DIGITAL EVIDENCE AND COMPUTER CRIME

SECOND EDITION

COMPUTER FORENSIC AND COMPUTER SECURITY RELATED BOOK TITLES:

- Casey, *Handbook of Computer Crime Investigation*, ISBN 0-12-163103-6, 448pp, 2002.
- Kovacich, *The Information Systems Security Officer's Guide*, ISBN 0-7506-7656-6, 361pp, 2003.
- Boyce and Jennings, *Information Assurance*, ISBN 0-7506-7327-3, 261pp, 2002.
- Stefanek, *Information Security Best Practices: 205 Basic Rules*, ISBN 0-878707-96-5, 194pp, 2002.
- De Clercq, *Windows Server 2003 Security Infrastructures: Core Security Features*, ISBN 1-55558-283-4, 752pp, 2004.
- Rittinghouse, *Wireless Operational Security*, ISBN 1-55558-317-2, 496pp, 2004.
- Rittinghouse & Hancock, *Cybersecurity Operations Handbook*, ISBN 1-55558-306-7, 1336pp, 2003.
- Speed & Ellis, *Internet Security*, ISBN 1-55558-298-2, 398pp, 2003.
- Erbschloe, *Implementing Homeland Security for Enterprise IT*, ISBN 1-55558-312-1, 320pp, 2003.
- XYPRO, *HP NonStop Server Security*, ISBN 1-55558-314-8, 618pp, 2003.

For more information, visit us on the web at **http://books.elsevier.com**

COMPUTER FORENSIC AND COMPUTER SECURITY RELATED PRODUCTS FROM ELSEVIER:

Compsec Newsletters and Journals:

- Biometric Technology Today
- Card Technology Today
- Computer Fraud & Security
- Computer Law and Security Report
- Computers & Security
- Information Security Technical Report
- Network Security
- Digital Investigation

Compsec Market Reports:

- Biometric Industry Report
- Smart Card Report

Compsec Conferences:

- Compsec2004
- Biometrics2004
- IDSmart

For more information, visit us on the web at **http://www.compseconline.com**

DIGITAL EVIDENCE AND COMPUTER CRIME

FORENSIC SCIENCE, COMPUTERS AND THE INTERNET

Second Edition

by Eoghan Casey

with contributions from

Robert Dunne
Monique Mattei Ferraro
Troy Larson
Michael McGrath
Gary Palmer
Tessa Robinson
Brent Turvey

ELSEVIER
ACADEMIC
PRESS

Amsterdam • Boston • Heidelberg • London • New York • Oxford
Paris • San Diego • San Francisco • Singapore • Sydney • Tokyo

First published 2000
Reprinted 2001, 2003
Second edition 2004

Academic Press
An imprint of Elsevier
84 Theobald's Road, London WC1X 8RR, UK
http://www.academicpress.com

Academic Press
An imprint of Elsevier
525 B Suite, Suite 1900, San Diego, California 92101-4495, USA
http://www.academicpress.com

ISBN 0-12-163104-4

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

Library of Congress Cataloging-in-Publication Data

Casey, Eoghan
Digital evidence and computer crime: forensic science, computers, and the Internet/Eoghan Casey.—2nd ed.
p. cm.
Includes bibliographical references.
ISBN 0–12–163104–4 (alk.paper)
1. Computer crimes. 2. Evidence, Criminal. I. Title

HV6773.C35.C35 2004
363.25′968—dc22 2003063576

Typeset by Newgen Imaging Systems (P) Ltd, Chennai, India
Printed and bound in Great Britain

CONTENTS

The substance and structure of this book are the result of several years of intensive case work, research, and teaching. Many colleagues, students, and my family and friends assisted me during this period. I am deeply grateful to each of you for your support and I would like to give special thanks to the following.

The contributors Robert Dunne, Monique Mattei Ferraro, Troy Larson, Mike McGrath, Gary Palmer, Tessa Robinson, and Brent Turvey for your inspiration, dedication, and for accepting the ambitious schedule. Barbara Troyer for your assistance with the figures in the text and your friendship over the years.

Colin Harris and Stephen Douglas for your direction and calming influence during the rough patches. Clare O'Connor for your lifelong encouragement and guidance. Jim Casey for your sage advice. Ita O'Connor for your clarity of thought and for making this all possible. Genevieve Gessert for your boundless love, friendship, and support.

H. Morrow Long, Andrew Newman, Shawn Bayern, and everyone else at Yale University for the supportive and challenging work–learning environment.

Bruce Patterson, Andy Russell, Jim Smith, Joe Sudol, Ken Gray, John Blawie, Mike O'Connor, Mark Califano and everyone in the Connecticut State Crime Laboratory, FBI, and State's and US Attorney's Offices for your dedication and camaraderie.

Fred Cotton, Todd Colvin, Jim Jolley, Keith Daniels, Glenn Lewis, and everyone at SEARCH for your continued support.

Tony Noble, Javier Torner, Larry Amos, Don Allison, Harlan Carvey, Paul Gillen, Harold Jones, Gary Gordon, Sarah Mocas, Warren Harrison, Mark Morrisey, Mark Bowser, Warren Kruse, and Carrie Whitcomb for your personal encouragement and contributions.

Brian Carrier for your technical review of Chapters 10–12 and E. Larry Lidz for your technical review of Chapters 16–18.

Brian Carrier, Joe Grand, Dan Mares, John Patzakis, Amber Schroader, Eric Thompson, Bob Weitershausen, and Walker Whitehouse for assistance with your digital evidence examination tools.

Mark Listewnik, Linda Beattie, Jennifer Rhuda, and the others at Academic Press who fostered this project over the years.

Eoghan Casey is a founding member of Knowledge Solutions LLC, a partnership of practicing forensic professionals who have made a commitment to providing quality training, information resources, and case consultations. He investigates network intrusions, intellectual property theft, and other computer-related crimes, and has extensive experience analyzing digital evidence. He has assisted law enforcement in a wide range of criminal investigations including homicide, child exploitation, cyber'stalking, and larceny. Eoghan also has extensive information security experience. As an Information Security Officer at Yale University and in subsequent consulting work, he has performed vulnerability assessments, deployed and maintained intrusion detection systems, firewalls and public key infrastructures, and developed policies, procedures, and educational programs. Eoghan holds a B.S. in Mechanical Engineering from the University of California at Berkeley, an M.A. in Educational Communication and Technology from New York University, and is currently working towards a Ph.D. in Computer Science at University College Dublin. Eoghan also brought together forensic experts to create the Handbook of Computer Crime Investigation: Forensic Tools and Technology. He can be contacted at eco@corpus-delicti.com.

Robert Dunne is an attorney and member of the faculty in the Department of Computer Science at Yale University, where he teaches "Computers and the Law," "Legal Implications of Computing Technology," and "Intellectual Property in the Digital Age." He has written on alternative paradigms for behavioral control in cyberspace, the impact of cyberspace on the legal profession, and Internet crime. Robert is Co-Director of Yale's Center for Internet Studies, an interdisciplinary enterprise whose goal is to explore the Internet's effect on society, and vice versa, from technological, legal, political, economic, cultural, and educational perspectives.

Monique Mattei Ferraro is an attorney with the Connecticut Department of Public Safety Computer Crimes and Electronic Evidence Unit and a Certified Information Systems Security Professional. She has been with the Department of Public Safety since 1987. She advises the Computer Crimes Unit and the Internet Crimes Against Children Task Force, develops training curricula for law enforcement, prosecutors and the public regarding Computer Crime Investigation and Internet Safety. Monique is co-author of Connecticut's Law Enforcement Guidelines for Computer and Electronic Evidence Search and Seizure, and is currently coauthoring a book on Investigating Child Exploitation with Eoghan. She holds a Master's degree from Northeastern University and a Law Degree from the University of Connecticut Law School.

Troy Larson is president of Digital Evidence Solutions, Inc., based in Seattle, Washington. Mr. Larson specializes in assisting attorneys with electronic evidence throughout all facets of litigation, particularly discovery and expert testimony. He is a member of the Washington State Bar and received both his undergraduate and law degrees from the University of California at Berkeley. He can be contacted at ntevidence@comcast.net.

Dr. Michael McGrath 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.

Gary Palmer is an INFOSEC Research Scientist for the MITRE Corporation, Bedford, MA in the Security and Information Operations Group (G021). He currently supports the Digital Forensic Research programs at the Air Force Research Laboratory's (AFRL) Rome Research Site in Rome, New York where he is focusing efforts on forensic identification, recovery and analysis of database systems as well as the forensic implications of wireless technology. Gary is also co-founder and a lead organizer of the Digital Forensic Research Workshop (DFRWS), sponsored by AFRL, which provides a forum for dialog between academic research and practice in the field. He attained a BS in 1979 from The Virginia Polytechnic Institute and State University (VATech). He has been active in the field of computer, network and information security since 1981 and wrote his first macro assembler program on a paper tape attached to a DEC PDP/11-44 running RSX11/M with 64K overlays. He lives in Sanford, FL, where he rides his motorcycle, plays the guitar and is currently enrolled in a Computer Forensic Graduate Certificate Program at the University of Central Florida.

Tessa Robinson B.L. studied at Trinity College Dublin and the Kings Inns. She is a practising barrister, called to the Irish bar in 1998. Her areas of practice include criminal, commercial, administrative and family law. Prior to commencing at the bar in Ireland she worked in New York with the Lawyers Committee for Human Rights, in Brussels with White & Case, in San Francisco with Morrison Foerster and in Washington D.C. with Hogan Hartson.

Brent Turvey received his Masters of Science in Forensic Science after studying at the University of New Haven, in West Haven, Connecticut. He also holds 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 has been studying violent sex offenders since 1990. He has consulted with law enforcement, attorneys, and private agencies in the United States, New Zealand, Canada, Australia, Korea and China on a range of serial rapes, homicides, staged crime scenes, and multiple death cases, as a forensic scientist and criminal profiler. He is author of the textbook Criminal Profiling: An Introduction to Behavioral Evidence Analysis, 2nd Ed., which is used in colleges and universities all over the world. He is currently a full partner, Criminal Profiler, and Instructor with Knowledge Solutions LLC.

INTRODUCTION

In the years since the first edition of this book, there has been an explosion of interest in digital evidence. This growth 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. Most 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.

AREAS OF SPECIALIZATION

Currently, there is little clarity in this field regarding areas of specialization and who should receive what training. For instance, there is no clear distinction between digital crime scene technicians (a.k.a. first responders) and digital evidence examiners, despite the fact that data recovery requires more knowledge than basic evidence documentation, collection, and preservation. The investigative process detailed in Chapter 4 suggests three distinct groups with different levels of knowledge and training.

- *Digital Crime Scene Technicians*: Individuals responsible for gathering data at a crime scene should have basic training in evidence handling and documentation as well as in basic crime reconstruction to help them locate all available sources of evidence on a network.
- *Digital Evidence Examiners*: Individuals responsible for processing particular kinds of digital evidence require specialized training and certification in their area.
- *Digital Investigators*: Individuals responsible for the overall investigation should receive a general training but do not need very specialized training or certification. Investigators are also responsible for reconstructing the actions relating to a crime using information from first responders and forensic examiners to create a more complete picture for investigators and attorneys.

Training and certification programs in this field should take into account these different areas of expertise.

For the purposes of this text, the more general term "digital investigator" is used to refer to individuals who play a key role in digital investigations, including computer security professionals, attorneys, law enforcement officers and forensic examiners.

RELIABILITY OF DIGITAL EVIDENCE

Digital investigators do not currently have a systematic method for stating the certainty they are placing in the digital evidence they are using to reach their conclusions. This lack of formalization makes it more difficult for courts and other decision makers to assess the reliability of digital evidence and the strength of digital investigators' conclusions. The Certainty Scale presented in Chapter 7 provides a consistent method of referring to the relative certainty of different types of digital evidence. The immediate aim of the Certainty Scale is to improve our ability to assess the reliability of digital evidence.

Ultimately, it is hoped that this Certainty Scale will point to areas that require additional attention in digital evidence research. Debate over C-values in specific cases may reveal that certain types of evidence are less reliable than was initially assumed. For some types of digital evidence, it may be possible to identify the main sources of error or uncertainty and develop analysis techniques for evaluating or reducing these influences. For other types of digital evidence, it may be possible to identify all potential sources of error or uncertainty and develop a more formal model for calculating the level of certainty for this type of evidence.

THE NEED FOR STANDARDIZATION

> Digital evidence is just another form of "latent" evidence that must be handed with scientific principles and legal boundaries. There is an investigative component for electronic crimes and a laboratory component for the digital evidence associated with those crimes. (Carrie Whitcomb, 2001, "*A Forensic Science Perspective on Digital Evidence Training, Education, and Certification*," National Center of Forensic Science)

In 1994, the O.J. Simpson trial exposed many of the weaknesses of criminal investigation and forensic science. The investigation was hampered from the start with incomplete evidence collection, documentation and preservation at the crime scenes. Arguably, as a result of these initial errors, experienced forensic scientists were confused by and incorrectly interpreted important exhibits, introducing sufficient doubt for the jurors. The controversy surrounding this case made it clear that investigators and forensic scientists were not as reliable as was previously believed, undermining not just their credibility but also that of their profession. This crisis motivated many crime laboratories and investigative agencies to revise their procedures, improve training, and make other changes to avoid similar problems in the future. More recently flaws have been found in the fingerprint and DNA analysis performed by some crime laboratories, calling many convictions into questions and creating doubts about the analytical techniques themselves.

A similar crisis is looming in the area of digital evidence. The lack of generally required standards of practice and training allows weaknesses to

persist, resulting in incomplete evidence collection, documentation and preservation as well as errors in analysis and interpretation of digital evidence. Innocent individuals may be in jail as a result of improper digital evidence handling and interpretation allowing the guilty to remain free. Failures to collect digital evidence have undermined investigations, preventing the apprehension or prosecution of offenders and wasting valuable resources on cases abandoned due to faulty evidence. If this situation is not corrected, the field will not develop to its full potential, justice will not be served, and we risk a crisis that could discredit the field. The only reason we have not already encountered such as crisis is that our mistakes have been masked by obscurity. As more cases become reliant on digital evidence and more attention is focused on it, we must take steps to establish standards of practice and compel practitioners to conform to them.

There have been several noteworthy developments toward standardization in this field. The International Organization of Computer Evidence (www.ioce.org) was established in the mid-1990s "to ensure the harmonization of methods and practices among nations and guarantee the ability to use digital evidence collected by one state in the courts of another state." In 1998, the Scientific Working Group on Digital Evidence (www.swgde.org) was established to "promulgate accepted forensic guidelines and definitions for the handling of digital evidence." In 2001, the first Digital Forensics Research Work Shop (www.dfrws.org) was held, bringing together knowledgeable individuals from academia, military and the private sector to discuss the main challenges and research needs in the field. This workshop also gave new life to an idea proposed several years earlier – a peer-reviewed journal – leading to the creation of the *International Journal of Digital Evidence* (www.ijde.org). In 2003, the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) updated its accreditation manual to include standards and criteria for digital evidence examiners in US crime laboratories. In 2004 the UK Forensic Science Service plans to develop a registry of qualified experts, and several European organizations, including the European Network of Forensic Science Institutes (ENFSI) will publish examination and report writing guidelines for digital investigators. Also, Elsevier will begin publishing Digital Investigation: The International Journal of Digital Forensics and Incident Response (http://www.compseconline.com/digitalinvestigation/).

Historically, Forensic Science disciplines have used certification to oversee standards of practice and training. Certification provides a standard that individuals need to reach to qualify in a profession and provides an incentive to reach a certain level of knowledge. Without certification, the target and rewards of extra effort are unclear. This is not to say that everyone who handles digital evidence requires the same level of skill or training. A strong certification program needs to have tiered levels of certification facilitating

progression upwards, setting basic requirements for crime scene technicians, and setting higher standards for specialists in a laboratory and for investigators who are responsible for analyzing evidence.

Although there are a growing number of certification programs for digital investigators, many are only available to law enforcement personnel and none are internationally accepted. In 2004, representatives from around the world convened to discuss the feasibility of an internationally accepted certification for digital investigators. The outcome is not decided and there are obstacles to such a certification. Some feel that proposed training requirements are too high while others fear that certification will enable anyone to enter the field and obtain specialized knowledge, even individuals who work for the defense on criminal cases. There is also the fear that setting standards and placing additional requirements on practitioners will make it more difficult to get digital evidence admitted in court.

Paradoxically, some of those concerned that training requirements will exclude them also want to exclude individuals who perform criminal defense work. In addition to being unethical, any attempt to withhold knowledge from criminal defense attorneys and experts stifles improvement and progress in the field by allowing misunderstandings and poor practices to persist. If we cannot work together despite our differences to improve the field, the only winners will be the criminals and the losers will be the innocents. The aim of everyone in this field should be to ensure the best reasonable standards and quality. In the long run, digital evidence processed properly by certified professionals is less likely to be impeached or cause an injustice.

The investigation into the Starnet Internet gambling company provides a good example of the successes of proper training and preparation. The August 1999 raid of Starnet's offices in Vancouver, BC, was the culmination of more then a year's worth of investigative effort and preparation by the Royal Canadian Mounted Police. Over 100 personnel from all over Canada were brought together to search and seize Starnet's systems. Search teams were trained to implement standard operating procedures to ensure consistency and were given sufficient equipment to store the large amounts of data that were anticipated. As a result of this planning, Starnet's office building and the network it contained were secured in a few minutes. Although it took several days, digital evidence from more than 80 computers was preserved. In 2001, Starnet pled guilty to violating Section 202 (1) b of the Canadian criminal code by having a machine in Canada for gambling or betting.

Although professionalization may not be desirable for some, it is necessary for all. Without generally accepted standards, there is no basis to judge work. Without certification, there is no basis upon which to assess qualifications. Our community has a duty to agree upon standards of practice and training, and to require practitioners to meet these standards through certification.

> This duty exists because in the forensic disciplines our opinions and interpretations are allowed to impact whether people are deprived of their liberties, and potentially whether they live or die. (Turvey, B., 2000, "*The Professionalization of Criminal Profiling*" *in Criminal Profiling*, Academic Press)

ROADMAP TO THE BOOK

This book draws from four fields: Law, Computer Science, Forensic Science, and Behavioral Evidence Analysis. The 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 a presentation of relevant legal issues and investigative methods in Part 1 (Chapters 1–7). Chapter 1 provides an overview. Chapter 2 (History and Terminology) provides relevant background, history, and terminology. Chapter 3 (Technology and Law) discusses legal issues that arise in computer related investigations, comparing US and European law. Chapter 4 (Investigative Process) discusses a systematic approach to investigating a crime based on the scientific method, providing a context for the remainder of this book. Chapter 5 (Investigative Reconstruction) describes how to use digital evidence to reconstruct events and learn more about the victim and the offender in a crime. Chapter 6 (Technology, MO, and Motive) is a discussion of the relationship between technology and the people who use it to commit crime. Understanding criminal motivation and behavior is key to assessing risks (will criminal activity escalate?), developing and interviewing suspects (who to look for and what to say to them), and focusing investigations (where to look and what to look for). Chapter 7 (Digital Evidence in Court) provides an overview of issues that arise in court relating to digital evidence.

Part 2 of this book (Chapters 8–13) 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 2 deals with specific kinds of computers and ends with a discussion of overcoming password protection and encryption on these systems.

Part 3 (Chapters 14–18) covers computer networks, focusing specifically on the Internet. A bottom-up approach is used to describe computer networks,

starting with the raw data transmitted on networks and progressively building up to the types of data that can be found on networked systems and the Internet. The "top" of a computer network is comprised of 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 appreciate fully the information found 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.

Part 4 of this book (Chapters 19–22) focuses on specific types of investigations starting with Computer Intrusions in Chapter 19. Tools and techniques specific to this type of investigation are presented and detailed case examples are used to demonstrate key points. Chapter 20 covers investigations of Cyberstalking. Chapter 21 details Sexual Predators on the Internet and Chapter 22 discusses computers as alibi.

Part 5 is a short segment that provides guidelines for handling and processing digital evidence. This text does not cover forensic image, video and audio analysis. For information about image/video/audio enhancement and other aspects of this kind of analysis, see Electronic Evidence by Gruber (Gruber 1995).

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. In place of the CD-ROM in the first edition of this book, an interactive Web site (www.disclosedigital.com) provides practical exercises based on actual cases to demonstrate key aspects of investigating computer related crimes and to help the reader apply the concepts in this book to his/her own investigations. This Web site epitomizes a general educational model that others can replicate or borrow from to create inexpensive, educational resources to assist investigators.

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. Competent legal advice should be sought to address the specifics of a case and to ensure that nuances of the law are considered.

PART 1

DIGITAL INVESTIGATION

CHAPTER 1

DIGITAL EVIDENCE AND COMPUTER CRIME

Within the past few years a new class of crime scenes has become more prevalent, that is, crimes committed within electronic or digital domains, particularly within cyberspace. Criminal justice agencies throughout the world are being confronted with an increased need to investigate crimes perpetrated partially or entirely over the Internet or other electronic media. Resources and procedures are needed to effectively search for, locate, and preserve all types of electronic evidence. This evidence ranges from images of child pornography to encrypted data used to further a variety of criminal activities. Even in investigations that are not primarily electronic in nature, at some point in the investigation computer files or data may be discovered and further analysis required.

(Lee *et al.* 2001).

Increasingly, criminals are using technology to facilitate their offenses and avoid apprehension, creating new challenges for attorneys, judges, law enforcement agents, forensic examiners, and corporate security professionals. Organized criminals around the globe are using technology to maintain records, communicate, and commit crimes. Offenders have obtained computer information about a police officer and his family to intimidate and discourage him from confronting them. As a result of the large amounts of drugs, child pornography, and other illegal materials being trafficked on the Internet, the US Customs Cybersmuggling Center has come to view every computer on the Internet in the United States as a port of entry. Felons have even broken into court systems to change their records and monitor internal communications.

CASE EXAMPLE (CALIFORNIA 2003):
William Grace and 22-year-old Brandon Wilson were sentenced to 9 years in jail after pleading guilty to breaking into court systems in Riverside, California, to alter records. Wilson altered court records relating to previous charges filed against him (illegal drugs, weapons, and driving under the influence of alcohol) to indicate that the charges had been dismissed. Wilson also altered court

Digital Evidence and Computer Crime Second Edition
ISBN: 0-12-163104-4

documents relating to several friends and family members. The network intrusion began when Grace obtained a system password while working as an outside consultant to a local police department. By the time they were apprehended, they had gained unauthorized access to thousands of computers and had the ability to recall warrants, change court records, dismiss cases, and read e-mail of all county employees in most departments, including the Board of Supervisors, Sheriff, and Superior Court judges. Investigators estimate that they seized and examined a total of 400 Gbytes of digital evidence (Sullivan 2003).

As more medical machinery, office equipment, home computers and appliances, and handheld devices are networked, there is greater exposure to abuse that could disrupt health care, office, and home life work. Network-based attacks targeting critical infrastructure such as power, health, communications, financial, and emergency response services are becoming a greater concern as terrorists become more technologically proficient.

CASE EXAMPLE (COWEN 2003):
Michael McKevitt was charged with directing terrorist activities. In addition to being accused of involvement in a bombing in Northern Ireland, McKevitt allegedly contacted an FBI informant on behalf of the Real IRA to obtain laptops for bomb detonation, encryption software, and personal digital assistants. McKevitt apparently saw cyberterrorism – the use of the networks to cause panic and loss of life – as the future over bombing and was taking steps to expand his terrorist organization's capabilities in this area. The evidence in the case includes laptops, e-mail messages, and mobile telephone records.

There is a positive aspect to the increasing use of technology by criminals – the involvement of computers in crime has resulted in an abundance of digital evidence that can be used to apprehend and prosecute offenders. For instance, computers played a role in the planning and subsequent investigations of both World Trade Center bombings. Ramsey Yousef's laptop contained plans for the first bombing and, during the investigation into Zacarias Moussaoui's role in the second attack, over 100 hard drives were examined (United States v. Moussaoui; United States v. Salameh *et al.*; United States v. Ramsey Yousef). Realizing the increasing use of high technology by terrorists compelled the United States to enact the USA Patriot Act and motivated the European Union to recommend related measures. E-mail ransom notes sent by Islamists who kidnapped and murdered journalist Daniel Pearl were instrumental in identifying the responsible individuals in Pakistan. In this case, the "threat to life and limb" provision in the USA Patriot Act enabled Internet Service Providers (ISPs) to provide law enforcement with information quickly, without waiting for search warrants.

While paper documents relating to Enron's misdeeds were shredded, digital records persisted that helped investigators build a case. Subsequent

investigations of financial firms and stock analysts have utilized e-mail and other digital evidence to build a case. Realizing the value of digital evidence in such investigations, the Securities and Exchange Commission set an example in December 2002 by fining five brokerage houses a total of $8.25 million for failing to retain e-mail and other data as required by the Securities and Exchange Act of 1934 (SEC 2002).

Digital evidence can be useful in a wide range of criminal investigations including homicides, sex offenses, missing persons, child abuse, drug dealing, and harassment. Also, civil cases can hinge on digital evidence, and digital discovery is becoming a routine part of civil disputes. Computerized records can help establish when events occurred, where victims and suspects were, whom they communicated with, and may even show their intent to commit a crime. Robert Durall's Web browser history showed that he had searched for terms such as "kill + spouse," "accident + deaths," and "smothering" and "murder" prior to killing his wife (Johnson 2000). These searches were used to demonstrate premeditation and increase the charge to first-degree murder. Sometimes information stored on a computer is the only clue in an investigation. In one case, e-mail messages were the only investigative link between a murderer and his victim.

CASE EXAMPLE (MARYLAND 1996):
A Maryland woman named Sharon Lopatka told her husband that she was leaving to visit friends. However, she left a chilling note that caused her husband to inform police that she was missing. During their investigation, the police found hundreds of e-mail messages between Lopatka and a man named Robert Glass about their torture and death fantasies. The contents of the e-mail led investigators to Glass's trailer in North Carolina and they found Lopatka's shallow grave nearby. Her hands and feet had been tied and she had been strangled. Glass pled guilty, claiming that he killed Lopatka accidentally during sex.

Digital data are all around us and should be collected in any investigation routinely. More likely than not, someone involved in the crime used a computer, personal digital assistant, mobile telephone, or accessed the Internet. Therefore, every corporate investigation should consider relevant information stored on computer systems used by their employees both at work and home. Every search warrant should include digital evidence to avoid the need for a second warrant and the associated lost time and evidence. Even if digital data do not provide a link between a crime and its victim or a crime and its perpetrator, they can be useful in an investigation. Digital evidence can reveal how a crime was committed, provide investigative leads, disprove or support witness statements, and identify likely suspects.

This book provides the knowledge necessary to handle digital evidence in its many forms, to use this evidence to build a case, and to deal with

the challenges associated with this type of evidence. This text presents approaches to handling digital evidence stored and transmitted using networks in a way that is most likely to be accepted in court. However, what is illegal, how evidence is handled, received, rejected, and how searches are authorized and conducted varies from country to country. Therefore, it is important to seek legal advice from a competent attorney, particularly since the law is changing to adapt to rapid technological developments.

1.1 DIGITAL EVIDENCE

For the purposes of this text, digital evidence is defined as *any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi* (adapted from Chisum 1999).

Digital evidence has been previously defined as any data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator (Casey 2000). The definition proposed by the Standard Working Group on Digital Evidence (SWGDE) is any information of probative value that is either stored or transmitted in a digital form. Another definition proposed by the International Organization of Computer Evidence (IOCE) is information stored or transmitted in binary form that may be relied upon in court. However, these definitions focus too heavily on proof and neglect data that simply further an investigation. Additionally, the term *binary* in the later definition is inexact, describing just one of many common representations of computerized data.

The data referred to in this definition are essentially a combination of numbers that represent information of various kinds, including text, images, audio, and video. Take a moment to consider the types of digital data that exist and how they might be useful in an investigation. Computers are ubiquitous and digital data are being transmitted through the air around us and through wires in the ground beneath our feet.

The terms digital evidence and electronic evidence are sometimes used interchangeably. However, an effort should be made to distinguish between electronic devices such as mobile telephones and the digital data that they contain. Although this text necessarily covers certain aspects of electronic devices, the focus is on the digital evidence they contain. When considering the many sources of digital evidence, it is useful to categorize computer systems into three groups (Henseler 2000).

Open computer systems: Open computer systems are what most people think of as computers – systems comprised of hard drives, keyboards, and monitors such as laptops, desktops, and servers that obey standards. These systems, with their ever increasing amounts of storage space, can be rich sources of digital evidence. A simple file can contain incriminating information and can have associated properties that are useful in an investigation. For example, details such as when a file was created, who created it, or that it was created on another computer can all be important.

Communication systems: Traditional telephone systems, wireless telecommunication systems, the Internet, and networks in general can be a source of digital evidence. For instance, the Internet carries e-mail messages around the world. The time a message was sent, who sent it, or what the message contained can all be important in an investigation. To verify when a message was sent, it may be necessary to examine log files from intermediate servers and routers that handled a given message. To verify the contents of a message, it may be necessary to eavesdrop on the communication as it occurs.

Embedded computer systems: Mobile telephones, personal digital assistants, smart cards, and many other systems with embedded computers may contain digital evidence. For example, navigation systems can be used to determine where a vehicle has been and Sensing and Diagnostic Modules in many vehicles hold data that can be useful for understanding accidents, including the vehicle speed, brake status, and throttle position during the last five seconds before impact. Microwave ovens are now available with embedded computers that can download information from the Internet and some home appliances allow users to program them remotely via a wireless network or the Internet. In an arson investigation, data recovered from a microwave can indicate that it was programmed to trigger a fire at a specific time.

Given the ubiquity of digital evidence it is the rare crime that does not have some associated data stored and transmitted using computer systems. A trained eye can use these data to glean a great deal about an individual, providing such insight that it is like looking through a stained glass window into the individual's personal life and thoughts. An individual's personal computer and their use of network services are effectively behavioral archives, potentially retaining more information about an individual's activities and desires than even his/her family and closest friends. E-commerce sites use some of this information for direct marketing and a skilled digital investigator can delve into these behavioral archives and gain deep insight into a victim or offender (Casey 2002).

Despite its prevalence, few people are well versed in the evidentiary, technical, and legal issues related to digital evidence and as a result, digital evidence is often overlooked, collected incorrectly, or analyzed ineffectively. The goal of this text is to equip the reader with the necessary knowledge and skills effectively to use digital evidence in any kind of investigation. This text illuminates the technical, investigative, and legal facets of handling and utilizing digital evidence.

1.2 INCREASING AWARENESS OF DIGITAL EVIDENCE

By now it is well known that attorneys and police are encountering progressively more digital evidence in their work. Less obviously, computer security professionals and military decision makers are concerned with digital evidence. An increasing number of organizations are faced with the necessity of collecting evidence on their networks in response to incidents such as computer intrusions, fraud, intellectual property theft, child pornography, stalking, sexual harassment, and even violent crimes.

More organizations are considering legal remedies when criminals target them and are giving more attention to handling digital evidence in a way that

will hold up in court. Also, by processing digital evidence properly, organizations are protecting themselves against liabilities such as invasion of privacy and unfair dismissal claims. As a result, there are rising expectations that computer security professionals have training and knowledge related to digital evidence handling.

System administrators who find child pornography on computers in their workplace are in a perilous position. Simply deleting the contraband material and not reporting the problem may be viewed as criminally negligent. A system administrator who did not muster his employer's support before calling the police to report child pornography placed on a server by another employee was disavowed by his employer, had to hire his own lawyer, testify in his own time, and ultimately find a new job. Well meaning attempts to investigate child pornography complaints have resulted in the system administrator being prosecuted for downloading and possessing illegal materials themselves. Therefore, in addition to being technically prepared for such incidents, it is important for organizations and system administrators to have clear policies and procedures for responding to these problems.

In addition to handling evidence properly, corporations and military operations need to respond to and recover from incidents rapidly to minimize the losses caused by an incident. Many computer security professionals deal with hundreds of petty crimes each month and there is not enough time or resources to open a full investigation for each incident. Therefore, computer security professionals attempt to limit the damage and close each investigation as quickly as possible. There are three significant drawbacks to this approach. First, each unreported incident robs attorneys and law enforcement personnel of an opportunity to learn about the basics of computer-related crime. Instead, they are only involved when the stakes are high and the cases are complicated. Second, computer security professionals develop loose evidence processing habits that can make it more difficult for law enforcement personnel and attorneys to prosecute an offender. Third, this approach results in underreporting of criminal activity, deflating statistics that are used to allocate corporate and government spending on combating computer-related crime.

Balancing thoroughness with haste is a demanding challenge. Tools that are designed for detecting malicious activity on computer networks are rarely designed with evidence collection in mind. Some organizations are attempting to address this disparity by retrofitting their existing systems to address authentication issues that arise in court. Other organizations are implementing additional systems specifically designed to secure digital evidence, popularly called Network Forensic Analysis Tools (NFATs). Both approaches have shortcomings that will be addressed gradually as software designers become more familiar with issues relating to digital evidence.

Government agencies are also interested in using digital evidence to detect terrorist activities and prevent future attacks. As a result, data mining technologies that were previously used to detect and investigate criminal activity that occurred in the past are now being adapted to identify suspicious, but not necessarily criminal, activities. Understandably, the possibility of the government freely sifting through every citizen's personal data for anything that looks suspicious is a privacy advocate's worst nightmare. There is certainly a risk that these pre-crime systems will do more harm than the problems they aim to address.

Ultimately, these systems will not achieve their intended goal because of inadequate training data sets, inaccurate data, high numbers of false positives, and information overload. With detailed knowledge of only several

thousand known terrorists and ignoring the fact that terrorists regularly change their behavior to evade detection, it is statistically impossible to develop data mining methods that can reliably distinguish between normal and suspicious activity. The resulting inaccurate data mining methods would result in false positives that could ruin the lives of thousands, perhaps millions, of innocent individuals. Considering the amount of junk mail that is incorrectly addressed to Mr Eogliam Casey, Mr Bogan Caseui, and Ms Eileen Casey, it is likely that erroneous data in the underlying databases will increase the number of false positives in data mining. Even if data mining stumbled upon one actual terrorist, this lead would probably be lost among the false positives and bureaucracy created by the data mining process. Let us just hope that careless efforts to utilize these powerful data mining technologies do not cause too much damage and inhibit our ability to use them to investigate crimes.

Keep in mind that criminals are also concerned with digital evidence and will attempt to manipulate computer systems to avoid apprehension. Therefore, digital investigators cannot simply rely on what is written in this book to process digital evidence and must extend the lessons to new situations. With this in mind, in addition to presenting specific techniques and examples, this text provides general concepts and methodologies that can be applied to new situations with some thought and research on the part of the reader.

1.3 CHALLENGING ASPECTS OF DIGITAL EVIDENCE

Digital evidence as a form of physical evidence creates several challenges for forensic examiners. First, it is a messy, slippery form of evidence that can be very difficult to handle. For instance, a hard drive platter contains a messy amalgam of data – pieces of information mixed together and layered on top of each other over time. Only a small portion of this amalgam might be relevant to a case, making it necessary to extract useful pieces, fit them together, and translate them into a form that can be interpreted.

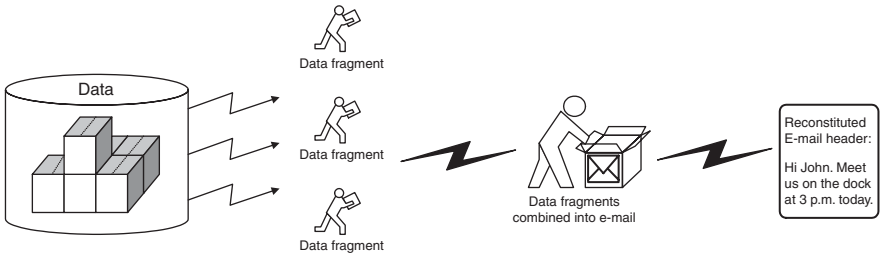

Figure 1.1

Conceptual depiction of data fragments being extracted from a hard drive platter, combined, and translated into an e-mail message.

Similarly, radio waves and microwaves traveling through the air contain a tangle of data, making it necessary to find the desired signal amongst the noise and translate it into the data that can be understood (Figure 1.1). This is conceptually similar to DNA analysis – the relevant information must be extracted from human fluid/tissue, processed, and translated into a form that we understand.

Second, digital evidence is generally an abstraction of some event or digital object. When a person instructs a computer to perform a task such as sending an e-mail, the resulting activities generate data remnants that give only a partial view of what occurred (Venema, Farmer 2000). Unless someone has installed surveillance equipment, individual mouse clicks, keystrokes, internal system commands, and other minutiae are not retained. Only certain results of the activity such as the e-mail message and server logs remain to give us a partial view of what occurred. Even when such minutiae are recorded, the electrical impulses of our mouse button clicks and keyboard depressions must be translated into data before they have any meaning. Similarly, an e-mail message and server log stored on a disk are the result of several layers of abstraction from magnetic fields on the disk to the letters and numbers that we see on the screen. Therefore, we never see the actual data but only a representation, and each layer of abstraction can introduce errors (Carrier 2003).

This situation is similar to that of the traditional crime scene investigation. In a homicide case, there may be clues that can be used to reconstruct events like putting a puzzle together. However, all of the puzzle pieces are never available, making it impossible to create a complete reconstruction of the crime. This book describes various sources of digital evidence and how these multiple, independent sources of corroborating information can be used to develop a more complete picture of the associated crime.

Third, the fact that digital evidence can be manipulated so easily raises new challenges for digital investigators. Digital evidence can be altered either maliciously by offenders or accidentally during collection without leaving any obvious signs of distortion. Fortunately, digital evidence has several features that mitigate this problem.

- Digital evidence can be duplicated exactly and a copy can be examined as if it were the original. It is common practice when dealing with digital evidence to examine a copy, thus avoiding the risk of damaging the original.
- With the right tools it is very easy to determine if digital evidence has been modified or tampered with by comparing it with an original copy.
- Digital evidence is difficult to destroy. Even when a file is "deleted" or a hard drive is formatted, digital evidence can be recovered.
- When criminals attempt to destroy digital evidence, copies and associated remnants can remain in places that they were not aware of.

CASE EXAMPLE (BLANTON 1995):
When Colonel Oliver North was under investigation during the Iran Contra affair in 1986, he was careful to shred documents and delete incriminating e-mails from his computer. However, unbeknown to him, electronic messages sent using the IBM Professional Office System (PROFS) were being regularly backed up and were later retrieved from backup tapes.

Fourth, digital evidence is usually circumstantial making it difficult to attribute computer activity to an individual. Therefore, digital evidence can only be one component of a solid investigation. If a case hinges upon a single form or source of digital evidence such as date–time stamps on computer files, then the case is unacceptably weak. Without additional information, it could be reasonably argued that someone else used the computer at the time. For instance, authentication mechanisms on more secure computers can be bypassed and many computers do not require a password, allowing anyone to use them. Similarly, if a defendant argues that some exonerating digital evidence was not collected from one system, this would only impact a weak case that does not have supporting evidence of guilt from other sources.

CASE EXAMPLE (UNITED STATES v. GRANT 2000):
In an investigation into the notorious online Wonderland Club, Grant argued that all evidence found in his home should be suppressed because investigators had failed to prove that he was the person associated with the illegal online activities in question. However, the prosecution presented enough corroborating evidence to prove their case.

1.4 FOLLOWING THE CYBERTRAIL

Many people think of the Internet as separate from the physical world. This is simply not the case – crime on the Internet mirrors crime in the physical world. There are several reasons for this cautionary note. First, a crime on the Internet usually reflects a crime in the physical world, with human perpetrators and victims and should be treated with the same gravity. To neglect the very real and direct link between people and the online activities that involve them limits one's ability to investigate and understand crimes with an online component. Auction fraud provides a simple demonstration of how a combination of evidence from the virtual and physical worlds is used to apprehend a criminal.

CASE EXAMPLE (AUCTION FRAUD 2000):
A buyer on E-bay complained to police that he sent a cashier's check to that seller but received no merchandise. Over a period of weeks, several dozen similar reports were made to the Internet Fraud Complaint Center against the same seller.

> To hide his identity, the seller used a Hotmail account for online communications and several mail drops to receive checks. Logs obtained from Hotmail revealed that the seller was accessing the Internet through a subsidiary of Uunet. When served with a subpoena, Uunet disclosed the suspect's MSN account and associated address, credit card and telephone numbers. Investigators also obtained information from the suspect's bank with a subpoena to determine that the cashier's checks from the buyers had been deposited into the suspect's bank account. A subpoena to E-bay for auction history and complaints and supporting evidence from each of the buyers helped corroborate the connections between the suspect and the fraudulent activities. Employees at each mail drop recognized a photograph of the suspect obtained from the Department of Motor Vehicles. A subpoena to the credit card company revealed the suspect's Social Security Number and a search of real estate property in the suspect's name turned up an alternate residence where he conducted most of his fraud.

Second, while criminals feel safe on the Internet, they are observable and thus vulnerable. We can take this opportunity to uncover crimes in the physical world that would not be visible without the Internet. Murders have been identified as a result of their online actions, child pornography discovered on the Internet has exposed child abusers in the physical world, and local drug deals are being made online. By observing the online activities of offenders in our neighborhoods, jurisdictions, and companies, we can learn more about the criminal activities that exist around us in the physical world. Third, when a crime is committed in the physical world, the Internet often contains related digital evidence and should be considered as an extension of the crime scene. For instance, a program like Chat Monitor can be used to find individuals from a specific geographical region who are using Internet Relay Chat (IRC) networks to exchange child pornography.

The crimes of today and the future require us to become skilled at finding connections between crimes on the Internet and in the physical world, following the cybertrail if you will. By following the cybertrail, investigators of physical world crime can find related evidence on the Internet and investigators of crime on the Internet find related evidence in the physical world. The cybertrail should be considered even when there is no obvious sign of Internet activity. Criminals are learning to conceal their Internet activities and even the most obvious indication that a computer is used to access the Internet is disappearing: a cable connecting the computer to a jack in the wall. With the rise in wireless networks fewer computers have network cables.

The Internet may contain evidence of the crime even when it was not directly involved. There are a growing number of sensors on the Internet such as cameras showing live highway traffic on the Web as shown in Figure 1.2. These sensors may inadvertently capture evidence relating to a crime. In one investigation of reckless driving that resulted in a fatal crash, the position of the victim's car and average speed was determined using