International Journal of Cybersecurity Intelligence & Cybercrime

Volume 5 | Issue 3 Article 5

11-1-2022

Book Review: Digital Forensics and Cyber Investigation

Parti et al. (2022). International Journal of Cybersecurity and Intelligence, 5(3), 68-70

Book Review: Digital Forensics and Cyber Investigation

Katalin Parti, Ph.D., Virginia Tech, U.S.A.
Chris Kayser, MCJ, CMT, Cybercrime Analytics Inc., Canada
Catherine Marcum*, Ph.D., Appalachian State University, U.S.A.

Abstract:
After much anticipation, Cognella Academic Publishing is releasing the first edition of *Digital Forensics and Cyber Investigation* by Dr. Kyung-shick Choi, Dr. Sinchul Back, and Marlon Mike Toro-Alvarez. Due to the multifaceted nature of the textbook, we believe it presents benefits for the private sector, academics and law enforcement. Below is a summary of the utility of the textbook for each group.

Benefits of the Text for Private Sector

As cybercrime rates escalate globally, the costs of being victimized by a malicious cyber-event are becoming increasingly impactive on individuals and organizations. The need to become more aware of how our actions can lead to becoming a cyber-victim, and best practices to avoid doing so, can be found in the well-structured chapters within this textbook.

Primarily directed at students wishing to learn more about this area of study, *Digital Forensics & Cyber Investigation* is an easily understandable reference for anyone interested in learning how to become more cyber-safe. Choi, Back, and Toro-Alvarez (2022) provide readers with a comprehensive history of cybercrime, types of cybercrime, how users of technology (UoT) can become cyber-victims, and many tools that can be utilized to investigate cybercrimes using digital forensics.

Many cybercriminals are proficient in the field of computer science, and social engineering – the art of convincing and manipulating recipients of a cyber-intrusion to respond to a bad actor's pursuit to elicit information to use for malicious purposes. This text provides an understanding of techniques used by cybercriminals, aspects of technology that can be used by bad actors, examples of actual cybercrimes and how they were investigated, and an introduction to the intricacies and secretive characteristics of the darkweb. Readers will also learn how cybercriminals are able to remain virtually undetected when committing cybercrimes, and the many challenges related to attempts to identify, charge, and successfully prosecute those responsible for committing cybercrimes.

When completed, readers will have gained a greater understanding of why cybercrime has become the most impactive and lucrative form of crime in history producing significant rewards with minimal risks.

*Corresponding author
Catherine Marcum*, Department of Government and Justice Studies, Appalachian State University, PO Box 32107, Boone, NC, 28608 U.S.A.
Email: marcumcm@appstate.edu

Digital Forensics and Cyber Investigation is a well-documented text that will prove instrumental in helping readers to reduce their risks of becoming a cyber-victim.

Benefits of the Text for Academia

The drastic increase in the frequency of cybercriminality, as well as the methods of performing crime online, have opened up a world of research and career opportunities for students of higher education and technical studies. Younger generations are extremely reliant on technology for their own personal use but are also realizing the career potential in this area. Choi, Back and Toro-Alvarez (2022) provide an extensive review of many facets of cybercriminality methods, but also the forums of investigation for specific types of cybercrime. This multifaceted textbook would serve as a great primary textbook for undergraduate or graduate courses, as well as supplemental text in a variety of courses in criminal justice, computer science, and information technology. Further, the lab exercises provided in the text make it an ideal classroom tool for both faculty and students.

The textbook's structure provides a logical, yet insightful, flow for a 15-week course in a semester of higher education. Notably, the textbook's first chapter addresses computer ethics in cybercrime investigation and practices. The following chapters (2-4) then launch into a thorough investigation of digital evidence and forensics, as well as information technology. Section one of the textbook logically wraps up with chapters 5 and 6 with the examination of mobile forensics and email evidence. The next section of the textbook (Chapters 7-9) explores three specific forms of cybercriminalty: electronic vandalism, phishing and online child sexual exploitation, and investigative techniques on interpersonal youth crimes.

Chapter 10 initiates a discussion of cybersecurity by exploring its history. Next, Chapter 11 provides the reader with a better understanding of geo-localization, followed by a thorough investigation of cybersecurity countermeasures (Chapter 12). One of the most prominent and nefarious forces online, the dark web, is explored in Chapter 13. Lastly, an overview of cyber-intelligence operations is provided, logically followed by the final chapter on cyberterrorism patterns and criminal measures (Chapters 14 and 15, respectively).

Benefits of the Text for Law Enforcement

The merit of a textbook is the diverse curriculum, comprehensive, and plain, intelligible content. Until now, only computer science students have had access to the theoretical and practical knowledge that the authors in this textbook provide in a digestible form for students and professionals in criminal justice, law enforcement, and law. Moreover, due to its easy-to-understand language, the textbook is also suitable for students and professionals who do not have a background in computer science. Since most law enforcement officers (and prosecutors) today are like this, the textbook can fill a gap for them.

The textbook presents the material colorfully and understandably, illustrated with case studies. Case studies reflect on significant cybercrime events. In addition, the story of a fictional villain, Mr. Evil Noodle, runs through the textbook. Students will have to solve various laboratory tasks during the investigation into Mr. Evil Noodle's misdeeds. Mr. Evil Noodle appears in various roles in the textbook, giving readers insight into the investigation through many different cyber offenses. For example, sometimes Mr. Evil Noodle is a

cyberstalker, or a cyberbully, other times, he is a cyberterrorist, a malicious hacker who breaks into computer systems, or an offender who sells illicit material on the darkweb or blackmails victims with ransomware.

By doing hands-on lab exercises, students can gain the necessary knowledge, without which a cybercrime investigator will not stand ground today. Such exercises are, among other things, the hash verification procedure (Chapter 3), reconnaissance on a network (Chapter 4), file encryption and description (Chapter 4), mobile forensics (Chapter 5), email evidence and analysis (Chapter 6), wireless network scanning (Chapter 7), digital evidence collection within an SNS environment (Chapter 8), investigative techniques of interpersonal crimes (Chapter 9), metadata analysis (Chapter 11), detecting someone's geolocation (Chapter 11), utilizing a honeypot and steganography technique (Chapter 12), conducting investigations on the darkweb (Chapter 13), cyber-intelligence operations such as examining DDoS attacks' files (Chapter 14), inspecting server vulnerability by examining a source code (Chapter 14), and website defacement (Chapter 15). These exercises are essential for prospective cybercrime detectives.

In addition, the textbook can be helpful for prosecutors who need an ample level of understanding of cyber investigations and digital forensics for the indictment, preserve evidence integrity, and represent digital evidence in court. The text introduces the reader to digital evidence altogether with the principles of collecting and preserving digital evidence. In addition, the reader learns how to write a search warrant and the features of search and seizure guidelines. Finally, future investigators learn how to secure data integrity and write an actual report about the steps of the investigation and the evidence found.

In addition to understanding cybercrimes on a technical level, the reader learns to think like perpetrators and discern victim vulnerabilities from the section on applied lessons for investigators (Chapter 9). Cyber-situational crime prevention techniques (Chapter 12) provide information on target hardening and system hardening. Finally, the policy recommendations section (Chapter 14) and cyberterrorism, as one of today's most threatening cybercrimes, are worth mentioning. After a comprehensive description of cyberterrorism, the reader can learn about strategic plans (Chapter 15) that can guide police leadership in the area of international cooperation, often required in the case of cybercrime.

Conclusion

It is because of the reasons presented above that we believe this textbook can serve a variety of audiences and not just reserved for academic instruction (although extremely important with only that facet). Choi, Back and Toro-Alvarez bring a magnitude of experience to the proverbial table, only making the contents of this book even more rich with information and value for practitioners, academics and law enforcement. We look forward to seeing it serve our cyber community today and in the future with updated editions.