Book Review

Kanellis, P., Kiountouzis, E., Kolokotronis, N., & Martakos, D. (2006). *Digital Crime and Forensic Science in Cyberspace*. Hershey, PA: Idea Group Publishing, 357 pages, ISBN: 1-59140-873-3 (paper), US$79.95.

Reviewed by Gary C. Kessler

This book, according to the preface, "is intended for those who are interested in a critical overview of what forensic science is, care about privacy issues, and wish to know what constitutes evidence for computer crime." It goes on to say that the specific audiences for which it was written are students in academia and professionals in the industry.

If used carefully, this book does a good job at providing a snapshot of some of the current issues in digital forensics, although perhaps best aimed at information security professionals. It is a collection of 15 chapters written by authors from Greece, Italy, The Netherlands, South Africa, the U.K., and the U.S. The international flavor of the writing is also welcome in the field.

The book is divided into four parts. Section I (53 pages) is titled Cyberspace and Digital Forensics. The two chapters in this section describe network attacks on computers and malware. While these chapters offer a good overview of these topics, neither provides a context for computer forensics, per se, although they are an excellent introduction for information security students and professionals. There is nothing here about computer investigations nor attacks in people, such as cyberstalking, privacy, child sexual exploitation, or any of the other problems commonly seen by computer forensics investigators.

Section II (162 pages) is titled Computer and Network Forensics. Comprising seven chapters, this section makes up nearly half of the book. The very first chapter offers a nice overview of both computer and network forensics processes and tools. The next two chapters also address tools; one provides a glimpse into next-generation forensics tools and the other discusses the all-important topic of tool validation techniques. These are followed by a chapter on network log analysis and correlation of logs to actual events.

The following two chapters address works-in-progress, one on the use of a network-based forensic profiling system for real-time evidence gathering and the other on the use of data mining in criminal investigations. The section wraps up with the longest chapter in the book and one of the better descriptions of steganography and steganalysis that this reviewer has read.

Section III (50 pages) is titled Incident Response and comprises two chapters. The first chapter is devoted to issues surrounding the creation of security policies aimed at preparedness and response to information security incidents. The second chapter describes the relationship between digital forensics and corporate, information technology, and information security governance. This section, however, does not really discuss any specifics about incident response methods, tools, and processes.

Finally, Section IV (73 pages) is titled Cyber Investigation and Training. The first chapter addresses some of the legal issues related to wide-scale digital investigations that cross international boundaries, particularly with respect to EU countries. The second chapter addresses issues related to the design of digital forensics academic curricula. The next chapter ostensibly discusses computer forensics training, although it does a better job on general information security training (why do so many authors mention the CISSP in the context of computer forensics?) and some computer forensics product-specific training; it doesn't actually mention any of the computer forensics training certifications that can be obtained.

The fourth chapter in this section, and the last of the book, is by M. Caloyannides and titled "Digital 'Evidence' is Often Evidence of Nothing." This is an interesting chapter to be in a book like this since Caloyannides has often made the case about the unreliability of digital evidence. While information found on computers does, indeed, need to be interpreted within the larger context of an investigation and a pattern of behavior, this reviewer disagrees that it is as weak as Caloyannides suggests. Nevertheless, hearing from a naysayer is probably a good thing for the reader, as the editors of this volume suggest in the book's foreword.

The writing in this book is of generally high-quality although the titles of some of the chapters are a bit misleading, as mentioned in several places above. The writing has value but my expectations were different than the reality because of the labeling.

While the book provides a snapshot of some aspects of information security and digital forensics, it is far from complete. There is, for example, no mention in the book of cryptography, whole disk encryption, or encrypting operating systems (e.g., Vista) and the impact on computer forensics. There is no mention of forensics on cell phones or other mobile devices, and this is undoubtedly a big part of the future of digital investigations.

All-in-all I liked this book and think that it makes a contribution to the literature. As a compendium, it belongs on the bookshelf next to the proceedings of the Digital Forensics Research Workshop (DFRWS) and IFIP 11.9 International Conference on Digital Forensics. But information security professionals are probably the better audience than digital forensics investigators.

This review appears in **The Journal of Digital Forensics, Security and Law*, 2006, 1(4), 55-57.***