

THIRD EDITION

DIGITAL EVIDENCE AND COMPUTER CRIME

FORENSIC SCIENCE, COMPUTERS AND THE INTERNET

EOGHAN CASEY



Digital Evidence and Computer Crime

Forensic Science, Computers and the Internet

Third Edition

Eoghan Casey

cmdLabs, Baltimore, Maryland, USA

Susan W. Brenner

Bert-Jaap Koops

Tessa Robinson

Bradley Schatz

Brent E. Turvey

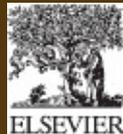
Terrance Maguire

Monique Ferraro

Michael McGrath

Christopher Daywalt

Benjamin Turnbull



AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO
Academic Press is an imprint of Elsevier



Related titles by Eoghan Casey

Handbook of Digital Forensics and Investigation

Edited by Eoghan Casey

<http://www.elsevierdirect.com/product.jsp?isbn=9780123742674>

Malware Forensics:

Investigating and Analyzing Malicious Code

By Cameron H. Malin, Eoghan Casey, and James M. Aquilina

<http://www.elsevierdirect.com/product.jsp?isbn=9781597492683>

Companion Web site for

Digital Evidence and Computer Crime, Third Edition

www.elsevierdirect.com/companions/9780123742681

Readers will have access to the author's accompanying Web site with supporting materials that integrate many of the topics in the text.

www.disclosedigital.com

Academic Press is an imprint of Elsevier

225 Wyman Street, Waltham, MA 02451, USA

525 B Street, Suite 1800, San Diego, California 92101-4495, USA

84 Theobald's Road, London WC1X 8RR, UK

© 2011 Eoghan Casey. Published by Elsevier Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: www.elsevier.com/permissions.

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data

Casey, Eoghan.

Digital evidence and computer crime: forensic science, computers and the internet / by Eoghan Casey; with contributions from Susan W. Brenner ... [et al.].—3rd ed.

p. cm.—

Includes index.

ISBN 978-0-12-374268-1

1. Computer crimes. 2. Electronic evidence. 3. Evidence, Criminal. I. Title.

HV6773.C35C35 2011

363.25' 968—dc22

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

ISBN: 978-0-12-374268-1

For information on all Academic Press publications visit our Web site at www.elsevierdirect.com

Printed in the United States of America

11 12 13 9 8 7 6 5 4 3 2 1

Working together to grow
libraries in developing countries

www.elsevier.com | www.bookaid.org | www.sabre.org

ELSEVIER

BOOK AID
International

Sabre Foundation

Acknowledgments

I would like to dedicate this work to my wife Rachel, and daughter Tigerlily.

Benjamin Turnbull

In the six years since the second edition of this text, I have worked with many brilliant digital investigators and I have taught hundreds of students. Together we tackled sophisticated network intrusions and complex forensic investigations that stretched us mentally and physically, taking over our lives for a time. I am deeply grateful to each of you for your friendship and influence, and I would like to give special thanks to the following.

The contributors Susan Brenner, Christopher Daywalt, Monique Mattei Ferraro, Ben Jaap Koops, Terrance Maguire, Mike McGrath, Tessa Robinson, Bradley Schatz, Ben Turnbull, and Brent Turvey, for your inspiration and persistence.

My entire family, for your support and patience. Genevieve, Roisin, and Hesper are my lifeblood, reminding me what is important in life and lifting me with limitless love every day. Ita O'Connor made all this possible, loving me unconditionally, teaching me right from wrong and how to write, and providing regular encouragement and editing during this revision. Clare O'Connor is my beacon and buttress, giving me guidance, love, and support throughout my life. Jim Casey, for your sage advice. Mary Allen Macneil, for your love and pride.

H. Morrow Long and everyone else at Yale University, who fostered my early interest in incident response and who continue to support my endeavors.

Robert Dunne, for his contribution to the previous edition; I mourn his passing.

Andy Johnson, for your continued camaraderie and sharing of ideas. Mike Lavine and Gerry Masson at Johns Hopkins University, for your support. All my colleagues at Stro Friedberg, particularly Ken Mendelson for actually reading the previous edition and pointing out typographical errors.

Christopher Brown, Brian Carrier, Michael Cohen, Stefan Fleischmann, Jesse Kornblum, Dario Forte, Brian Karney, Matt Shannon, and other tool developers for your continued efforts to improve digital forensic tools.

Liz Brown, Kristi Anderson, and the entire team at Elsevier for your support and patience during the incubation of this project.

Author Biographies

Susan W. Brenner

She is NCR Distinguished Professor of Law and Technology at the University of Dayton School of Law in Dayton, Ohio.

Professor Brenner has spoken at numerous events, including two Interpol Cybercrime Conferences, the Middle East IT Security Conference, the American Bar Association's National Cybercrime Conference, and the Yale Law School Conference on Cybercrime. She spoke on cyberthreats and the nation-state at the Department of Homeland Security's Global Cyber Security Conference and participated in a panel discussion of national security threats in cyberspace sponsored by the American Bar Association's Standing Committee on Law and National Security. In 2009, she spoke at a meeting on cyberthreats organized by the U.S. Department of State Bureau of Intelligence and Research and National Intelligence Council. She has also spoken at a NATO Workshop on Cyberterrorism in Bulgaria and on terrorists' use of the Internet at the American Society of International Law conference. She was a member of the European Union's CTOSE project on digital evidence and served on two Department of Justice digital evidence initiatives. Professor Brenner chaired a Working Group in an American Bar Association project that developed the ITU Toolkit for Cybercrime Legislation for the United Nations International Telecommunications Union. She is a Senior Principal for Global CyberRisk, LLC.

Professor Brenner is a member of the American Academy of Forensic Sciences. She has published a number of law review articles dealing with cybercrime, including "Fantasy Crime," *11 Vanderbilt Journal of Technology and Entertainment Law* 1 (2008), "State-Sponsored Crime: The Futility of the Economic Espionage Act," *26 Houston Journal of International Law* (2006), "Cybercrime Metrics," *University of Virginia Journal of Law & Technology* (2004), and "Toward a Criminal Law for Cyberspace: Distributed Security," *Boston University Journal of Science & Technology Law* (2004). Her books *Law in an Era of "Smart" Technology* and *Cyber Threats: Emerging Fault Lines of the Nation-States* were published by Oxford University Press in 2007 and 2009, respectively. In 2010, Praeger published her most recent book, *Cybercrime: Criminal Threats from Cyberspace*.

Eoghan Casey

He is founding partner of cmdLabs, author of the foundational book *Digital Evidence and Computer Crime*, and coauthor of *Malware Forensics*. For over a decade, he has dedicated himself to advancing the practice of incident handling and digital forensics. He specializes in helping organizations handle security breaches, including network intrusions with international scope. He has been involved in a wide range of digital investigations, including network intrusions, fraud, violent crimes, identity theft, and online criminal activity. He has testified in civil and criminal cases, has been involved in international tribunals, and has submitted expert reports and prepared trial exhibits for digital forensic and cybercrime cases.

Previously, as a Director at Stroz Friedberg, he maintained an active docket of cases, supervised a talented team of forensic examiners, managed the company's technical operations, and spearheaded external and in-house forensic training programs. Eoghan has performed thousands of forensic acquisitions and examinations, including cellular telephones and other mobile devices. He has performed vulnerability assessments; deployed and maintained intrusion detection systems, firewalls, and public key infrastructures; and developed policies, procedures, and educational programs for a variety of organizations. In addition, he conducts research and teaches graduate students at Johns Hopkins University's Information Security Institute, is editor of the *Handbook of Digital Forensics and Investigation*, and is Editor-in-Chief of Elsevier's *International Journal of Digital Investigation*.

Eoghan holds a B.S. in Mechanical Engineering from the University of California at Berkeley and an M.A. in Educational Communication and Technology from New York University.

Christopher Daywalt

He is a founding partner of cmdLabs, specializing in digital forensics, incident response, and related training. Chris has held positions ranging from system administrator to global security architect. Most recently he served as an instructor and course developer at the Defense Cyber Investigations Training Academy (DCITA), teaching Federal law enforcement and counter intelligence agents methodologies for investigating computer network intrusions.

Chris has also served as both a security analyst and an incident manager, handling enterprise-scale security incidents that involved large numbers of compromised hosts and massive data theft. He has performed a wide array of tasks in this area including forensic analysis of compromised systems, network monitoring, and assessment of malware and incident containment. He also holds a Master of Science in Network Security.

Monique M. Ferraro

She is the principal at Technology Forensics, LLC, an electronic evidence consulting firm in Waterbury, Connecticut. She is a Certified Information Systems Security Professional as well as a Digital Certified Forensic Practitioner. A licensed attorney, she is also a professor. She teaches in the Forensic Computing Master's Degree Program at John Jay College and American Intercontinental University.

She is a graduate of Western Connecticut State University with a Bachelor's Degree in Criminal Justice Administration (1985); she received her Master's Degree from Northeastern University in Criminal Justice (1987) and her Juris Doctorate from the University of Connecticut School of Law (1998).

She worked for 18 years in several different capacities with the State of Connecticut Department of Public Safety: 8 years with the Crimes Analysis Unit of the State Police, 5 years with the Intelligence Unit of the State Police, and 5 years with the Computer Crime and Electronic Evidence Laboratory within the Division of Scientific Services.

Attorney Ferraro has written a number of scholarly articles, book chapters, and one book (*Investigating Child Exploitation and Pornography: The Internet, the Law and Forensic Science*). She is an active member of the Connecticut Bar Association and has served as Chair of the Technology Section and has served on the Children and the Law Committee as well as the Women and the Law Committee.

In addition to her academic endeavors and professional service, Attorney Ferraro volunteers for Lawyers for Children America and has served on the State's Commission on Child Protection as an appointee of the Governor. She is a member of the board of directors of Jane Doe No More, a nonprofit organization whose mission is to educate police officers and the public about proper methods of investigating sexual assault and dealing with its victims.

Bert-Jaap Koops

He is professor of regulation and technology at the Tilburg Institute for Law, Technology and Society (TILT), the Netherlands. His main research interests are law and technology, in particular, criminal law issues such as cybercrime, investigation powers and privacy, and DNA forensics. He is also interested in other topics of technology regulation, such as data protection, identity, digital constitutional rights, "code as law," human enhancement, and regulation of bio- and nanotechnologies. Koops studied mathematics and general and comparative literature and received his PhD in law in 1999. He coedited six books on ICT regulation, including *Cybercrime and Jurisdiction: A Global Survey* (2006) and *Dimensions of Technology Regulation* (2010). His online Crypto Law Survey is a standard publication of

Terrance Maguire

He is a partner at cmdLabs, conducting cybercrime investigations, including those involving network intrusions, insider attacks, anonymous and harassing e-mails, data destruction, electronic discovery, and mobile devices. He has nearly 20 years of experience in physical and digital forensic investigations, has developed and led training programs in various areas of law enforcement and digital evidence, and has experience implementing counterintelligence intrusion detection programs.

Before working at cmdLabs, Terry was assistant director of Digital Forensics at Stro Friedberg, where he was responsible for casework, lab management, and internal training efforts. His prior experience includes senior-level forensic computer analyst the U.S. State Department, where he was responsible for conducting analysis on digital evidence. As a cyber operations specialist for the Department of Defense, he implemented network surveillance, network packet analysis, wireless surveys, and intrusion detection. In addition, at the Defense Computer Investigations Training Program (DCITP), Terry developed and presented a broad range of instruction to federal law enforcement on topics such as computer search and seizure, incident response, digital evidence, computer forensic examinations, and intrusion investigations.

Earlier in his investigative career, as a forensic detective with the Chesterfield County Police Department in Virginia, Terry collected, evaluated, and processed evidence from crime scenes, prepared comprehensive case reports, and trained department personnel in forensic techniques. Subsequently, as a forensic scientist for the Virginia Division of Forensic Science, he conducted bloodstain pattern analysis in criminal cases and testified in court as an expert witness, and he was the principal instructor at the Forensic Science Academy.

Terry is a professorial lecturer at the George Washington University, where he teaches graduate-level courses focusing on incident response and computer intrusion investigations involving network-based attacks. He received an M.S. in Communication Technology from Strayer University and a B.S. in Chemistry from James Madison University. He is qualified as an ASCLD/LAB inspector in digital evidence and is a member of the Virginia Forensic Science Academy Alumni Association.

Michael McGrath

He divides his time between clinical, administrative, teaching, and research activities

His areas of special expertise include forensic psychiatry and criminal profiling. He has lectured on three continents and is a founding member of the Academy of Behavioral Profiling. He has published articles and/or chapters related to criminal profiling, sexual predators and the Internet, false allegations of sexual assault, and sexual asphyxia.

Tessa Robinson

She studied at Trinity College, Dublin, and at the Honorable Society of the King's Inns. She was called to the Irish Bar in 1998.

Bradley Schatz

He is the director of the digital forensics consultancy Schatz Forensic and an adjunct associate professor at the Queensland University of Technology, Australia. Dr. Schatz divides his time between providing forensic services primarily to the legal sector and researching and educating in the area of computer forensics and digital evidence. Dr Schatz is the only Australian private practice practitioner to hold a PhD in computer forensics.

Benjamin Turnbull

He is a Post-Doctorate Researcher for the University of South Australia Defence and Systems Institute. His research interests include the misuse and evidentiary value of wireless networks, and understanding how the Internet facilitates global drug crime.

Brent E. Turvey

He spent his first years in college on a pre-med track only to change his course of study once his true interests took hold. He received a Bachelor of Science degree from Portland State University in Psychology, with an emphasis on Forensic Psychology, and an additional Bachelor of Science degree in History. He went on to receive his Master's of Science in Forensic Science after studying at the University of New Haven, in West Haven, Connecticut.

Since graduating in 1996, Mr. Turvey has consulted with many organizations, attorney and law enforcement agencies in the United States, Australia, Scotland, China, Canada, Barbados, Singapore, and Korea on a range of rapes, homicides, and serial/multiple rape/death cases, as a forensic scientist and criminal profiler. In August of 2002, he was invited by the Chinese People's Police Security University (CPPSU) in Beijing to lecture before groups of detectives at the Beijing, Wuhan, Hanzou, and Shanghai police bureaus.

2005, he was invited back to China again, to lecture at the CPPSU, and to the police in Beijing and Xian—after the translation of the second edition of his text into Chinese for the university. In 2007, he was invited to lecture at the First Behavioral Sciences Conference at the Home Team (Police) Academy in Singapore, where he also provided training to the Behavioral Science Unit. In 2010, he examined a series of sexual homicides for the Solicitor General of the Crown Office and Procurator Fiscal Service (COPFS) in Edinburgh, Scotland.

He has also been court qualified as an expert in the areas of criminal profiling, crime scene investigation, crime scene analysis, forensic science, victimology, and crime reconstruction in many courts and jurisdictions around the United States.

Mr. Turvey is the author of *Criminal Profiling: An Introduction to Behavioral Evidence Analysis*, 1st, 2nd, 3rd, and 4th Editions (1999, 2002, 2008, 2011), and coauthor of the *Rape Investigation Handbook* (2004), *Crime Reconstruction* (2006), *Forensic Victimology* (2009), and *Forensic Criminology* (2010)—all with Elsevier Science. He is currently a full partner, forensic scientist, criminal profiler, and instructor with Forensic Solutions, LLC, and an adjunct professor of justice studies at Oklahoma City University.

He can be contacted via email at bturvey@forensic-science.com.

Introduction

In 2004, when I wrote the previous edition of this book, I described technology as a window into our lives and the lives of criminals. In this metaphor was a separation between the virtual and physical world. Now this separation is gone. Technology is integrated inseparably into our lives, present and active wherever we are.

In a sense, cyberspace turns itself inside out when the technology is aware of our physical location in the world, providing location-dependent services to the user and conversely enabling digital investigators to determine where an individual of interest was during the time of a crime. In *Spook Country*, William Gibson describes various facets of the perversion of cyberspace.

The locative properties of modern technology provide a prime example of this perversion. For instance, while I am having an Aussie at Brewer's Art in Baltimore, my smart phone is chattering with various systems to orient itself and provide me with information about my immediate surroundings. Opening the map function not only shows my location but also points out places of interest in the area such as Baltimore Symphony Orchestra (Meyerhoff Symphony Hall), Lyric Opera House, and Penn Station (Figure 1).

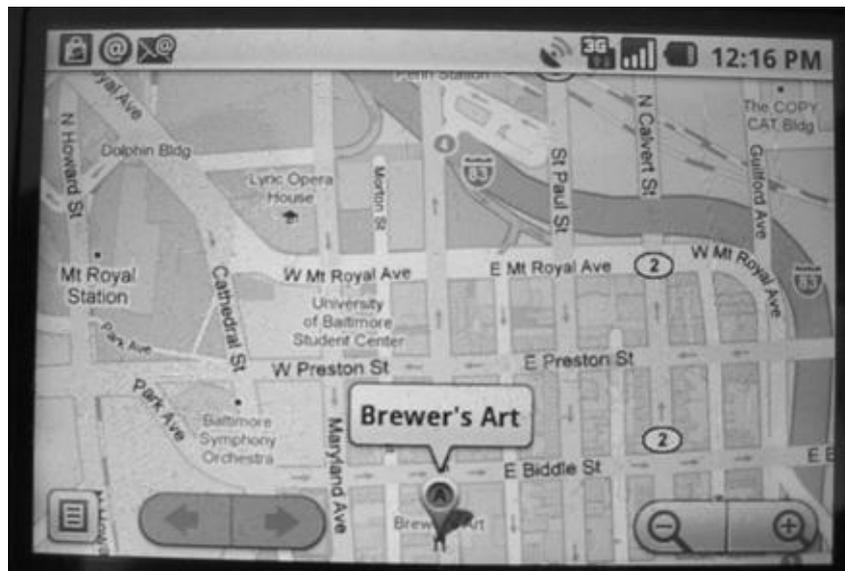


Figure 1 Map application on mobile device showing Brewer's Art and surrounding area.

When I settle the tab, my credit card payment generates a record of the time and place. Walking out of the microbrewery down historic Charles Street exposes me to various CCT

cameras in the neighborhood, recording my physical presence in digital video format.

GPS technology like the device shown in [Figure 2](#) is widely used to determine the most direct route to a destination. Forensic examination of such devices can reveal the location of an individual when a crime was committed.



Figure 2 Photograph of Garmin GPS with directions to Brewer's Art.

The commercialization of GPS technology not only helps us navigate but also enables us to track others as demonstrated in the George Ford case described in [Chapter 10](#). Individuals can share their location with friends via online services such as Google Latitude, and parents can use this technology to keep track of their family. For example, Verizon's Family Locator service tied to their mobile telephones can be configured with zones, causing the GPS coordinates of a mobile device to send a message to parents when their child enters or leaves home or school.

Our location can also be used to generate crowdsource services. For instance, Google aggregates location data from many people's GPS-enabled mobile devices to generate information such as traffic patterns.

Reach out and hurt someone

With this integration or eversion of cyberspace comes an increase in the realness of virtual events. Bullying in high schools and hate crimes in universities have moved into cyberspace, amplifying these harmful behaviors by delivering virtual blows anytime, anywhere. In January 2010, 15-year-old Pheobe Prince committed suicide as a result of cyberbullying (see [Chapter 1](#)). In September 2010, Rutgers student Tyler Clementi committed suicide after his roommate secretly set up a Webcam in their dorm room to stream video of Clementi making

out with another man.

As covered in [Chapter 12](#), pedophiles use the Internet to groom victims and arrange meetings to sexually exploit children.

Cyberstalkers use technology in creative ways to harass victims, not only causing psychological harm but also putting victims at risk of physical harm. In several cases, cyberstalkers have posted online ads encouraging others on the Internet to contact a victim for sex. In the case of Dellapenta (see [Chapter 14](#)), men showed up at the victim's home.

Organized criminal groups are gaining unauthorized access to individuals' bank accounts, viewing their computers and stealing their savings. In September 2010, members of a criminal group were arrested for their use of a malicious computer program named ZeuS to steal money from the bank accounts of thousands of victims.

Identity thieves are stealing personal information that is stored on computers and using this information to obtain credit cards and other loans, buy houses and other valuable property, and even file for bankruptcy in the victim's name. Identity fraud burdens victims with debts that can take years and substantial resources to clear from their name.

Nations are developing cyberweapons to cause physical damage through computers. The StuxNet malware that emerged in 2010 is a powerful demonstration of the potential for such attacks. It was a sophisticated program that enabled the attackers to alter the operation of industrial systems such as those in a nuclear reactor by accessing programmable logic controllers connected to the target computers. This type of attack could shut down a power plant or other components of a society's critical infrastructure, potentially causing significant harm to people in a targeted region.

Digital and multimedia science

As the seriousness and scope of crimes involving computers increases, greater attention is being focused on apprehending and prosecuting offenders. New technologies and legislative measures are being developed to facilitate the investigation of criminal activities involving computers. More organizations are seeking qualified practitioners to conduct digital investigations. In addition, increased awareness of digital forensics has drawn many people to the field.

One thing about digital forensics that appeals to many practitioners is the social contribution of serving the criminal justice system or another system such as national defense. Another thing about digital forensics that is appealing to many is that every case is different. Investigating human misuse of computers creates new puzzles and technical challenges, particularly when offenders attempt to conceal incriminating evidence and their activities on computer systems and networks. In addition, the growing demand for qualified

practitioners also makes digital forensics an attractive career choice.

This growing interest and need has sparked heated debates about tools, terminology, definitions, standards, ethics, and many other fundamental aspects of this developing field. It should come as no surprise that this book reflects my positions in these debates. More notably, this text reflects my firm belief that this field must become more scientific in its approach. The primary aim of this work is to help the reader tackle the challenging process of seeking scientific truth through objective and thorough analysis of digital evidence. A desired outcome of this work is to encourage the reader to advance this field as a forensic science discipline.

In an effort to provide clarity and direction, [Chapter 6](#) specifically addresses the application of scientific method in all phases of a digital investigation. In addition, I encourage you to become involved in the DFRWS Conference (www.dfrws.org) and the Digital and Multimedia Section of the American Academy of Forensic Sciences (www.aafs.org). Finally, I encourage training programs and educational institutions to integrate forensic science into their digital forensics courses and not simply treat it as a technical subject.

By increasing the scientific rigor in digital forensics, we can increase the quality and consistency of our work, reducing the risk of miscarriages of justice based on improper digital evidence handling.

Terminology

The movement toward standardization in how digital evidence and computer crime are handled has been made more difficult by the lack of agreement on basic terminology. There has been a great deal of debate among experts on just what constitutes a computer crime. Some people use the term *computer crime* to describe any crime that involves a computer. More specifically, computer crime refers to a limited set of offenses that are defined in law, such as the U.S. Computer Fraud and Abuse Act and the U.K. Computer Abuse Act. These crimes include theft of computer services; unauthorized access to protected computer systems; software piracy and the alteration or theft of electronically stored information; extortion committed with the assistance of computers; obtaining unauthorized access to records from banks, credit card issuers, or customer reporting agencies; traffic in stolen passwords; and transmission of destructive viruses or commands.

One of the main difficulties in defining computer crime is that situations arise where a computer or network was not directly involved in a crime but still contains digital evidence related to the crime. As an extreme example, take a suspect who claims that she was using

the Internet at the time of a crime. Although the computer played no role in the crime, contains digital evidence relevant to the investigation. To accommodate this type of situation the more general term *computer-related* is used to refer to any crime that involves computers and networks, including crimes that do not rely heavily on computers. Notably, some organizations, such as the U.S. Department of Justice and the Council of Europe, use the term *cybercrime* to refer to a wide range of crimes that involve computers and networks.

In an effort to be inclusive and most useful for practical application, the material in this book covers digital evidence as it applies to any crime and delves into specific computer crimes that are defined by laws in various countries. The term *digital investigation* is used throughout this text to encompass any and all investigations that involve digital evidence including corporate, civil, criminal, and military.

The term *computer forensics* also means different things to different people. Computer forensics usually refers to the forensic examination of computer components and their contents such as hard drives, compact disks, and printers. However, the term is sometimes used more loosely to describe the forensic examination of all forms of digital evidence including data traveling over networks (a.k.a. network forensics). To confuse matters, the term *computer forensics* has been adopted by the information security community to describe a wide range of activities that have more to do with protecting computer systems than gathering evidence.

As the field has developed into several distinct subdisciplines, including malware forensics and mobile device forensics, the more general term *digital forensics* has become widely used to describe the field as a whole.

Roadmap to the Book

This book draws from four fields:

Forensic Science

Computer Science

Law

Behavioral Evidence Analysis

Law provides the framework within which all of the concepts of this book fit. Computer Science provides the technical details that are necessary to understand specific aspects of digital evidence. Forensic Science provides a general approach to analyzing any form of digital evidence. Behavioral Evidence Analysis provides a systematized method of synthesizing the specific technical knowledge and general scientific methods to gain a better

understanding of criminal behavior and motivation.

This book is divided into five parts, beginning with the fundamental concepts and legal issues relating to digital evidence and computer crime in Part 1 (Digital Forensics: [Chapters 1–5](#)). [Chapter 2](#) (Language of Computer Crime Investigation) explains how terminology of computer crime developed and provides the language needed to understand the different aspects of computer crime investigation. [Chapter 3](#) (Digital Evidence in the Courtroom) provides an overview of issues that arise in court relating to digital evidence. [Chapters 4 and 5](#) (Cybercrime Law: A United States Perspective and Cybercrime Law: A European Perspective) discuss legal issues that arise in computer-related investigations, presenting U.S. and European law side-by-side.

Part 2 (Digital Investigations: [Chapters 6–9](#)) discusses a systematic approach to investigating a crime based on the scientific method, providing a context for the remainder of this book. [Chapter 7](#) (Handling a Digital Crime Scene) provides guidance on how to approach and process computer systems and their contents as a crime scene. [Chapter 8](#) (Investigative Reconstruction with Digital Evidence) describes how to use digital evidence to reconstruct events and learn more about the victim and offender in a crime. [Chapter 9](#) (Modus Operandi, Motive, and Technology) is a discussion of the relationship between technology and the people who use it to commit crime. Understanding the human elements of a crime and the underlying motivations can help answer crucial questions in an investigation, helping assess risks (will criminal activity escalate?), develop and interview suspects (who to look for and what to say to them), and focus inquiries (where to look and what to look for).

Part 3 (Apprehending Offenders: [Chapters 10–14](#)) focuses on specific types of investigations with a focus on apprehending offenders, starting with violent crime in [Chapter 10](#). [Chapter 11](#) discusses computers as alibi. [Chapter 12](#) details sex offenders on the Internet. Investigating computer intrusions is covered in [Chapter 13](#). [Chapter 14](#) covers investigation of cyberstalking.

Part 4 (Computers: [Chapters 15–20](#)) begins by introducing basic forensic science concepts in the context of a single computer. Learning how to deal with individual computers is crucial because even when networks are involved, it is usually necessary to collect digital evidence stored on computers. Case examples and guidelines are provided to help apply the knowledge in this text to investigations. The remainder of Part 4 deals with specific kinds of computer systems and ends with a discussion of overcoming password protection and encryption on these systems.

Part 5 (Network Forensics: [Chapters 21–25](#)) covers computer networks, focusing specifically on the Internet. A top-down approach is used to describe computer networks, starting with the types of data that can be found on networked systems and the Internet, and

progressively delving into the details of network protocols and raw data transmitted over networks. The “top” of a computer network comprises the software that people use, like e-mail and the Web. This upper region hides the underlying complexity of computer networks and it is therefore necessary to examine and understand the underlying complexity of computer networks to fully appreciate the information that we find at the top of the network. Understanding the “bottom” of networks—the physical media (e.g., copper and fiber-optic cables) that carry data between computers—is also necessary to collect and analyze raw network traffic.

The forensic science concepts described early on in relation to a single computer are carried through to each layer of the Internet. Seeing concepts from forensic science applied in a variety of contexts will help the reader generalize the systematic approach to processing and analyzing digital evidence. Once generalized, this systematic approach can be applied to situations not specifically discussed in this text.

Disclaimer

Tools are mentioned in this book to illustrate concepts and techniques, not to indicate that a particular tool is best suited to a particular purpose. Digital investigators must take responsibility to select and evaluate their tools.

Any legal issues covered in this text are provided to improve understanding only and are not intended as legal advice. Seek competent legal advice to address specifics of a case and to ensure that nuances of the law are considered.

Table of Contents

Cover Image

Title

Front Matter

Copyright

Acknowledgments

Author Biographies

Introduction

Digital Forensics

Chapter 1. Foundations of Digital Forensics

1.1 Digital Evidence

1.2 Increasing Awareness of Digital Evidence

1.3 Digital Forensics: Past, Present, and Future

1.4 Principles of Digital Forensics

1.5 Challenging Aspects of Digital Evidence

1.6 Following the Cybertrail

1.7 Digital Forensics Research

1.8 Summary

Chapter 2. Language of Computer Crime Investigation

2.1 Language of Computer Crime Investigation

2.2 The Role of Computers in Crime

2.3 Summary

Chapter 3. Digital Evidence in the Courtroom

3.1 Duty of Experts

3.2 Admissibility

3.3 Levels of Certainty in Digital Forensics

3.4 Direct versus circumstantial evidence

3.5 Scientific Evidence

3.6 Presenting Digital Evidence

3.7 Summary

Chapter 4. Cybercrime Law

4.1 Federal Cybercrime Law

4.2 State cybercrime law

4.3 Constitutional law

4.4 Fourth Amendment

4.5 Fifth Amendment and encryption

Chapter 5. Cybercrime Law

5.1 The European and National Legal Frameworks

5.2 Progression of Cybercrime Legislation in Europe

5.3 Specific Cybercrime Offenses

5.4 Computer-Integrity Crimes

5.5 Computer-Assisted Crimes

5.6 Content-Related Cybercrimes

5.7 Other Offenses

5.8 Jurisdiction

5.9 Summary

Digital Investigations

Chapter 6. Conducting Digital Investigations

6.1 Digital Investigation Process Models

6.2 Scaffolding for Digital Investigations

6.3 Applying the Scientific Method in Digital Investigations

6.4 Investigative Scenario: Security Breach

6.5 Summary

Chapter 7. Handling a Digital Crime Scene

7.1 Published Guidelines for Handling Digital Crime Scenes

7.2 Fundamental Principles

7.3 Authorization

7.4 Preparing to Handle Digital Crime Scenes

7.5 Surveying the Digital Crime Scene

7.6 Preserving the Digital Crime Scene

7.7 Summary

Chapter 8. Investigative Reconstruction with Digital Evidence

8.1 Equivocal Forensic Analysis

8.2 Victimology

8.3 Crime Scene Characteristics

8.4 Threshold Assessments

8.5 Summary

Chapter 9., Motive, and Technology

9.1 Axes to Pathological Criminals and Other Unintended Consequences

9.2 Modus Operandi

9.3 Technology and Modus Operandi

9.4 Motive and Technology

9.5 Current Technologies

9.6 Summary

Apprehending Offenders

Chapter 10. Violent Crime and Digital Evidence

10.1 The Role of Computers in Violent Crime

10.2 Processing The Digital Crime Scene

10.3 Investigative Reconstruction

10.4 Conclusions

Chapter 11. Digital Evidence as Alibi

11.1 Investigating an Alibi

11.2 Time as Alibi

11.3 Location as Alibi

11.4 Summary

Chapter 12. Sex Offenders on the Internet

12.1 Old Behaviors, New Medium

12.2 Legal Considerations

12.3 Identifying and Processing Digital Evidence

12.4 Investigating Online Sexual Offenders

12.5 Investigative Reconstruction

12.6 Case Example: Scott Tyree³

12.7 Case Example: Peter Chapman⁶

12.8 Summary

Chapter 13. Computer Intrusions

13.1 How Computer Intruders Operate

13.2 Investigating Computer Intrusions

13.3 Forensic Preservation of Volatile Data

13.4 Post-Mortem Investigation of a Compromised System

13.5 Investigation of Malicious Computer Programs

13.6 Investigative Reconstruction

13.7 Summary

Chapter 14. Cyberstalking

14.1 How Cyberstalkers Operate

14.2 Investigating Cyberstalking

14.3 Cyberstalking case example³

14.4 Summary

Computers

Chapter 15. Computer Basics for Digital Investigators

15.1 A Brief History of Computers

15.2 Basic Operation of Computers

15.3 Representation of Data

15.4 Storage Media and Data Hiding

15.5 File Systems and Location of Data

15.6 Dealing with Password Protection and Encryption

15.7 Summary

Chapter 16. Applying Forensic Science to Computers

16.1 Preparation

16.2 Survey

16.3 Documentation

16.4 Preservation

16.5 Examination and Analysis

16.6 Reconstruction

16.7 Reporting

16.8 Summary

Chapter 17. Digital Evidence on Windows Systems

17.1 File Systems

17.2 Data Recovery

17.3 Log Files

17.4 Registry

17.5 Internet Traces

17.6 Program Analysis

17.7 Summary

- [download online Hear No Evil \(Jack Swyteck, Book 4\)](#)
- [download Methods in Brain Connectivity Inference Through Multivariate Time Series Analysis for free](#)
- [Conspiracy here](#)
- [Michelin Green Guide: Wine Trails of Italy pdf, azw \(kindle\)](#)
- [The Threat of Force in International Law \(Cambridge Studies in International and Comparative Law\) pdf](#)

- <http://www.uverp.it/library/BBC-Easy-Cook--UK---May-2016-.pdf>
- <http://honareavalmusic.com/?books/Suicide-Kings--Wild-Cards--Book-20-.pdf>
- <http://aneventshop.com/ebooks/Sewing-101--Revised-and-Updated--Master-Basic-Skills-and-Techniques-Easily-through-Step-by-Step-Instruction.pdf>
- <http://tuscalaural.com/library/Michelin-Green-Guide--Wine-Trails-of-Italy.pdf>
- <http://kamallubana.com/?library/The-Threat-of-Force-in-International-Law--Cambridge-Studies-in-International-and-Comparative-Law-.pdf>