BOOK REVIEWS

Jigang Liu
Editor
Metropolitan State University
St. Paul, MN 55106
Jigang.Liu@metrostate.edu

If you have any suggestions on books for review, or you would like to write a book review for us, or you have any comments and concerns on the book reviews published on this column, please feel free to send an email to Jigang Liu at Jigang.Liu@metrostate.edu.

BOOK REVIEW

Vacca, J. R. and Rudolph, K. (2011). *System Forensics, Investigation, and Response.* Sudbury, MA: Jones and Bartlett Learning. 339 + xv pages, ISBN: 978-0-7637-9134-6, US$89.95.

Reviewed by Nate Keith, MBA, (natejkeith@gmail.com)

I recently expressed an interest to a respected colleague in finding a way to "give back" to the forensic community. He suggested writing a review for a text he recently received and provide feedback to the community. It is my intent to present an objective analysis of *System Forensics, Investigation, and Response.*

Written by John R. Vacca and K Rudolph, this book is part of the Jones and Bartlett Learning Information Systems Security & Assurance Series. Both Vacca and Rudolph have considerable experience in the information technology field as is demonstrated by the back cover notes:

"John R. Vacca is an information technology consultant and internationally known best-selling author based in Pomeroy, Ohio. Since 1982, he has written 62 books and more than 600 articles in the areas of advanced storage, computer security, and aerospace technology.

K Rudolph is a Certified Information Systems Security Professional (CISSP) with a degree from Johns Hopkins University. She is the primary author of the chapter on security awareness from the *Computer Security Handbook,* Vol. 5, and is also the author of the chapter on security awareness in the *Handbook of Information Security* published in 2006 and 2009."

The book consists of fifteen chapters divided into three major sections and includes a list of common abbreviations, a glossary, and a complete index to the text. Also included is an answer key to a set of relevant questions posed at the end of each chapter. A copious list of references rounds out the work.

The first part of the book, "The System Forensics Landscape", consists of four

chapters: "System Forensic Fundamentals", "Overview of Computer Crime", "Challenges of System Forensics", and "Forensic Methods and Labs." The section begins by discussing computer crime (cybercrime) and the genesis of system forensics. The authors consider system forensics to be synonymous with computer forensics, system forensics, electronic discovery, data discovery, etc. and explain that it is essentially the process of examining digital containers for evidence. They go on to describe the functions and responsibilities of a system forensics specialist, who uses forensics, and why. A description of how computers are used in crimes follows along with what constitutes computer crime vs. ordinary crime. Motives, means, and opportunities of and for criminals are covered. Many examples of different types of crime are included as are relevant laws and agencies to report the different crimes to. The challenges of forensics, i.e., collecting evidence, dealing with anti-forensics, and data dynamics are thoroughly discussed. Lastly, the authors talk about forensic methods and considerations for those considering building systems or labs to do forensics. These guidelines differentiate between law enforcement and corporate or private labs and also include a list of common tools.

The second section of the book, "Technical Overview: System Forensics tools, techniques, and Methods", contains eight chapters: "System Forensics Technologies", "Controlling a Forensic Investigation", "Collecting, Seizing, and Protecting Evidence", "Understanding Information-Hiding Techniques", "Recovering Data", "Investigating and Scrutinizing E-mail", "Performing Network Analysis", and "Searching Memory in Real Time with Live System Forensics." This section begins with a very general overview of physical disk structure and where data may be hiding, e.g. various types of slack, the HPA, unallocated space, etc. The text again discusses basic forensic processes and provides another overview of common tools, such as FTK, EnCase, UFED, and Device Seizure. The next chapter, "Controlling a Forensic Investigation" provides a good overview of things that the examiner should be cognizant of when presented with an investigation. The highlights include scene preservation, live vs. dead analysis, data duplication considerations, physical vs. logical analysis, and general steps in examining evidence. A summary of certain legal aspects regarding evidence acquisition discusses the Fourth Amendment and scientific evidence standards such as Frye, Daubert, and the common sense principle.

Chapter 7 in section two is where the real working part of the text begins. A FYI in "Collecting, Seizing, and Protecting Evidence" states that this chapter should be used as a guide only and this is sound advice. This chapter covers only the basics and in generalities of planning evidence collection, steps in collection, and the overall do's and don'ts when acquiring evidence. The chapter also covers recommendations on generating key word search lists, which portions of a drive to deeply evaluate, documentation, physical security of evidence, and creating a timeline. Again, these are all discussed at a relatively high level.

Chapter 8, "Understanding Information-Hiding Techniques", provides a discussion of data hiding techniques that analysts may encounter. There are three short sections covering network packet manipulation, alternate data streams, and rootkits. Then follows a lengthy discussion of steganography: what it is, how it is used, and the tools and techniques to generate, detect, and decrypt steganography content.

"Recovering Data" (Chapter 9) is not so much a how-to of recovering data for forensic analysis as it is a chapter on backing up important data and recovering from failure. In this chapter, the authors focus on the prevention of logical and physical damage to data, some basic recovery techniques, and then the theory and principles around data backup. Key elements such as how to handle failures, planning for the worst, ensuring the availability of resources, and procedure evaluation are briefly discussed.

Chapters 9 and 10 ("Investigating and Scrutinizing E-mail", "Performing Network Analysis") are both fairly short chapters on E-mail tracing and network investigation, respectively. The treatment of E-mail tracing is fairly thorough relative to its length in the book and covers mail servers and clients, E-mail headers, and header interpretation. The authors provide a guide to tracing the headers (and thus origins) of a message, replete with examples. Spoofing and re-mailing are also addressed.

The E-mail topic provides segue into the subsequent chapter on network analysis, which, as with much of the rest of the book, is still at a very high level. The authors present a basic overview of networks, protocols, and types of network attacks. Using log files in investigations and as evidence is addressed. The subsection on collecting router evidence includes a set of router commands recommended for use during an investigation, although one wonders at the applicability of these same commands across all router vendors. There is also a subsection on network sniffing that is primarily a list of tools and suppliers of collection and analysis tools.

The last chapter in the book's second section is "Searching Memory in Real Time with Live System Forensics." It contains a robust review of why live analysis should be considered, live vs. dead analysis, and the pros and cons of live analysis. The authors provide a primer on basic memory structure in a segmented environment in non-technical terms to address data consistency in live collection. This includes basic memory architecture and the code, data, stack, and heap segments. The text also includes an outline of tools that can be used for examining memory and even provides two open-source examples that will aid in performing a memory dump and its subsequent analysis.

The final section of the book is "Incident Response, Future Directions, and Resources." This section provides an overview of incident response and a fairly comprehensive take on the steps one should be thinking about before, during, and after an incident. The text describes a proactive prevention approach that

highlights steps like establishing and enforcing policies, training end users and IT personnel, monitoring traffic, and establishing baselines. Knowing that an incident is a will-happen and not an if-happen event, the authors provide recommendations for assembling an incident response team, establishing roles for team members, defining a response plan, and assessing, communicating, and containing an incident. Once the attack is contained, the authors further make recommendations for incident evaluation (determining how serious it was), recovery (getting things back on-line), and documentation/review (identifying costs of the incident and lessons learned). This section also provides the authors' view on trends in hardware, software, and computing models, including cloud computing. The legal environment, both current and future trends, is also addressed, as is the probable requirement for examiner licensure at some point in the future. The final chapter provides an extensive list of software, vendors, professional groups, and organizations involved in system forensics to at least some extent.

This book tends to be somewhat "feast or famine." It is an acceptable text for someone wanting a general overview of system forensics, but it is not in any way a how-to book on digital forensics. It does some things well, but many things not so well.

For example, the first section does a decent job of providing an overview of cybercrime, system forensics, legal considerations, forensic methods, and considerations in putting a lab together, even while many of the topics are highly simplified. (The authors do appear to lump digital forensics, e-discovery, data recovery, data discovery, etc. together as synonyms. I find this to be an incorrect oversimplification. Each of these share similarities but are not the same.)

However, the second section and "meat" of the text is not nearly thorough enough. For example, there is virtually no discussion of message digests, and only real reference to one is an obscure comment about a 32-bit CRC used by law enforcement since 1989. This is a gross omission.

Furthermore, there is little treatment of write-blockers, rootkits, and cryptography while steganography is given 12 ½ pages. The one small subsection on write-blockers is in Chapter 12 ("Searching Memory in Real Time with Live System Forensics"). How one is to go about attaching a write-blocker to a live system is not elaborated upon.

Chapter 9, "Data Recovery", would be better left to what system forensic analysts consider data recovery is: getting back data from physical devices or images and not learning how to write policies and rotate backups. There is no real discussion in the book of file systems at even a basic level. The text still references RAM slack as containing data from memory (and as a valuable resource for searching), although Windows systems reportedly have not used this method of slack filling for many years. (One could argue that other operating systems might, but the overall bias of the book is to Microsoft Windows operating systems.)

I do appreciate the portions of the text discussing incident response, trends, and resources. These are well documented and provide generous food for thought. The resources throughout the book and in the final section are well documented. My only concern with some of the references to software and vendors throughout the book is that there appears to be a bias to certain vendors, such as Guidance Software and NTI.

I do not believe the target audience of this book can be to students who are embarking on a forensics education, at least as a primary text. It seems as if the importance and treatment of some topics is not aligned with what one would expect out of a forensics investigation and response book. It is best suited for those individuals who want an overview of what the authors describe as system forensics and are not concerned with any how-to's or comprehensive understanding.

Nate Keith is a Digital Forensic Analyst and holds Bachelor's degrees in Computer Information Systems and Computer Forensic Sciences and a Master's degree in Business Administration. His research interests include using natural language processing to improve digital forensic examination efficiency, the use of existing tools and off-the-shelf software in image processing to match similar elements in seemingly unrelated images, and the evolution of digital forensics into a true and respected forensic science. He resides in the Twin Cities of Minnesota, USA.