Computer Forensics

Evidence Collection and Management

Robert C. Newman

Auerbach Publications
Taylor & Francis Group

Computer Forensics

Evidence Collection and Management

Robert C. Newman

Auerbach Publications
Taylor & Francis Group
Boca Raton New York

Auerbach Publications is an imprint of the
Taylor & Francis Group, an informa business

Auerbach Publications
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Auerbach is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2

International Standard Book Number-10: 0-8493-0561-6 (Hardcover)
International Standard Book Number-13: 978-0-8493-0561-0 (Hardcover)

Library of Congress Cataloging-in-Publication Data

Newman, Robert C.
Computer forensics : evidence, collection, and management / Robert C. Newman. -- 1st ed.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-0-8493-0561-0 (alk. paper)
ISBN-10: 0-8493-0561-6 (alk. paper)
1. Evidence, Expert--United States. 2. Computer crimes--Investigation--United States. I. Title.

KF8961.N49 2007
345.73'0268--dc22 2006031576

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the Auerbach Web site at
http://www.auerbach-publications.com

Computer Forensics

OTHER INFORMATION SECURITY BOOKS FROM AUERBACH

802.1X Port-Based Authentication
Edwin Lyle Brown
ISBN: 1-4200-4464-8

Audit and Trace Log Management: Consolidation and Analysis
Phillip Q. Maier
ISBN: 0-8493-2725-3

The CISO Handbook: A Practical Guide to Securing Your Company
Michael Gentile, Ron Collette and Tom August
ISBN: 0-8493-1952-8

Complete Guide to CISM Certification
Thomas R. Peltier and Justin Peltier
ISBN: 0-849-35356-4

Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI
Debra S. Herrmann
ISBN: 0-8493-5402-1

Computer Forensics: Evidence Collection and Management
Robert C. Newman
ISBN: 0-8493-0561-6

Curing the Patch Management Headache
Felicia M. Nicastro
ISBN: 0-8493-2854-3

Cyber Crime Investigator's Field Guide, Second Edition
Bruce Middleton
ISBN: 0-8493-2768-7

Database and Applications Security: Integrating Information Security and Data Management
Bhavani Thuraisingham
ISBN: 0-8493-2224-3

Guide to Optimal Operational Risk and BASEL II
Ioannis S. Akkizidis and Vivianne Bouchereau
ISBN: 0-8493-3813-1

Information Security: Design, Implementation, Measurement, and Compliance
Timothy P. Layton
ISBN: 0-8493-7087-6

Information Security Architecture: An Integrated Approach to Security in the Organization, Second Edition
Jan Killmeyer
ISBN: 0-8493-1549-2

Information Security Cost Management
Ioana V. Bazavan and Ian Lim
ISBN: 0-8493-9275-6

Information Security Fundamentals
Thomas R. Peltier, Justin Peltier and John A. Blackley
ISBN: 0-8493-1957-9

Information Security Management Handbook, Sixth Edition
Harold F. Tipton and Micki Krause
ISBN: 0-8493-7495-2

Information Security Risk Analysis, Second Edition
Thomas R. Peltier
ISBN: 0-8493-3346-6

Intelligence Support Systems: Technologies for Lawful Intercepts
Paul Hoffmann and Kornel Terplan
ISBN: 0-8493-285-51

Investigations in the Workplace
Eugene F. Ferraro
ISBN: 0-8493-1648-0

Managing an Information Security and Privacy Awareness and Training Program
Rebecca Herold
ISBN: 0-8493-2963-9

Network Security Technologies, Second Edition
Kwok T. Fung
ISBN: 0-8493-3027-0

A Practical Guide to Security Assessments
Sudhanshu Kairab
ISBN: 0-8493-1706-1

Practical Hacking Techniques and Countermeasures
Mark D. Spivey
ISBN: 0-8493-7057-4

Securing Converged IP Networks
Tyson Macaulay
ISBN: 0-8493-7580-0

Security Governance Guidebook with Security Program Metrics on CD-ROM
Fred Cohen
ISBN: 0-8493-8435-4

The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments
Douglas J. Landoll
ISBN: 0-8493-2998-1

Wireless Crime and Forensic Investigation
Gregory Kipper
ISBN: 0-8493-3188-9

AUERBACH PUBLICATIONS
www.auerbach-publications.com
To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401
E-mail: orders@crcpress.com

Preface

Why Is This Book Important?

Every day a new revelation concerning some Internet or cyber-crime is splashed across the television screen. Someone has compromised a corporation's database, threatening the security of the population's financial resources. Some corporate official has "cooked the books," causing employees and investors to lose millions of dollars. Someone has hacked into a computer system and stolen information that can be used in identity theft schemes. Millions of dollars are at stake—those of citizens, the government, and corporations.

On a larger scale, numerous scam and fraud schemes are being directed toward the public, specifically Internet users. A serious issue involves identity theft and identity fraud. Internet criminals are using personal information to steal personal assets from savings and checking accounts. These criminals are using phishing techniques to trick Web users into providing social security numbers, birth dates, and other information that is then used to commit some cyber-crime. Techniques called "dumpster diving," "phishing," and "shoulder surfing" are used to learn confidential personal information.

Numerous crimes are committed using the Internet, computers, and electronic devices. Of particular interest are those crimes relating to child predators and child pornography. Serious crimes such as murder, rape, kidnapping, stalking, drug trafficking, and numerous other felonies are committed using electronic devices. Criminals and cyber-terrorists are using these electronic resources as a tool. Everyone is aware of the use of computing devices and cell phones by terrorist cells to commit mayhem.

The current computer and networking market has been growing at an unbelievable rate and security preparedness has not kept pace with this growth. This is due in large part to the expansion of Internet access to almost all sectors of society. Everyone who has a computer can now have access to the Web. Nowadays, children are introduced to the Web at an early age at school and at home. Numerous

electronic devices such as personal digital assistants (PDAs) and portable computers are saturating the network. The opportunity for expansion of services for the entire population is astronomical. This book is part of a program that is designed to provide a broad working knowledge of the security issues that permeate today's computer and network systems, and the forensic evidence that can be retrieved from these devices. It has been designed to provide corporate security personnel, educational organizations, government agencies, and members of law enforcement with a general understanding and working knowledge of the computer and electronic forensic environment.

This book is geared toward computer users in the business, government, and education communities, with the expectation that they can learn the basics of computer forensics. It is beneficial if the reader has some basic understanding of the telecommunications and computer topics; however, this is not necessary, as sufficient background is presented on all of the subjects. Two companion books by the author—*Broadband Communications* (ISBN 0-13-089321-8) and *Enterprise Security* (ISBN 0-13-047458-4)—provide a technical understanding of the current communications technologies and security issues. These books specifically cater to the business, government, and education markets and are more technical in nature.

This book provides a wide range of information relating to cyber-crime, E-commerce, and Internet activities that could exploit computer and electronic devices. Emphasis is placed on the numerous vulnerabilities and threats that are inherent in the Internet and networking environment. Efforts are made to present techniques and suggestions for corporate security personnel, first responders, investigators, and forensic examiners to successfully identify, retrieve, and protect valuable forensic evidence for litigation and prosecution.

In summary, this book is not highly technical. It provides just enough detail that allows the reader to apply the information provided and successfully address the numerous issues relating to computer and electronic evidence.

Organization of This Book

This book is divided into two major parts. Part 1 contains six chapters that provide basics relating to various crimes, laws, policies, forensic tools, and information needed to understand the underlying concepts of computer forensic investigations.

Chapter 1, Computer Forensic Investigation Basics, introduces the basic concepts that make up the field of computer forensics. The four-step process for computer forensic investigations is identified, as are the different types of evidence that are elements of computer forensics. The reader will become familiar with the various risks, threats, and incidents that relate to computer forensics. Differences between criminal and business policy investigations will be explored. This chapter sets the stage for the remainder of the book.

Chapter 2, Policies, Standards, Laws, and Legal Processes, introduces numerous laws and statutes that apply to computer-related crimes. It presents various techniques employed in court proceedings and acceptable electronic evidence. Security and computer-use policies and standards are related to security policy violations and criminal activities. The reader is exposed to numerous definitions of legal terms relating to electronic litigation. Expert witness requirements are presented.

Chapter 3, Electronic Forensic Examination Categories, identifies various crimes and incidents that are involved in electronic forensic investigations. This chapter shows how identity theft and fraud permeate all elements of the computer and electronics environment. It describes various types of evidence that can be gathered for each category of crime. The reader will become familiar with the various terms associated with these types of investigations and understand the importance of security and computer-use policies. Incidents that may be investigated by the corporate security department are described.

Chapter 4, Computer, Internet, and Electronic Crimes, explains to the reader what scams are and how scam artists work. The reader will become familiar with the crimes of identity theft and Internet fraud and their relationship to each other. The chapter identifies methods and techniques used to obtain evidence from Internet and Web resources. Resources for identifying evidence stored on business and personal computer assets, technical and legal terms relating to scams, fraud, and identity theft, and issues of child molestation and predators who are using the Web are described.

Chapter 5, Computers, Electronics, and Networking Environment, presents an overview of the E-commerce, networking environment, and the various hardware and software components and electronic devices that might contain forensic evidence. The chapter gives examples of forensic evidence that might be obtained from the crime/incident scenes and the types of evidence that can be recovered from computer and electronic devices. It lists the features available on network surveillance and management systems for the forensic investigator. The reader will learn about the hardware and software solutions that can provide investigative information addressing network security issues.

Chapter 6, Investigative Tools, Technical Training, and Forensic Equipment, identifies specialized tools and supplies required for electronic and computer forensic investigations. It describes various techniques employed for identifying and collecting electronic forensic evidence. It also discusses training requirements for electronic forensic investigators and examiners. It explains the use of software in computer network administration and surveillance and the equipment that provides for surveillance and capture of network traffic.

Part 2 contains eight chapters that provide information relating to crime scene investigations and management, disk and file structure, laboratory construction and functions, and legal testimony. Separate chapters are devoted to investigations involving computer systems, e-mail, and wireless devices.

Chapter 7, Managing the Crime/Incident Scene, makes the reader familiar with the responsibilities of the first responder at an incident site and helps the reader understand the requirements for managing the incident/crime scene. The reader will identify those steps necessary to make electronic evidence admissible in court, as well as the various players involved in an electronic/computer investigation. The chapter presents the issues relating to electronic and computer crime-scene investigations and shows how electronic forensics provides support in solving crimes. It presents a comparison of the investigative differences between corporate security and those of law enforcement. Information presented in this chapter can provide the investigator with the tools to make or break a case.

Chapter 8, Investigating Computer Center Incidents, helps the reader distinguish between white collar and blue collar crimes and corporate security violations and identify those processes taken when responding to security and policy violations. It explains how corporate incidents differ from law enforcement investigations and teaches specific steps to be taken when identifying, collecting, and protecting electronic evidence. The reader will be familiar with the requirements regarding the chain of custody for forensic evidence and will look at the possible areas where computer and electronic evidence resides.

Chapter 9, Computer Systems Disk and File Structures, identifies the various components of a hard drive and the structure of disk media. It explains the differences among the numerous disk drive interfaces and functions and stresses the importance of becoming familiar with the Windows, Macintosh, and Linux file structures. The chapter presents forensic tools used to identify and retrieve evidence from Windows, Macintosh, and Linux systems. The reader will learn the definitions of numerous terms relating to file and storage structures, and that most of the latent evidence that an examiner will recover will be located on the computer's hard drive.

Chapter 10, The Computer and Electronic Forensic Lab, exposes the reader to the functions of an electronic forensics laboratory and identifies the software, hardware, and infrastructure requirements of a forensics laboratory. The chapter discusses the processes required to identify and recover electronic evidence and the importance of documentation and chain of custody in the forensic process. The reader will see how evidence is recovered in the laboratory and learn the terms that are used in this environment.

Chapter 11, Extracting Computer and Electronic Evidence, teaches the functions that occur in a computer forensics lab and stresses the importance of the chain of custody and documentation. The reader will identify a process for deciding what evidence to collect, will look at the steps required to successfully process latent electronic evidence, and will understand the techniques required to image a hard drive.

Chapter 12, E-Mail and Internet Investigations, explains the basics of e-mail investigations oriented toward scams, spam, and other network activities. The reader will identify the various resources that can be utilized in these investigations and will look at the process for extracting investigative information from e-mail headers.

Chapter 13, Mobile Phone and PDA Investigations, identifies the components of mobile devices and how they can contain important investigative information. The chapter presents considerable information concerning the Subscriber Identity Module (SIM) component. The chapter provides a look at the different techniques and tools used on mobile phones and PDAs in a forensic investigation.

Chapter 14, Court Preparation, Presentations, and Testimony, helps the reader identify testimony requirements for electronic evidence presentations and learn how to be effective in technical courtroom presentations. The reader will also understand why examiners and investigators must be technically proficient, will learn the various legal terms associated with forensic testimony, and will become familiar with direct examination and cross-examination processes. Techniques will be presented to provide the forensic team with an edge in court testimony.

Appendices A through D provide a set of forensic investigation forms, exercises, answers to review questions, and other aids supporting the book.

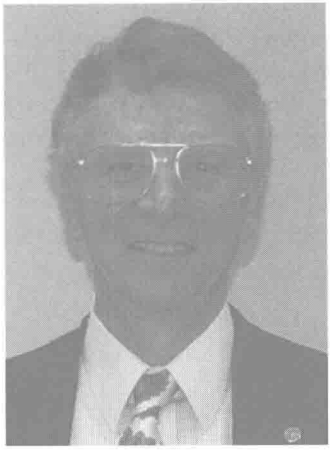
How to Utilize This Book

More than 200 key terms are provided throughout the book (**bold type**) and the definitions of these can be found in the Glossary.

More than 100 review questions, which provide a fairly complete coverage of the material, are presented throughout the book. The answers to these questions can be found in Appendix C. Found in Appendix B are optional exercises and cases that emphasize the book's content. Users should practice safe Internet and computer use when working through the cases and exercises. Keep backup copies of everything!

Many Web resources were utilized in developing this book. The selected bibliography lists a number of resources that would be beneficial to the forensic professional. The information presented in this book is patterned after technical, legal, and managerial classes by computer forensic professionals from Cyber Crime Summits held at Kennesaw State University in Kennesaw, GA in 2005 and 2006.

About the Author



Robert C. Newman, CISSP, is currently an instructor of Information Systems in the College of information technology at Georgia Southern University. Before that, he was associate professor of telecommunications management at the Decatur, Georgia campus of DeVry Institute of Technology. He is a long-time student and practitioner of data processing, data communications, and networking technologies, having started his career at the University of South Carolina in 1969 in the computer science department, where he held a number of positions in a large computer operation, including operations manager. He has taught in the computer information technology departments in a number of institutions of higher learning. Professor Newman has an ongoing working relationship concerning technical networking, disaster contingency planning, and security issues with the Georgia Southern University IT Services' organization.

Newman has authored two college-level books, *Enterprise Security* and *Broadband Communications. Enterprise Security*, published in 2003, covers all aspects of security from a technical manager's viewpoint and is widely used both in undergraduate and graduate studies, in the United States and several foreign countries. *Broadband Communications*, published in 2002, covers all of the current broadband communications technologies from strategic, tactical, and operations points of view.

Newman earned degrees from the University of South Carolina, Columbia and Georgia State University in Atlanta. He has advanced degree work in computer science at the University of Alabama, Birmingham. In addition, he has completed many formal technical courses in computer technology and in telecommunications marketing and sales support environments. He is currently active in computer-

forensic and enterprise information systems security education and has developed a security awareness program for the Georgia Southern campus.

Newman's professional experience includes many years in the telephone industry at BellSouth and AT&T. He accumulated a considerable amount of hands-on networking knowledge in software development, broadband operations, and network management and surveillance at BellSouth. Early in his career, he developed a solid background in IBM mainframe hardware and software.

Before his life in the computer industry, he was a member of federal, state, and county law enforcement agencies in Georgia, Alabama, and South Carolina. He is a graduate of the Northeast Georgia Police Academy and Georgia Post certified (GaPOST) and a Certified Information Systems Security Professional (CISSP). He is an active member of the Federal Bureau of Investigation's Coastal Empire Infragard organization. He has accumulated a wealth of knowledge on security and protection of data and computer resources and network administration. Security lectures are part of the network administration, management information systems, and data communications courses he currently teaches.

Professor Newman can be contacted at newmanrc@frontiernet.net or newmanrc@georgiasouthern.edu for comments and suggestions on the contents of this book.

Contents

SECTION I COMPUTER FORENSIC INVESTIGATION BASICS