BOOK REVIEW

Computer Forensics:
Cybercriminals, Laws, and Evidence

Reviewed by Szde Yu, Department of Criminal Justice, Wichita State University, Wichita, KS, USA

Computer Forensics: Cybercriminals, Laws, and Evidence
Marie-Helen Maras
© 2011 Jones & Bartlett Learning
372 pp.
$93.95
ISBN 978-144-9600-72-3

In her own words, Dr. Marie-Helen Maras wrote this book in an attempt to appeal to the individual who does not have a comprehensive legal or technical background in computer forensics. Indeed, most law enforcement officers and students who are considering a career in computer forensics do not or have not had sufficient training in both computer science and criminal justice. Even those criminologists who claimed specialty in cybercrime usually do not have enough technical knowledge on the application of technology. On the other hand, those who possess computer skills often are not familiar with the legal requirement and the sophistication of evidence integrity. A book that can narrow the gap is much needed in the field of computer forensics.

In totally 13 chapters, the author thoroughly introduces the basics of computer forensics and the cyber environment in which forensic works would be conducted. In chapter 1, the definition and typology of cybercrime are discussed. This is utmost important in that different types of cybercrime may require different skill sets to extract digital evidence, and they also usually generate different types of digital evidence, which entails different legal consideration in the presentation of evidence. In the following chapter, the concept of electronic evidence is introduced and the procedure of computer forensics is also described. The differences between public and private investigations are emphasized, and the rules of evidence within different areas of law are also addressed. In chapter 3, it first explains telecommunications and electronic communications data. Then it briefly but adequately introduces the laws that govern the privacy of personal data. In chapter 4, the author focuses on the legal protection for privacy and how it applies to computers. It discusses searches and seizures of computers and electronic evidence. Chapter 5 talks about cybercrime statutes and the crimes they cover.

The author makes a nice distinction among different types of cybercrime as the law that applies may differ. The crimes covered in the chapter include hacking, website defacement, writing and distributing malicious code, computer intrusions and attacks, cyberterrorism, different types of fraud, intellectual property theft, electronic espionage, cyberharassment, and cyberstalking. In chapter 6, the cyber environment which breeds multiple types of cybercrime (e.g. cyberbullying, identity theft, and online scam) is discussed. Cyberspace can be and should be seen as a social setting that creates or facilitates certain crimes. This is an important aspect that is usually missing in a book that is too technical to address the social environment of crime. Nonetheless, in this book the content also covers technical knowledge. In chapter 7, the tools that can be used to collect evidence are introduced. It also addresses the problems investigators may run into when extracting electronic evidence. Chapter 8 discusses what an investigator should do at a crime scene when digital evidence is involved. The procedure is detailed and the concept of evidentiary integrity is reinforced. Chapter 9 is about how to conduct a corporate investigation. This is very useful because computer forensics indeed is often used in a private domain rather than in criminal justice. This makes the book more appealing to a wider audience. Chapter 10 is about email forensics. Email forensics should be emphasized because email can potentially be used to commit crime or contain crucial evidence. The author craftily uses illustrations to explain the technical concepts involved in email forensics. Chapter 11 is about network forensics. It discusses the purpose of network forensics and the tools that can be useful for such purposes. In this chapter the author avoids bombarding the reader with too many technical terms. Instead, she adeptly talks about the network structure in a way easier to understand for people who lack extensive computer literacy. In chapter 12, mobile phone and PDA investigations are addressed. Considering how prevalent nowadays mobile phones are, it is important to know how computer forensics is applied to portable devices. However the discussion in this chapter is a bit limited as it fails to include some of more advanced and popular devices, such as iPad. The discussion of smartphones is also lacking in how the applications may facilitate crime and hinder forensic works. In chapter 13, what a computer forensics investigator should be prepared to face in a courtroom is also discussed. Evidence is never all about techniques. How it is interpreted and presented is as crucial as how it was collected. This chapter is particularly valuable for practitioners who may possess the skill but lack sufficient knowledge on the legal proceedings.

All in all, as mentioned, this book should be recommended to people who first started studying computer forensics. It is very helpful in establishing a conceptual framework for computer forensics, and it paints a fairly solid idea of what to expect in both the technical and legal aspects. It is finally a book about computer forensics that is suitable for readers who are primarily trained in social sciences but it will also suit technicians well. I particularly appreciate the fact that the author stresses the differences in different types of cybercrime separately in terms of their respective cyber environments, techniques required, evidence generated, and the legislation applied. As in all other fields, there are many subdivisions in computer forensics. You cannot expect to tackle all cybercrimes by knowing just one or two techniques. Understanding the broadness of cybercrime is crucial. In addition to the technical aspects of cybercrime, investigators would be better prepared if they familiarize themselves with the human aspects of cybercrime as well. After all, crime is committed by people. *Computer Forensics: Cybercriminals, Laws, and Evidence* does touch on the "criminal" part, although the main focus is still on the "crime".

Despite my overall appreciation for Dr. Maras' book, I offer some critique. In the book Dr. Maras seems to imply computer forensics is for the investigation of cybercrime. I must point out the fact that in today's society where technology has been embedded in our everyday life, digital evidence can be applicable to any

crime, because electronic devices could be used in any crime that is not normally construed as cybercrime. For example, a murderer could videotape his killing using his cell phone. It is not a cybercrime but the crucial evidence can be stored in the form of digital evidence. Email can be used for communication between criminals. Even though they did not commit crime through email, the email conversation could still serve as evidence. GPS devices also could store important evidence related to a criminal's whereabouts in a case that is not necessarily cybercrime. To think of computer forensics as cybercrime investigation is incomprehensive. Computer forensics ought to be seen as part of forensic science that could be applicable in any crime investigations. Moreover, computer forensics not only generates evidence in a legal sense, but also provides useful leads for investigation. This is to say even if the information extracted from electronic devices is not forensic evidence per se, computer forensics might still be able to offer clues for investigators to look for evidence somewhere else or to profile the suspect. For example, the websites a suspect frequently visits may not prove any crime but such information can help understand the suspect's hobby and interest. If the full utility of computer forensics can be clearly identified, it would be beneficial for the reader to understand the practicality of computer forensics and thus circumvents the misconception that suggests computer forensics is only relevant to cybercrime.

Moreover, in comparison with other books about computer forensics, some weaknesses of this book are noteworthy. Perhaps due to the intent to avoid overwhelming the readers who are not familiar with the operating system of a computer, in this book the discussion on how a computer system would affect the operation of computer forensics is limited. For example, the forensic tools working on a Windows system may not work properly on a mackintosh machine, not to mention other mobile devices. Usually textbooks on computer forensics would stress this but the author only shallowly addresses this in the book. This aspect is deemed important because in my opinion a digital system as to digital investigation is analogous to a physical crime scene in a street crime investigation. The structural environment affects how forensic works can or should proceed effectively. The book may need to emphasize and illustrate this more because it is the fundamentals of computer forensics. In addition, I would recommend more consideration on the "criminal" aspect of computer forensics. As mentioned, in this book the main focus is still on "crime". This is a norm in most books related to computer forensics. However, since Dr. Maras is a criminologist and a former investigator, it is a shame she does not integrate the human element into the discussion of digital evidence more extensively. For instance, how have modern technologies changed a criminal's modus operandi? What are the criminological theories that are most applicable to cybercriminals? Discussions in these aspects would engender a more comprehensive perspective. These aspects are generally lacking in books about computer forensics, but I think they would be especially suitable for this book, given the fact that the book title does emphasize cybercriminals. Finally, another weakness of this book is the failure to take into consideration the transnational nature of digital evidence when discussing the legislation governing computer forensics. With the increasing popularity of cloud storage, much digital evidence is not locally stored. Especially when it involves a foreign nationality, what are the legal and technical implications?

Granted, it is impossible to cover everything in a book and the speed of book writing can never catch up with the advancement of new technologies. Nonetheless, these critiques merely serve as suggestions. It seems the author intends to distinguish her book from other books on computer forensics by simplifying the computer science domain in the discussion. Although this might have been accomplished for good reason, I do believe introducing more of a criminological angle in supplement to the deficiency of computer science would better distinguish this book, considering the author's backgrounds.

In conclusion, I would recommend this book to anyone, including practitioners, academics, and students, who is interested in computer forensics. It addresses not only the technique, but also the law and the criminal background. Dr. Maras' writing style renders great readability and the organization of the book is superb. It can serve as a good textbook for it provides practical exercise, critical thinking questions, and review questions at the end of each chapter, although they are not consistently offered for every chapter. Nonetheless, students would have sufficient knowledge to learn about and some insightful questions for research and brainstorming. For those who are seeking more advanced knowledge and detailed techniques on computer forensics, however, there might be more suitable books available.

REFERENCES

Maras, M. (2012). *Computer forensics: Cybercriminals, laws, and evidence*. Sudbury, MA: Jones & Bartlett Learning.

Szde Yu is a former military investigator from Taiwan in charge of computer security and criminal investigation. He is currently an Assistant Professor of Criminal Justice in the School of Community Affairs at Wichita State University in USA. He used to serve in the College Information Security Oversight Committee at the state university of New York. With educational background in both computer science and criminology, Dr. Yu's research interests involve cybercrime, computer forensics, cyber-psychology, and criminal profiling. He has published journal articles on subjects such as email forensics, digital piracy, and cyber-profiling. In research, he particularly appreciates interdisciplinary collaboration. In teaching, Dr. Yu has taught terrorism, research methods, criminological theory, police problems, and criminal investigations.