BOOK REVIEWS

Gary C. Kessler
Editor
Champlain College
Burlington, VT 05401
gary.kessler@champlain.edu

BOOK REVIEW

Nelson, B., Phillips, A., Enfinger, F., & Steuart, C. (2008). *Guide to computer forensics and investigations* (3rd ed.). New Jersey: Pearson Education, Inc. 693 pages, ISBN: 1-4180-6733-4 (paper).

Reviewed by Keyu Jiang (kjiang@fhsu.edu) and Ruifeng Xuan (r_xuan@scatcat.fhsu.edu), Department of Information Networking and Telecommunications, Fort Hays State University, Hays, KS 67601

Nelson, Phillips, Enfinger, and Steuart's book is about the science of computer forensics and its implications in crime investigations. This book is not intended to provide comprehensive training in computer forensics, but introduce the science the science of computer forensics and its implications in crime investigations. It focused on establishing a solid foundation for those who are new to this field. Nelson, Philips, Enfiger, and Steuart are experienced experts in different areas of computer forensics. Different expertise makes this book could benefit many groups of people at different educational level and industrial background.

As the third edition of the book, it is revised and added with new contents to keep up with the ever-changing field of computer forensics and the development of digital devices. Some of the popular GUI tools have been added. This edition included two new chapters. One deals with PDAs and cell phones as a result of their increased impact on the market. The other one is on professional ethics. All software packages and Web sites have been updated to reflect currency.

Chapter 1 briefly introduces the history of the science of computer forensics with other related disciplines. The process of a crime investigation, including the use of electronic evidence and legal issues in both public and private sectors, is addressed.

Chapter 2 illustrates an overview of a computer crime investigation. The authors emphasize the significance of applying a systematic approach to an investigation. A list of steps of the systemic approach to a case is provided for an investigator to follow. The authors believe it's important to understand the nature of the case, when planning a case. This chapter also presents a detailed,

step by step, demonstration on a forensic tool.

Chapter 3 tackles how to set up a private office and an effective forensics laboratory. This is a very helpful and practical chapter. It not only provides detailed information on forensics lab certification requirements, and the duties of a lab manager and staff, a section about lab budgeting is also included. The authors even provide some examples of floor layouts for computer forensics labs.

Chapter 4 introduces the process of copying data from electronic media, mainly from PCs. Understanding of different operating systems (OSs) are important for an investigator. Several forensic acquisition tools, including remote network acquisition tools are introduced in this chapter, with a detailed demonstration on the software of ProDiscover.

Chapter 5 is aptly titled "Identifying Digital Evidence." The collection of admissible digital evidence requires an investigator's understanding and compliance to the rules and guidelines for digital evidence. The guidelines for processing evidence collected at private-sector incident scenes are different from law enforcement crime scenes. An investigator must review the case to identify its nature, requirements, and plan the investigation. After obtaining the evidence, procedures for storing digital evidence must also be followed.

Chapter 6 focuses on the Windows and DOS operating systems and how data is stored and managed in them. This chapter starts with a general introduction on file systems, the boot sequence of an OS, and the physical structure of disk drives. The authors spend a great length in this chapter to discuss the files systems, namely the FAT and NTFS file systems, used by Microsoft. Other components and their functions, such as the Registry and Virtual Machine of the Windows systems are also explained.

Chapter 7 details current computer forensics tools. Forensics tools featured differently in areas of data acquisition, validation and discrimination, extraction, reconstruction, and reporting. Since there is a variety of computer forensics tools are available on the market today, it's very nice for the authors to include a table of comparison. We can make a better decision on which tool to use in a forensics lab by referring to the table. Some command-line and GUI forensics tools are introduced in detail in this chapter.

Chapter 8 explores the Macintosh and Linux operating systems and their file systems. Detailed introductions on the components of Macintosh's Hierarchical File System (HFS) and UNIX/Linux's files systems are provided. Storage media and hardware, such as CDs and DVD, SCSI, IDE, and SATA drives are also discussed.

Chapter 9 shows the audience how to apply forensics skills and techniques to a computer forensics investigation. The authors make an emphasis on determining the nature of a case and creating an investigative plan first. A

revelation of some computer forensics tools that have built-in validation features is presented. Some common techniques of data-hiding are described to help investigators to uncover potential electronic evidences. Remote acquisition is made possible by using software like the DiskExplorer. A step-by-step demonstration of how to apply this software is discussed.

Chapter 10 addresses the process of recovering graphic files in forensics investigations. Many forensics tools, such as Prodiscoer, EnCase, FTK, X-Ways and many more are available to analyze graphic files. Towards the end of the chapter, the authors introduce the concept of steganography and steganalysis tools that are available to detect hidden data in graphic files.

Chapter 11 is a relatively short chapter that gives the audience an overview of network forensics. Several network tools and bootable Linux CDs that can be used for tracking network traffic, cracking passwords, and more are discussed.

Chapter 12 brings in techniques of tracing, recovering, and analyzing e-mail messages by using forensics tools. Over the years, e-mail systems have become a significant source for evidence in investigations, litigation, and audits of financial statements. It's important to understand how e-mail services operate and where the e-mail files store.

Chapter 13 explains how to obtain information from cell phone and mobile devices. This chapter provides to the audience basic understandings of mobile devices, such as cell phone, PDA, music player and many others. The authors also introduce many techniques and software tools that can be used to acquire data stored in mobile devices.

Chapter 14 addresses guidelines of writing reports on findings in computer forensics investigations. A computer forensics report should be specific, concise, and with the goal of an investigation clearly stated. A thorough discussion of different types of report, the structure, clarity, and the tone of a report is presented.

Chapter 15 subsequently explains the rules of evidence and procedures for testifying in court. A careful preparation is crucial in order to present evidence in a professional demeanor. It's also important to establish communication with your attorney in the preparation phase. This chapter is very thorough and explains well about the whole testimonial process.

Chapter 16 is the final chapter, titled "Ethics for the Expert Witness." When dealing with legal issues, it's essential for computer forensics professionals to maintain at the highest level of ethical ground. A computer forensics investigator can be easily disqualified as an expert by violating court rules or conducting deviations from opinions given in previous cases. It's also crucial to use forensics tools that are reliable.

I've noticed a few outstanding features of the book. This book spends lots of

time on each section and provides detailed information on each concept of computer forensics. It uses similar lengths to explain the Linux system as much as they used when explaining the Windows systems. This book provides some step-by-step demonstrations on how to use the tools, especially for the software of ProDiscover. This is very helpful for the beginners to start with. This book targets a boarder range of audiences from high school students to students at graduate level and current working professionals as well.

However, I do have some quibbles with this book by Nelson et al. First, I wish the authors could include some more real-life cases for discussion. That will help the audience to better understand concepts of computer forensics, and communicate interests of the audience to learn more about the subjects. Secondly, in the last chapter of the book, only some general guidelines and rules for testimony are provided. It doesn't introduce federal or state laws and rules associated with electronic evidence, investigation, and the testimonial process.

Overall, this is a book that's worth-buying. It is well-organized and appropriate for students at different educational level with a solid computer and networking background, or as a professional reference.