding where this information is coming from or how it is being created or derived. The "Age of Nintendo Forensics," i.e., of loading an acquired image into a forensic analysis application and pushing a button, is *over*. As analysts and examiners, we can no longer expect to investigate a case in such a manner. Cybercrime has increased in sophistication, and investigators need to understand what artifacts are available on a system, as well as how those artifacts are created and modified. With this level of knowledge, we come to understand that the absence of an artifact is itself an artifact. In addition, more and more presentations and material are available regarding anti-forensics, or techniques used to make forensic analysis more difficult. Not only that, there have been presentations at major conferences that discuss anti-forensic techniques, of using the responder or examiner's training and tools against them. This book is intended to address the need for a more detailed, granular level of understanding. Its purpose is not only to demonstrate what information is available to the investigator on both a live Windows system as well as in an acquired image but also to provide information on how to go about locating additional artifacts that may be of interest, and correlating multiple data sources to build a more complete picture of the incident.

My primary reason for writing this book has been so that I can give back to a community and field of endeavor that has given so much to me. Since I became involved in the information security field over 12 years ago (prior to that, I was in the military and involved in physical and communications security), I've met a lot of great people and done a lot of really interesting things. Over time, people have shared things with me that have been extremely helpful, and some of those things have served as stepping stones into further research. Some of that

research has found its way into presentations I've given at various conferences, and from there, others have asked questions and provided insight and answers that have helped push that research forward. The repeated exchange of information and engagement in discussion have moved both the interest and the level of knowledge forward, advancing the field. This is my attempt to give back, and in doing so, expand the field a little bit more.

This book is intended to address the technical aspects of collecting and analyzing data during both live and postmortem investigations of Windows systems. This book does not cover everything that could possibly be addressed. There is still considerable room for research in several areas, and a great deal of information needs to be catalogued. My hope is that this book will awaken the reader to the possibilities and opportunities that exist within Windows systems for a more comprehensive investigation and analysis.

Intended Audience

This book focuses on a fairly narrow technical area—Windows incident response and forensic analysis—but it's intended for anyone who does, might do, or is thinking about performing forensic analysis of Windows systems. This book will be a useful reference for many, and my hope is that any readers who initially feel that the book is over their heads or beyond their technical reach will use some of the material they find as a starting point and a basis for questions and further study. When I started writing the first edition of this book, it was not intended to be a second or follow-on edition to my first book, *Windows Forensics and Incident Recovery*, published by Addison-Wesley in July, 2004. Rather, my intention was to move away from a more general focus and provide a resource for not only myself but also others working in the computer forensic analysis field. This second edition was written to continue in this vein, particularly in light of the fact that Microsoft keeps developing and releasing new versions of the Windows operating system, each subsequent version with its own unique twists and nuances.

In writing this book, my goal was to provide a resource for forensic analysts, investigators, and incident responders. My hope is to provide not only useful material for those currently performing forensic investigations but also insight to system administrators who have been faced with incident response activities and have been left wondering, "What should I have done?" On that front, my hope is that we can eventually move away from the misconception that wiping the hard drive and reinstalling the operating system from clean media is an acceptable resolution to an incident. Even updating the patches on the system does not address configuration issues, and in many cases, will result in reinfection or the system being compromised all over again.

This book is intended for *anyone* interested in performing incident response and forensic analysis of Windows systems—corporate or government investigators, students or instructors of any of the burgeoning curricula that have sprung up in recent years, law enforcement officers, or corporate consultants (such as myself). My hope is that this book will also serve

as a useful reference for those either developing or attending computer forensic programs at colleges and universities.

Throughout this book, the terms *investigator*, *first responder, examiner*, and *administrator* are used interchangeably. This is due to the fact that in many cases, the same person may be wearing all of these hats. In other cases, the investigator may come into the corporate infrastructure and work very closely with the administrator, even to the point of obtaining an Administrator level account within the domain in order to perform data collection. In some cases, the administrator may escort the investigator or first responder to a compromised system, and the user account may have Administrator privileges on that system. Please don't be confused by the use of the terms, as they are synonymous in most cases.

Reading through this book, you'll likely notice a couple of things. First, there is a heavy reliance on Perl as a scripting language. There's nothing magical about this choice—Perl is simply a very flexible, powerful scripting language that I like to use because I can make changes to the code and run it immediately without having to recompile the program. Speaking of compiling, I should mention that if you're not familiar with Perl and have never used it, you don't have anything to worry about. With only a few exceptions, the Perl scripts presented in the book and provided on the accompanying DVD have been "compiled" into stand-alone Windows executables using Perl2Exe. This will allow you to run the Perl scripts without having to install Perl (the version of Perl used throughout this book is freely available from ActiveState.com) or anything else. Simply extract the necessary files from the location or archive on the DVD and run them. Another useful feature of Perl is that with some care, Perl scripts can be written to be platform independent. Many of the Perl scripts included on the DVD perform data extraction (and to some degree, analysis) from binary files, and where possible, I have tried to make them as platform independent as possible. What this means is that although the Perl script (and the accompanying Windows executable) will run on the Windows platform, the Perl script itself can be run on Linux or even Mac OS X. Many of the Perl scripts on the DVD (although admittedly not all) have been tested and run successfully within the Perl environment on Linux. What this means is that the examiner is not restricted to any particular analysis platform. Some of the scripts will require the installation of additional modules, which can be done via the Perl Package Manager (PPM) application that is part of the ActiveState distribution of Perl, which is available for Windows, Linux, Mac OS X, and a number of other platforms. Another very useful aspect of using Perl is to meet the needs of automation. Many times, I find myself doing the same sorts of things (data extraction, translation of binary data into something human-readable, etc.) over and over again, and like most folks, I'm bound to make mistakes at some point. However, if I can take a task and automate it in Perl, I can write the code once, and not have to be concerned with making a mistake the second, twentieth, or two-hundredth time I perform that same task. It's easy to correct a process if you actually have a process. I find it extremely difficult to correct what I did if I don't know what it was that I did!

Second, you'll notice that the forensic analysis application used throughout this book is ProDiscover Incident Response Edition, from Technology Pathways. Thanks to Chris Brown's generosity, I have worked with ProDiscover since Version 3 (Version 5 was available at the time that the book was being written) and have found the interface to be extremely intuitive and easy to navigate. When it comes to examining images acquired from Windows systems, ProDiscover is an excellent tool to use (albeit not the only one), and it has many useful and powerful features. Chris and Alex Augustin have been extremely responsive to questions and updates, and Ted Augustin (all three of whom are with Technology Pathways) has been an excellent resource when I've met him at conferences and had a chance to speak with him. Not only is ProDiscover itself an excellent analysis platform, but the Incident Response Edition has made great strides into the live response arena, providing an easy and effective means for collecting volatile data. Also, in my opinion, Chris made an excellent decision in choosing Perl as the scripting language for ProDiscover, allowing the investigator to perform functions (e.g., searches, data extraction, a modicum of data analysis, etc.) within the image via Perl "ProScripts." The accompanying DVD contains several ProScripts that I've written and used quite regularly during examinations (please note that although the ProScripts are Perl scripts, they are not "compiled" with Perl2Exe, as the ProScripts must be scripts to be used with ProDiscover).

Another useful and powerful utility that is mentioned in several locations within the book is F-Response. In 2008, Matthew Shannon, through his own efforts, ushered in a new era of incident response and the acquisition of data from live systems. F-Response can be used in three modes, the most powerful of which is the Enterprise Edition (EE). F-Response EE provides a single administrator or consultant with the capability to reach across a data center, across a city, or even between continents to access systems in a read-only mode. Matt has also provided a powerful management console that makes deploying F-Response EE easier than writing this paragraph. Once deployed, F-Response EE provides you with read-only (write operations are buffered and dropped) access not only to the hard drive(s) on the remote system but also to physical memory (or RAM), in a completely tool-agnostic manner. This means that you can use whichever tool you wish to access the resources now available to acquire an image of the hard drive, access physical memory, and so on. You're not restricted to using just one commercial application to do, well, anything.

Organization of this Book

This book is organized into nine chapters following this preface. Those chapters are:

Chapter 1: Live Response: Data Collection

This chapter addresses the basic issues of collecting volatile data from live systems. Because of several factors (an increase in sophistication of cybercrime, increases in storage capacity, etc.),

live response has gained a great deal of interest, and responders are recognizing the need for live response more and more every day. This increase in interest has not been restricted to consultants such as me, either—law enforcement is beginning to see the need for collecting volatile information from live systems in order to support an investigation. This chapter lists tools and methodologies you can use to collect volatile information and presents the most recent incarnation of the Forensic Server Project.

Chapter 2: Live Response: Data Analysis

I've separated data collection and data analysis, as I see them as two separate issues. In many cases, the data that you want to collect doesn't change, as you want to get a snapshot of the activity on the system at a point in time. However, how you go about interpreting that data is what may be important to your case. Also, it's not unusual to approach a scene and find that the initial incident report is only a symptom of what is really happening on the system or that it has nothing to do with the real issue at all. During live response, how you analyze the data you've collected, and what you look for, can depend on whether you're investigating a fraud case, an intrusion, or a malware infection. This chapter presents a framework for correlating and analyzing the data collected during live response in order to develop a cohesive picture of activity on the system and make analysis and identification of the root cause a bit easier and more understandable.

Chapter 3: Windows Memory Analysis

Windows memory analysis is an area of study that has really taken off since its formal introduction to the community during the summer of 2005, and it really grew by leaps and bounds in 2008. In the past, if the contents of physical memory (i.e., RAM) were collected from a live system, they were searched for strings (i.e., potential passwords), IP and e-mail addresses, and then archived. Unfortunately, any information found in this manner had little context. Thanks to research that has been done since the DFRWS 2005 Memory Challenge, methods of obtaining RAM dumps have been investigated, and data within those RAM dumps can be identified and extracted on a much more granular level, even to the point of pulling an executable image out of the dump file. This chapter attempts to provide a snapshot of what tools are available for performing memory collection and analysis, demonstrating what data can be collected (e.g., Registry hives, encrypted passwords, etc.) from memory dumps.

Chapter 4: Registry Analysis

The Windows Registry maintains a veritable plethora of information regarding the state of the system, and in many cases, the Registry itself can be treated like a log file, as the information that it maintains has a time stamp associated with it in some manner. However, because of the nature of how the data is stored, searches for ASCII or even Unicode strings do not reveal some of the most important and useful pieces of information. This chapter

presents the structure of the Registry to the readers so that they'll be able to recognize Registry artifacts in binary data and unallocated space within an acquired image. The chapter then discusses various artifacts (Registry keys and values) at great length, describing their usefulness and value to an investigation, as well as presenting a number of tools for extracting that information from an acquired image. Other important factors discussed in this chapter include differences inherent to various versions of Windows (XP versus Vista, for example), the use of tools such as RegRipper to extract and correlate information from within hive files (including across Windows XP System Restore Points), and how to retrieve deleted Registry keys from unallocated space within hive files.

Chapter 5: File Analysis

Windows systems maintain a number of log files that many examiners simply are not aware of, and those log files often maintain time-stamp information on the entries that are recorded. In addition, there are a number of files on Windows systems that maintain time-stamp information within the files themselves that can be incorporated into your timeline analysis of an event. Many of these time stamps are maintained by the application and are not immediately obvious. Various files, file formats, and file metadata are discussed in detail, and tools are presented for extracting much of the information that is discussed. Chapter 5 in this edition expands greatly on what was available in the first edition, including illustrating WFPCheck, an application to determine if files "protected" by the operating system were modified or infected (note that this application is illustrated, but is *not* provided on the media that accompanies this book).

Chapter 6: Executable File Analysis

Executable files represent a special case when it comes to file analysis. For the most part, executable files follow a known and documented structure, as they need to be launched and run on various versions of Windows. However, malware authors have discovered ways to obfuscate the structure in order to make their malware more difficult (albeit not impossible) to analyze. By understanding the format of these files and what they *should* look like, examiners can go further in their investigations in determining which files are legitimate, in addition to what effect the suspicious files have on a Windows system. Using the techniques and information presented in this chapter, the examiner can determine which files are legitimate, as well as what artifacts to attribute to a particular piece of malware.

Chapter 7: Rootkits and Rootkit Detection

This chapter addresses the topic of rootkits in the hopes of piercing the veil of mystery surrounding this particular type of malware and presenting the administrator, first responder, and forensic analyst (remember, these could all be the same person) with the necessary information to be able to locate and recognize a rootkit. Rootkits are seeing a surge in use, not only

in cybercrime but also in "legitimate" commercial applications. An understanding of rootkits and rootkit detection technologies is paramount for anyone working with Windows systems, and this chapter presents a great deal of the information that an investigator will need. Many times, responders will be unable to quickly locate the source of some unusual behavior, and instead of following a thorough, rigorous investigative approach, will chalk it up to "a rootkit." By presenting this information about rootkits and exposing the "rootkit paradox," my hope is that responders and examiners will have the tools they need to determine truly if there is a rootkit or some sort of rootkit functionality involved in their incident.

Chapter 8: Tying It All Together

It became clear following the release of the first edition of the book that many examiners were taking the information from one chapter, applying it, and then realizing that they were stuck over what to do next. I have seen or heard about this phenomenon from corporate consultants as well as law enforcement examiners. My goal for this chapter is to demonstrate how information from different areas of your examination—the file system, specific files, the Event Logs, and even the Registry—can be correlated and tied together to build a more complete picture, whether you're a law enforcement examiner attempting to disprove the "Trojan defense" or a corporate analyst or consultant attempting to determine if (and when) a system may have been compromised. As such, the chapter reads as a series of case studies or "war stories," I hope that I was able to illustrate, by these examples, how data from various locations within an examination (not just within an acquired image) can be used to corroborate other data and build a thorough examination.

Chapter 9: Performing Analysis on a Budget

Sometimes, full-blown commercial forensic applications simply are not suitable for use in analysis. They may lack some needed functionality or the functionality you need may be far too cumbersome to get to. As such, the solution should not be to spend thousands of dollars on additional commercial applications when a freely available (or low-cost) tool will be more than sufficient. My goal for this chapter is to demonstrate that forensic analysis is about process, not about tools; remember, the Age of Nintendo forensics is over! Understanding where to look for data, and how to extract and interpret that data, allows an examiner to select the appropriate tool for the job. Many times, freeware tools can provide functionality that commercial tools cannot, and commercial tools can provide validation of findings originally derived from those freeware tools.

DVD Contents

The DVD that accompanies this book contains a great deal of useful information and tools. All of the tools provided are grouped into the appropriate directory based on the chapter in which they were presented. The DVD also contains all of the tools that were provided in the first edition of the book, even those replaced by other tools. For example, all of the original

scripts from Chapter 4 of the first edition are still provided on the DVD, even though they've been replaced by the RegRipper framework. In addition, there is a bonus directory containing several tools that were not specifically discussed in any chapter, but I developed them to meet a need that I had and thought that others might find them useful. This directory also contains a subdirectory titled "WFA_articles," which are a series of PDF documents that I developed to cover specific analysis topics. Each of the documents explains one aspect of analysis in detail; for example, one describes different locations within an image where an analyst might find information about the host system's media access control (MAC) address, while another describes the purpose of each ACMru subkey in detail. My intention in writing these articles was to provide a means for distributing training in specific analysis topics; by providing each topic in a PDF document, users can print and read (and annotate) these documents during travel or place them in a directory and search them when needed.

All of the tools available on the DVD are Perl scripts. However, almost all of the Perl scripts have been "compiled" into stand-alone Windows executables for ease of use. The Perl scripts themselves are, for the most part, platform independent and can be run on Windows, Linux, and even Mac OS X (note that there are some exceptions), and providing Windows executables simply makes them easier for those without Perl installed to use. Several of the chapters also contain ProScripts, which are Perl scripts specifically written to be used with the ProDiscover forensic analysis application from Technology Pathways (the current version available is 5.0). These Perl scripts are launched via ProDiscover and are not "compiled."

In addition, several of the chapter directories contain sample files that the reader can use to gain a familiarity with the tools. It's one thing to have a tool or utility and an explanation of its use, but it's quite another thing to actually use that tool to derive information. Having something immediately available to practice with means that readers can try out the tools anywhere they have a laptop, such as on a plane, and not have to wait until they're able to get copies of those files themselves.

Finally, I have included several movie files on the DVD that I use to explain certain topics. In the past, I wrote an appendix to explain the setup and use of the Forensic Server Project, but I've found that listening to podcasts and watching movies can be much more educational than reading something in a book.

— Harlan Carvey

Author's Acknowledgments

First, I'd like to thank God for the many blessings He's given me in my life, for which I am immensely and eternally grateful. My life has been a continuous chain of His wondrous bounty since I accepted Jesus into my heart and my life.

I'd like to thank the true love and light of my life, Terri, and her beautiful daughter, Kylie, for their continued patience and understanding in supporting me while I wrote this second edition (as if the first one wasn't enough!), and what amounted to my fourth book. I know that I've left them both wondering as I've stared off into space, reasoning and turning over phrases in my mind as I attempted to put them down on "paper." It can't be easy for either of these two wonderful women to be living with a nerd, particularly one who enjoys being a nerd as much as I do.

A huge thank-you goes out to Eoghan Casey for agreeing to be the technical editor for this edition of the book and for putting forth the effort to do such a great job. One of the drawbacks of performing analysis or writing a book is that you often find yourself with your head deep down in the weeds, and when you poke your head up to take a look around, you often find yourself off track. At least, that's how things have gone for me, and Eoghan's done a great job of grounding my efforts with this book. My only regret is that there simply wasn't enough time to fully implement all of Eoghan's suggestions, several of which will be included in any future works.

I'd also like to thank a number of other people for their contributions to this effort. Brett Shavers and his son deserve special thanks for setting up RegRipper.net (and creating a logo for the site), as a showcase for RegRipper and its associated tools. Matt Shannon has been an inspiration to me since we met, not only for his ingenuity in producing F-Response but also for his outlook on life, approach to his business, and the insight and advice he's provided me. Aaron Walters is one of those really smart people who never cease to amaze me. He's one of