BOOK REVIEWS

Diane Barrett
Book Review Editor
University of Advancing Technology
2625 W. Baseline Rd
Tempe, AZ 85283

If you have any suggestions on books for review, would like to write a book review for us, or have any comments or concerns on the book reviews published in this column, please feel free to send an email to Diane Barrett, the editor for this column, at dm_barrett@msn.com.

BOOK REVIEW

Sammons, John. (2012). *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*. Waltham, MA: Syngress, 208 pages, Print Book ISBN: 9781597496612.
eBook ISBN : 9781597496629. Print: US $29.95. eBook: US$20.97. Includes exercises, case studies, references, and index.

Reviewed by ***Stephen Larson***, ***PhD***. ***Assistant Professor***, ***Slippery Rock University of PA***

The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics is well-named– it really is very basic. And it should be, as the book's intended audience includes entry-level digital forensics professionals and complimentary fields such as law enforcement, legal, and general information security. Though the copyright is 2012, some of the data is from 2009, and there is mention of estimates for 2010.

Author John Sammons is an Assistant Professor at Marshall University, teaching digital forensics, electronic discovery, information security and technology. He is also the founder and Director of the Appalachian Institute of Digital Evidence, a non-profit organization that provides research and training for digital evidence professionals including attorneys, judges, law enforcement and information security practitioners in the private sector. He has extensive industry experience in digital forensics and e-discovery. He is a member of the FBI WV Cybercrime Task Force, an Associate Member of the American Academy of Forensic Sciences, the High Technology Crime Investigation Association, the Southern Criminal Justice Association, and Infragard. Additionally, he routinely provides training for the legal and law enforcement communities in the areas of digital forensics and electronic discovery. In other words, he is quite qualified to write this book.

The technical editor, Jonathan Rajewski, is an Assistant Professor in the Computer & Digital Forensic program at Champlain College who also serves as a member of the Vermont Internet Crimes Task Force serving law enforcement and governmental entities. He is also a Director and Principle Investigator with the Senator Patrick Leahy Center for Digital Investigation. He holds several security and forensic certifications (EnCe, CCE, CISSP, CFE, CSI, SANS Lethal Forensicator).

I am reviewing this book as part of choosing a book for an introduction to computer forensics course. I obtained the e-book, which contains everything the print book has with the exception of the practical exercises. Without the exercises, the page length is 177 pages. To summarize, this book provides a primer for people new to the digital forensics field. This book teaches you how to conduct examinations by discussing what digital forensics is, the methodologies used, key technical concepts and the tools needed to perform examinations. Details on digital forensics for computers, networks, cell phones, GPS, the cloud, and Internet are briefly discussed. It also introduces how to collect digital evidence, document the scene, and how deleted data is recovered. The book focuses entirely on offline systems (e.g., computers and digital devices that are turned off), and does not discuss forensics of running systems.

The book is quite easy to read – the author uses colloquial language and the text flows more like long magazine articles rather than a text book. A nice addition is computer forensic case studies that are

peppered throughout the book. Each chapter starts with a summary of what will be discussed, and ends with a summary of what has been discussed. At the end of each chapter is a list of bibliographic references so the reader can refer to the source of information quoted therein.

In chapter 1, the book defines Forensic Science and Digital Forensics using Zatyko's definition (Zatyko, 2007). This chapter also explains use of digital forensics in criminal investigations, civil litigation, intelligence gathering (concerning terrorism), and administrative matters. An introduction to Locard's Exchange Principle and the scientific method follow, and the chapter finishes by discussing organizations that make significant contributions to the discipline of digital forensics and the role of the forensic examiner in the judicial system.

Chapter 2 introduces key technical concepts. This is quite good for beginners (this is a primer after all) and a nice review for experienced digital forensic examiners. The author introduces and explains memory, storage, file systems, networks, and cloud storage.

Chapter 3 explores different types of computer forensic laboratory setups as well as the hardware and software tools in common use in those labs. The securityof the labs, including secure evidence storage, is discussed, as well as the accreditation and certification of labs. Outside the lab, chapter 4 deals with collecting digital evidence: securing both the scene and the evidence, documenting via photographs and notes, preservation of evidence (cloning hard disk drives, capturing ram, doing live versus dead acquisition), brief discussion on reports.

Chapter 5 discusses deleted data, data in the hibernation file, the registry, the print spool file, recycle bin, metadata, thumbnail cache, most-recently-used, restore points and shadow copy, prefetch, link files, and installed programs. This chapter basically summarizes where "evidence of specific files, actions, or events can be recorded in multiple locations."

AntiForensics is the topic of Chapter 6 and the author reviews several techniques used to hide or destroy digital evidence, such as encryption, password protection, steganography, and data destruction. Methods to overcome anti-forensics are also discussed. The authors also point out that the existence of anti-forensic tools on the computer can be used as evidence in an investigation; why have those tools if you have nothing to hide?

I am glad the authors included a chapter on the legal aspects of digital forensics. Chapter 7 touches on many legal issues such as the Fourth Amendment, searching with and without a warrant and their exceptions, private searches and consent, the Electronic Communications Privacy Act, and so forth. The authors further explain items such as "exigent circumstances" and "plain view doctrine", issues that are of importance in search warrants and evidence discovery. Tips on appropriate wording for effective affidavits that allow full searching and analysis of digital evidence at a lab are given, as well as a discussion on e-discovery and expert testimony.

Internet and email forensics are both discussed in chapter 8. I thought that these could use more coverage than they were given. Concerning the Internet portion, this chapter discusses the process of getting a web page to appear on your computer screen, such as using html tags and xml. It also mentions that the index.dat files contain forensically interesting information, and briefly covers html, http, cookies, temp internet files, internet history, IE artifacts in the registry, and chat clients. On the email topic, the chapter touches on the POP, SMTP, and IMAP protocols, and explains how to read email headers for forensically interesting information. There is a mention of social networking, but nothing on how to discover evidence of its use beyond searching the index.dat or page (swap) files.

Chapter 9 discusses network forensics and how networks have made it easier for hackers to attack networks using attacks such as DDoS, IP Spoofing, MitM, and social engineering. The authors briefly explain social engineering, network types and network protocols to give the reader a quick explanation of how they work as a start to performing forensic tasks. This chapter also introduces firewalls and intrusion detection systems, and discusses network evidence and investigations using items such as log files and sniffers. This chapter also includes more than one case study of insider threats in the form of disgruntled employees.

In this chapter, the authors also mention the phases of incident response as outlined by NIST: preparation, prevention, detection and analysis containment, eradication and recovery, and post

incident activity, as an introduction to incident response.

Mobile device forensics is discussed in chapter 10. The authors introduce cellular communications, CDMA, GSM, and iDEN, and the hurdle pre-paid cell phones provide in forensic investigations. They also briefly discuss cell phone operating systems, cell phone evidence such as abbreviations, and call detail records. The authors emphasize the need to isolate a cell phone from the network using a Faraday bag or arson can in order to get evidence off the cell phone, including a discussion on what information the SIM (subscriber identity module) card can contain. Several cell phone forensic tools are introduced and the authors stress that no one tool can do all that may be required. This chapter also explores GPS devices and what evidence they may contain, and includes a Q&A with Christopher Vance, a Digital Forensic Specialist assisting the West Virginia State Police Digital Forensics Unit, concerning cell phone and mobile forensics.

The final chapter, titled "Looking Ahead: Challenges and Concerns" discusses the "game changing" challenges" that cloud computing a solid state hard drives present. The authors introduce the difficulties cloud computing adds to the forensic process, as files can get deleted and overwritten almost immediately, making recovery nigh unto impossible. The complications solid state drives present is that they reset unused portions of the drive, sometimes automatically, which can make the before and after hash values unequal.

As I mentioned earlier, this book is well named. It is an entry-level primer to digital forensics, and could be used as an introductory book in a beginning computer forensics course. It does not contain enough technical information to make it a useful reference manual, but if one needs a quick review on a certain topic it will suffice.

REFERENCES

Zatyko, K. (2007). Commentary: Defining Digital Forensics. Retrieved February 19, 2011, from: http://www.forensicmag.com/node/128.

REVIEWER'S NOTE

I was disappointed to find the word "imminent" (immediate or will most likely occur) misspelled as "immanent" (present throughout the universe, usually referring to God) in chapter 7, but it was the only spelling error I remember encountering.