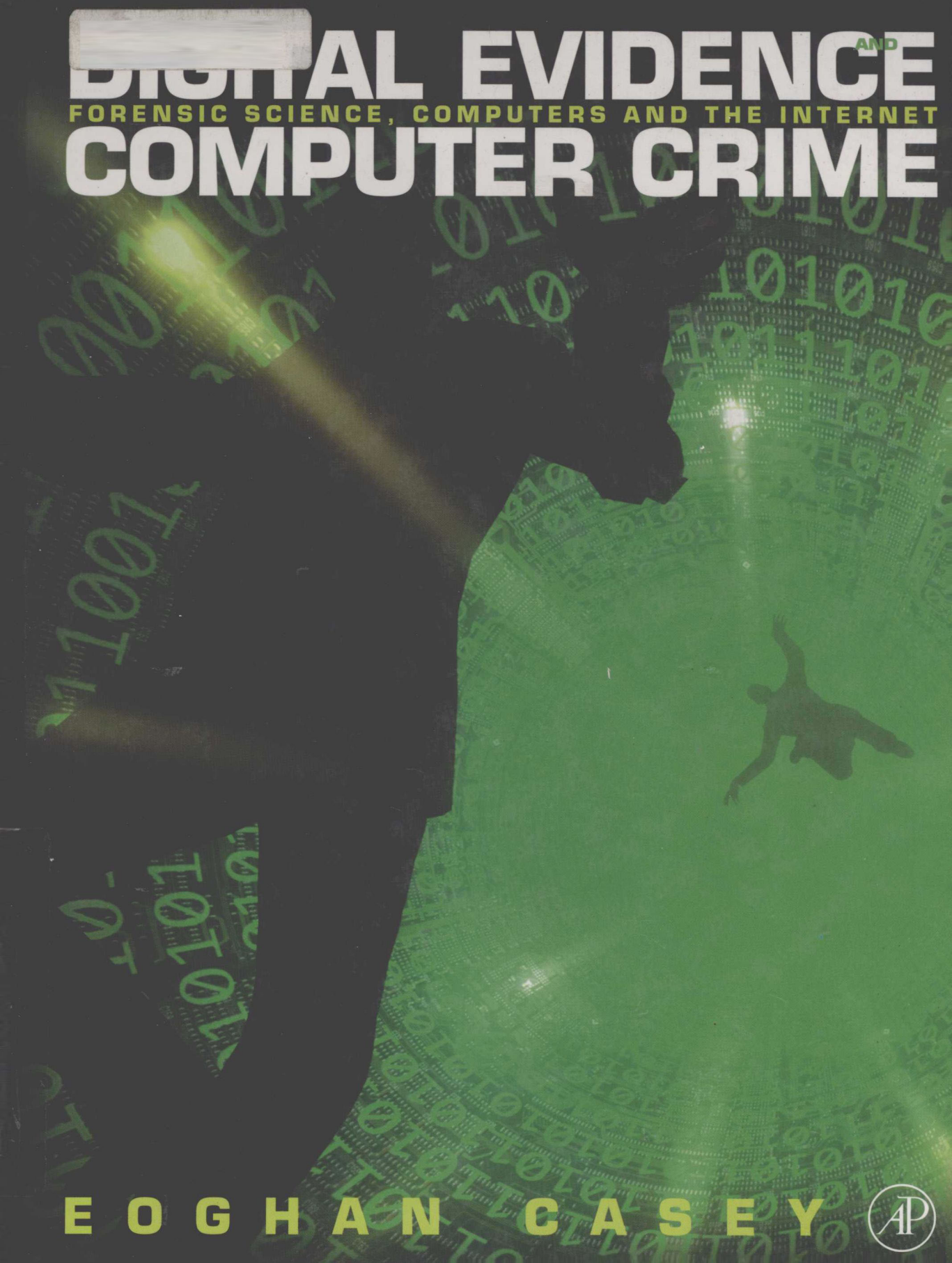
DIGITAL EVIDENCE AND COMPUTER CRIME

FORENSIC SCIENCE, COMPUTERS AND THE INTERNET



EOGHAN CASEY

AP

DIGITAL EVIDENCE AND COMPUTER CRIME

FORENSIC SCIENCE, COMPUTERS AND THE INTERNET

Eoghan Casey

ACADEMIC PRESS

San Diego San Francisco New York Boston
London Sydney Tokyo

This book is printed on acid-free paper

ACADEMIC PRESS
Harcourt Place,
32 Jamestown Road,
LONDON NW1 7BY
http://www.hbuk.co.uk/ap/

ACADEMIC PRESS
A Harcourt Science and Technology Company
525 B Street, Suite 1900, San Diego,
California 92101–4495, USA
http://www.apnet.com

ISBN 0–12–162885–X
CD 0–12–162886–8

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

Typeset by Selwood Systems Typesetting, Bath
Printed in Great Britain by Cambridge University Press, Cambridge

00 01 02 03 04 05 CUP 9 8 7 6 5 4 3 2 1

From our present vantage point, perched at the end of a century filled with innovation and invention, it is clear to most of us that one of that century's most significant and influential inventions was the computer. Surprisingly, that idea might have seemed absurd even as recently as 20 years ago.

The story of computers and computing has been one of evolution of purpose. The stories of other major inventions of this century, such as the automobile, the telephone, the electric light, or the elevator have been tales of success at achieving intended purposes. The automobile transports us more quickly and efficiently than the horse and buggy; the telephone permits us easier, faster communication; the electric light does just that; the elevator facilitated the vertical development of cities. Except for various improvements in efficiency these inventions have remained largely unchanged in purpose and use since their creation. The primary role of today's computers, however, is certainly not what its early inventors envisioned. It has metamorphosed from a giant calculating machine like the thirty-ton ENIAC, to a stand-alone personal tool for performing assorted routine tasks like word-processing and bookkeeping, to today's networked device permitting virtually instantaneous and global personal, corporate, and governmental interaction. The calculating machine has become the portal to a new world of human activity, a world different in so many essential ways from our everyday world that we have dubbed this new place 'cyberspace.'

Yet, cyberspace is, in the end, a place populated by humans, or perhaps more correctly, by human minds, since it is our intellects that reside and meet one another there. It should come as no surprise, then, that many of the problems of the 'real' world carry over into this new realm. Crime is one of them.

The Internet (a term which once referred to a specific set of networked computers but which has now increasingly come to mean the global network of computers) is growing so quickly that it is impossible to know at any given moment the actual number of computers connected to it. It is even less possible to determine the number of people with access to it. But use of the

Internet is clearly growing very, very quickly, and so is computer crime and the need to control it.

Some cyberspace crimes, such as unauthorized access to a computer, are new and specific to the online world. Others, such as fraud or theft of valuables, are familiar from the real world. In either case, the disembodied, often anonymous nature of activity in cyberspace creates problems in enforcing laws. Evidence, of course, is the foundation for identifying, catching, and prosecuting criminals. Forensic Science has developed well-understood techniques for dealing with real-world evidence, but how can these methods be applied in cyberspace? What must investigators do to collect, preserve, and authenticate digital evidence? How can legal admissibility of digital evidence be assured? How can digital evidence be used to reconstruct crimes and generate leads?

Many, perhaps most, of the police, lawyers, programmers or systems administrators, and forensic scientists involved in the investigation or prosecution of computer-related crimes do not know the answer to these questions. This book will tell them. It should, of course, be equally interesting to lawyers with the task of defending alleged computer criminals, since it provides a detailed guide to possible procedural weaknesses in the prosecution's evidence.

In this book, Eoghan Casey has provided a much needed 'nuts and bolts' guide to dealing with digital evidence, with step-by-step instructions for dealing with an assortment of evidentiary problems. However, and to my mind at least as importantly, Casey illustrates how these details fit within the broader contexts of forensic science, crime, and society in general, never omitting mention of the potential downsides of detection and detectability. So, for example, the difficult balancing act between a secure computing environment and individual privacy is made clear.

Nor does Casey ever lose sight of the counter-intuitive importance of the human element in a world of intangible activity, and of the ways in which the nature of digital evidence and activity in cyberspace may alter or augment the rules of real-world behavioral analysis. For example, in any crime, the victim, and the choice of that victim, can provide important clues regarding the identity or a profile of the criminal. Investigators therefore devote considerable energy to analyzing a victim's habits and activities. In cases of cyberstalking or computer harassment, the need to examine digital evidence related to the victim's activities is clear. But Casey reminds us here that digital evidence can play an important role in assessing a victim's behavioral pattern when investigating real-world crime as well, particularly if the victim is a frequent visitor to cyberspace. The unaware investigator may overlook the fact that people's cyberspace personalities are sometimes extraordinarily

different than those presented to the real world. The anonymity possible in cyberspace provides a tempting opportunity to assume other identities, to play out other lives and fantasies. When these alter egos are of a particular 'high-risk' nature and spill over into the real world, the consequences can be tragic, as is illustrated by one case study presented here.

The investigation of computer crime requires a team effort of police, forensic scientists, lawyers, and programmers or systems administrators. No single individual is likely to have the requisite skill sets. Police can generally be expected to know how to oversee an investigation, but may not know much about computers and computing and thus not know what evidence to look for. Programmers and systems administrators may know a great deal about computers, networks, and how they work, but nothing about legal procedural requirements regarding the collection and preservation of evidence. Forensic scientists may know how to deal with evidence but, like the police, may not know what to look for when dealing with digital evidence or how to apply real-world forensic science methods to it. Lawyers may know about the law of evidence but not much else. Together, however, this team can know how to conduct an investigation of a computer crime, what evidence to look for, how to find it, and how to treat it so as to preserve its admissibility once it is found.

The danger in dealing with digital evidence is that the absence or ignorance of one or more members of this hypothetical investigatory team will lead to evidence being overlooked or rendered legally useless. This book addresses that danger by making police, forensic scientists, lawyers, and programmers aware of what they do not know. It is an important contribution and should be required reading for anyone involved either in criminal investigation or computer administration.

Robert L. Dunne, J.D.
Co-Director, The Center for Internet Studies
Lecturer, Department of Computer Science
Yale University

PREFACE

In the past thirty years, there has been a dramatic shift in the way computers are used. Previously, computer technology was seen simply as a tool, used selectively for a specific purpose. Now, however, the very infrastructure of society relies on computers and there is only a vague awareness of their prevalence and multifarious functions. Financial networks, communication systems, power stations, medical facilities, modern automobiles and appliances all depend on computers, and these computers can record withdrawals, deposits, purchases, telephone calls, usage of electricity, medical treatments, driving patterns, the time an individual awakes, and much more. In addition to the computers that form our infrastructure, individuals use personal computers regularly for convenience, education and entertainment – typing letters, managing personal finances, exploring educational CD-ROMs and playing computer games. Furthermore, personal computers are connected to networks to take advantage of a wide range of network services including e-mail and the World Wide Web. Computer networks extend the reach and control of the individuals, giving them great freedom and power to be creative – and destructive.

It should come as no surprise that computer technology is involved in a growing number of crimes. In addition to being used as a tool to perpetrate crimes (e.g. computer intrusion, stalking, harassment, and fraud), computers can contain evidence related to any crime, including homicide and rape. It is no longer sufficient to have a few experts familiar with evidence stored on and transmitted using computers. Any investigation can involve computers or networks and everyone involved in a criminal investigation or prosecution can benefit from knowledge of the associated technical, legal and evidentiary issues related to this technology.

This text is written for the computer security professionals, law enforcement officers, attorneys and forensic scientists who are making efforts to become more familiar with the technical, legal, evidentiary and behavioral aspects of investigating computer-related crime. Although these professional groups have similar goals, there is a large amount of distrust and conflict between them. Computer security professionals who are employed

to minimize the impact that an investigation has on an organization often come into conflict with law enforcement officers who are responsible for exploring every lead and examining every detail. Computer security professionals view law enforcement officers as heavy-handed and law enforcement officers see computer security professionals as unhelpful and even resistant. Also, computer security professionals who are already familiar with the particular system often perceive law enforcement officers, attorneys and forensic scientists who do not have a clear understanding of computer technology as technically inept. There are many other sources of conflict between these groups that can interfere with an investigation.

The expertise of each group is required for the successful investigation and prosecution of computer-related crime. Law enforcement officers, attorneys and forensic scientists depend on computer security professionals to help them collect and interpret evidence in technically challenging situations. Computer security professionals, attorneys and forensic scientists depend on law enforcement officers to coordinate investigations. Attorneys provide legal guidance and forensic scientists provide tools and techniques for getting the most out of available evidence. Therefore, it is important for these professional groups to gain a better understanding of each other and to work in collaboration. If these groups do not collaborate, criminals will continue to escape capture and prosecution and will feel justifiably safe using computers and networks to facilitate their criminal activities.

Although computer security professionals are primarily responsible for protecting information that is stored on their computer systems, they are often responsible for investigating and resolving criminal activity on their networks with minimum disruption to the users of the system. In the past, collecting evidence was not a priority for computer security professionals. However, victims of computer-related crime are becoming more interested in pressing charges and there is an increasing pressure on computer security professionals to collect evidence to be accepted in court. When computer security professionals are compelled to collect evidence from their networks, it is important that they abide by applicable privacy laws and rules of evidence. If computer security professionals collect evidence illegally, they can be sued. If they do not collect evidence in a way that meets the legal requirements, the evidence might not be accepted in court and their efforts will be wasted.

Law enforcement officers are responsible for responding to complaints, looking for evidence, determining if a crime has been committed and obtaining authorization to gather and examine evidence. In some cases, law enforcement officers rely on computer security professionals to collect evidence from computers and networks but in certain situations the officers

are required to search for and collect evidence themselves. Law enforcement officers encounter personal computers at crime scenes that contain a large amount of evidence. Additionally, the Internet often contains information about suspects, victims and even the crime itself.

Whether at a crime scene or in a corporate environment, law enforcement officers must adjust quickly to an unfamiliar computing environment. A solid understanding of the technical, legal and evidentiary aspects of computers and networks is required to adjust to these unfamiliar settings, locate sources of evidence quickly, obtain necessary assistance or authorization to search for and seize evidence, and collect evidence in a way that will be accepted in court.

Both defense and prosecuting attorneys are responsible for protecting their clients' interests. Since computers are almost as common as file cabinets and can be involved in any case, it is not sufficient to have a few attorneys familiar with computer technology. All attorneys should be comfortable dealing with evidence stored on and transmitted using computers. Defense attorneys need to recognize and make use of exculpatory evidence and prosecuting attorneys need to recognize and make use of incriminating evidence. Also, defense and prosecuting attorneys will be at a loss if they are not acquainted with the common arguments regarding evidence obtained from computers.

As computer security professionals, law enforcement officers and attorneys become more familiar with computers and networks as a source of evidence, the expectations regarding its collection and processing are increasing. Attorneys are becoming more adept at challenging evidence so the individuals who collect and process evidence are becoming more circumspect. Already, the demand for improved tools and techniques for processing computer-related evidence is increasing. Forensic scientists are in a position to meet this demand.

This text is written with the hope that this diverse audience can learn to tolerate each other and cooperate sufficiently to address the mounting problems of computer-related crime effectively. To emphasize this common goal, the term *investigator* is used throughout this text to refer to members of the computer security, law enforcement, legal and forensic science communities who investigate computer-related crime.

This text grew out of my work with Knowledge Solutions. I owe special thanks to Brent Turvey and Barbara Troyer-Turvey for their continued assistance and friendship. Without them, this work would not have been possible. Thank you, Brent, for demonstrating that you can investigate heinous crimes and be subjected to defamation and unprofessional criticism without becoming cynical and callous. Admirably, you have used your understanding of diabolical human behavior to improve yourself. Thank you, Barbara, for your kindness and tireless exertions in support of my teaching and writing. You are the calm at the eye of the storm.

This work spent its formative years in New York University. I would like to thank Paul Henry, Donald Payne and Francine Shuchat-Shaw for their insights and guidance. My deep appreciation goes out to my good friend Hon-Chih Chen for his assistance developing the CD-ROM. Also, I would like to thank Gene DeLibero and Tim O'Connor for their willingness to share their extensive knowledge and experience.

I am continually grateful to Yale University for providing me with the opportunity to exercise and refine my interests and skills. It is a joy to work with a knowledgeable and supportive group of people and I am particularly thankful to H. Morrow Long for his unfathomable perspicacity and regular tutelage. I am also beholden to Robert Dunne for expanding my view of cybercrime, deepening my knowledge of the law, and repeatedly assisting me at pivotal points in my career.

I would like to thank the folks at Academic Press for their encouragement, continuing support, and tireless efforts to complete and disseminate this work. In particular, I would like to thank Nick Fallon for initiating this adventure and for sticking by us through all of the rough patches.

I am indebted to Kathy Baken for her stunning design on the cover of this book – may your creative well never run dry. I am also indebted to Jim Casey and Irena Herskowicz for their contributions without which the CD-ROM might not have come to fruition.

My mother Ita O'Connor deserves special mention for her initial critique of this work and her enduring encouragement. Thank you for making

reconstructive surgery seem like a walk in the park. Finally, I give my endless gratitude and love to my wife Genevieve for her patience, kindness and stability. I expect to have the opportunity to return the favors during your upcoming projects.

CONTENTS

FOREWORD		vii
PREFACE		xi
ACKNOWLEDGEMENTS		xv
CHAPTER 1	INTRODUCTION TO DIGITAL EVIDENCE	1
2	THE LANGUAGE OF CYBERCRIME	15
3	*MODUS OPERANDI*, MOTIVE AND TECHNOLOGY	25
4	APPLYING FORENSIC SCIENCE TO COMPUTERS	41
5	DIGITAL EVIDENCE ON COMPUTER NETWORKS	75
6	DIGITAL EVIDENCE ON THE INTERNET	99
7	DIGITAL EVIDENCE AT THE TRANSPORT AND NETWORK LAYERS	121
8	DIGITAL EVIDENCE ON THE DATA-LINK AND PHYSICAL LAYERS	145
9	USING DIGITAL EVIDENCE AND BEHAVIORAL EVIDENCE ANALYSIS IN AN INVESTIGATION	161
10	COMPUTER CRACKERS	171
11	CYBERSTALKING	187
12	DIGITAL EVIDENCE AS ALIBI	199
13	LAWS, JURISDICTION, SEARCH AND SEIZURE	207
14	THOUGHTS FOR THE FUTURE	223
APPENDIX I	SUMMARY OF RESOURCES	231
APPENDIX II	MULTIMEDIA SUPPLEMENT	243
GLOSSARY		257
AUTHOR INDEX		267
SUBJECT INDEX		269

CHAPTER 1

INTRODUCTION TO DIGITAL EVIDENCE

The term *digital evidence* encompasses any and all digital 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[1]. Digital data is essentially a combination of numbers that represent information of various kinds, including text, images, audio and video. With the increasing use of computers, digital evidence is becoming more common and more important to investigative efforts. 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.

[1] *This definition is adapted from the definition of physical evidence in (Saferstein 1998).*

CASE EXAMPLE

In October 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 pleaded guilty, claiming that he killed Lopatka accidentally during sex.

There are large amounts of digital evidence all around us. A hard drive can store a small library, digital cameras can store hundreds of high-resolution photographs, and a computer network can contain a vast amount of information about people and their behavior (Casey 1999). At any given moment, private telephone conversations, financial transactions, confidential documents, and many other kinds of information are moving around us, through the surrounding air and wires in digital form – all potential sources of digital evidence. However, few investigators 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 you, the

reader, with the necessary knowledge and skills to effectively use digital evidence in any kind of investigation.

OVERVIEW OF THIS WORK

The ultimate aim of this text is to demonstrate how digital evidence can be used to identify suspects, prosecute the guilty, defend the innocent, and understand criminal behavior and motivation. To reach this end, three fields are drawn from: computer science, forensic science, and behavioral evidence analysis (Turvey 1999). 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 (Chapter 9).

This text 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. Several scenarios and a general set of guidelines are provided to help transfer the knowledge out of this text and apply it to investigations.

The remainder of the text covers computer networks, focusing on the Internet specifically. A top-down approach is used to describe computer networks, starting with a general overview and progressively going into more detail. 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 is, therefore, an excellent place to start learning about computer networks as a source of digital evidence. The underlying complexity of computer networks is gradually explored until you reach the "bottom" – the physical media (e.g. copper and fiber optic cables) that carry data between computers.

The basic forensic science concepts that are described early on in relation to a single computer are carried through to each layer of the Internet to give you an understanding of digital evidence on computer networks. Seeing concepts from forensic science applied in a variety of contexts will help you 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.

As well as providing a practical understanding of how computer networks function and how they can be used as evidence of a crime, this text presents

relevant legal issues and behavioral evidence analysis, a systematic approach to focusing investigations and understanding criminal motivation. 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).

Case examples are interspersed throughout to emphasize important points and demonstrate the usefulness of digital evidence. Also, scenarios provide a practical understanding of digital evidence. The hope is that, after reading this text, you will have a solid comprehension and a basic working knowledge of digital evidence.

FORENSIC SCIENCE

Forensic science is a core component of this text, providing principles and techniques that facilitate the investigation and prosecution of criminal offenses. Generally speaking, forensic science is the application of science to law – any scientific principle or technique that can be applied to identifying, recovering, reconstructing, or analyzing evidence during a criminal investigation is part of forensic science. The scientific principles behind evidence processing are well established and are used in such procedures as:

- detecting, processing and examining fingerprints and DNA;
- ascertaining the authenticity and source of a questioned document or examining charred documents for evidence of a crime;
- determining a firearm's unique characteristics;
- recovering damaged or deleted documents from a computer hard drive;
- making an exact copy of digital evidence – ensuring that no information is lost during collection;
- collecting digitized data that is being transmitted through networks in a way that preserves its integrity and authenticity;
- using a message digest algorithm to verify that digital evidence has not been modified;
- signing digital evidence digitally to affirm that it is authentic and to preserve chain of evidence;
- determining the unique characteristics of a piece of digital evidence (e.g. documents, programs, transmissions).

In addition to using scientific techniques and theories to process individual pieces of digital evidence, forensic scientists use their training to help investigators reconstruct crimes and generate leads. Applying the scientific

method, forensic scientists analyze available evidence, create hypotheses about what occurred to create the evidence, and perform tests to confirm or contradict their hypotheses. Through this process, forensic scientists can generate strong possibilities about what occurred[2].

[2] *In forensic science, certainty is a word that is used with great care. Forensic scientists cannot be certain of what occurred at a crime scene because they only have a limited amount of information. Therefore, they can only present possibilities based on that limited amount of information.*

One of the fundamental principles in forensic science that is extremely useful for crime reconstruction and linking an offender to a crime is Locard's Exchange Principle, depicted in Figure 1.1. According to this principle, anyone, or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they depart. In the physical world, an offender might inadvertently leave a hair at the scene and take a fiber from the scene. With one of these pieces of evidence, investigators can demonstrate the strong possibility that the offender was at the crime scene. With two pieces of evidence the link between the offender and crime scene becomes stronger and easier to demonstrate.

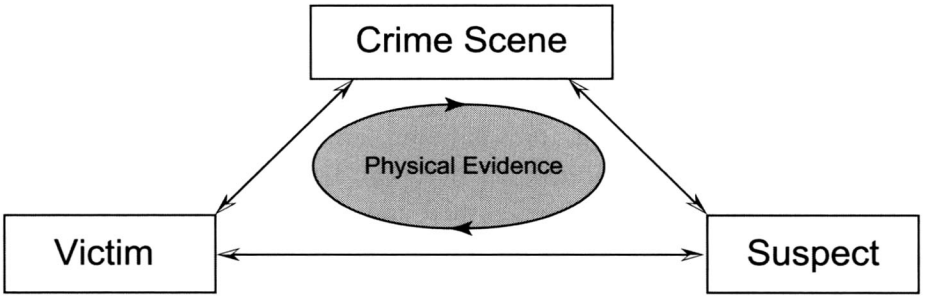


Figure 1.1
Locard's Exchange Principle.

In short, forensic science provides tools, techniques and a systematic (scientific) approach that can be used to process and analyze digital evidence and use this evidence to reconstruct what occurred during the perpetration of a crime with the ultimate purpose of linking an offender, victim and crime scene.

DIGITAL EVIDENCE VERSUS PHYSICAL EVIDENCE

Digital evidence is a type of physical evidence. Although digital evidence is less tangible than other forms of physical evidence (e.g. fingerprints, DNA, weapons, computer components), it is still physical evidence. Digital evidence is made of magnetic fields and electronic pulses that can be collected and analyzed using special tools and techniques. Furthermore, courts have held that such intangible property can be seized as evidence. Digital evidence actually has several advantages over other kinds of physical evidence:

- It 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 the original.
- It is relatively difficult to destroy. Even if it is "deleted," digital evidence can be recovered from a computer disk.
- When criminals attempt to destroy digital evidence, copies can remain in places that they were not aware of.

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

Computers can perform millions of operations based on this digitized information in one second, and can transmit them around the world in an instant. The fact that digital evidence can be manipulated and transmitted so easily raises new challenges for investigators of crimes that involve computers. This text addresses these challenges and emphasizes the positive aspects of digital evidence.

CRIMINAL ACTIVITY AND DIGITAL EVIDENCE ON COMPUTER NETWORKS

Computer networks facilitate daily activities – including telephone calls, credit card purchases, and money withdrawals from ATMs – bringing increasing convenience to our lives. However, along with convenience comes risk and complexity. Computer networks have been involved in a wide range of crimes including child pornography, solicitation of minors, stalking, harassment, fraud, espionage, sabotage, theft, privacy violations, and defamation. Criminals are taking advantage of new technology so quickly that investigators are finding it difficult to keep up – as Carter and Katz point out:

> Law enforcement has withstood many challenges over the years. Prohibition, organized crime, riots, drug trafficking, and violent crime exemplify some of the complex problems the police have faced. Now law enforcement confronts another problem that is somewhat unusual – computer-related crime.
>
> Several factors make this type of criminality difficult to address. Lawbreakers have integrated highly technical methods with traditional crimes and developed creative new types of crime, as well. They use computers to cross state and national boundaries electronically, thus complicating investigations. Moreover, the evidence of these crimes is neither physical nor human but, if it exists, is little more than electronic impulses and programming codes.
>
> Regrettably, the police have fallen behind in the computer age and must overcome a