J Forensic Sci, Mar. 2003, Vol. 48, No. 2
Paper ID JFS2002313_482
Published 3 Feb. 2003
Available online at: www.astm.org

BOOK REVIEW

Judith M. Collins[1]

Review of: *Digital Evidence and Computer Crime*

REFERENCE: Eoghan C. Digital evidence and computer crime. New York, NY: Academic Press, 2001, 279 pp.

Hundreds of books have been written on computers and computing, but my search found none that included the topics of cybercrime and computer forensics. Further, most computer-related books are targeted toward audiences knowledgeable about computer technology, and many of these are strictly applied, providing no theoretical basis for interpreting underlying concepts. For the average citizen who has no background in "digital data" and the reader who seeks a conceptual framework for what is written, most texts seem limited and lacking. In *Digital Evidence and Computer Crime,* however, Eoghan Casey (2001) brilliantly articulates technical details in lay terms for a wide audience ranging from those with little or no computer-related experience to knowledgeable experts in the field.

Digital Evidence and Computer Crime is about computers and computer forensics—conducting computer investigations of cybercrimes. The book is guided by theories from computer science, forensic science and the behavioral sciences, and for the beginner, Casey (2001) amazingly translates sophisticated technological issues and concepts into straightforward, easy-to-understand language. For the experienced computer technician, *Digital Evidence and Computer Crime* extends technology into the realm of crime and the disciplines of criminal justice and the behavioral sciences.

In its introduction, *Digital Evidence and Computer Crime* provides the reader with a cognitive map for a fascinating journey into the inner sanctum of World Wide Web. In chapters that consecutively build upon one another, readers first learn about the language of cybercrime and then are shown the "insides" of a computer and how information (digital data) transmitted using a computer can be retrieved from that computer and analyzed.

Using graphic illustrations throughout, Casey (2001) goes on to describe digital evidence on computer networks and on the Internet, and on the mechanisms that link computer networks with one another and with the Internet. Integrated into the chapters are interesting case examples of actual crimes committed at several levels—computer, computer networks, the Internet and their interconnections. One chapter focuses solely on forensic science—the investigation and analysis of digital data, and the chapter on "behavioral evidence analysis" presents the basic elements of forensic analysis, victimology, risk assessment, and crime scene characteristics. Casey's book is comprehensive: A book about crimes without laws would be incomplete. Casey (2001) therefore includes a chapter on "Laws, Jurisdiction, Search and Seizure." Interestingly, the chapter uses actual court case examples to illustrate how old legal precedents can be applied to new (cyber) crimes.

Important features of the book include a summary of computer crime and forensic science resources, and, especially noteworthy, is the CD-ROM containing cases of cybercrimes. The mission is to use information on the crime scene, the victim, and the suspect to solve the crime. The information is in the form of streaming photographs with accompanying textual descriptions; "learning goals" are presented at the beginning of each crime case and "prompts" throughout guide the investigations. Each case concludes with a crime "report" that confirms or disconfirms the crime analyst's solution. The reader-investigator can even exchange information and ideas about the cases and the concepts covered in the text in online discussions with the author and other readers. One only registers to obtain a password.

Reviews of most texts point out the positive as well as potentially negative aspects, and though I searched for I could not uncover any detracting features whatsoever. Only one minor comment is the repeated use of data in the singular form, instead of datum.

In summary, *Digital Evidence and Computer Crime* provides a foundation for understanding computers, computer networks, and the Internet, and describes and illustrates computer forensic investigation and analysis at each of these levels. *Digital Evidence and Computer Crime* contains material useful for novices as well as for computer experts who are interested in digital technology and how it is used to commit old crimes in new ways.

In conclusion, *Digital Evidence and Computer Crime* is written for a broad audience. It can be used as a textbook to guide academic curricula in any discipline and at any level—high school or college, undergraduate or graduate (I used it as the primary text for a criminal justice graduate course). The book also has great potential for courses on professional development, for managers and employees having little computer experience; or, the book may be simply enjoyed as leisure reading for anyone interested in 21st century cyber issues. However, the book should be *required reading* for certain groups of individuals, including defense lawyers, prosecutors, judges, law enforcement officers, security administrators and criminal justice teachers and their students.

[1] Associate Professor of Industrial and Organizational Psychology, School of Criminal Justice, Michigan State University, East Lansing, MI.