

COMPUTER FORENSICS

Cybercriminals, Laws, and Evidence



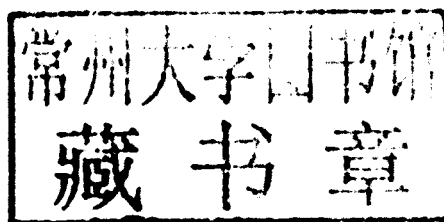
MARIE-HELEN MARRAS

COMPUTER FORENSICS

Cybercriminals, Laws, and Evidence

MARIE-HELEN MARAS, PhD

Assistant Professor of Criminal Justice
State University of New York—Farmingdale



JONES & BARTLETT
LEARNING

World Headquarters

Jones & Bartlett Learning
40 Tall Pine Drive
Sudbury, MA 01776
978-443-5000
info@jblearning.com
www.jblearning.com

Jones & Bartlett Learning
Canada
6339 Ormindale Way
Mississauga, Ontario L5V 1J2
Canada

Jones & Bartlett Learning
International
Barb House, Barb Mews
London W6 7PA
United Kingdom

Jones & Bartlett Learning books and products are available through most bookstores and online booksellers. To contact Jones & Bartlett Learning directly, call 800-832-0034, fax 978-443-8000, or visit our website, www.jblearning.com.

Substantial discounts on bulk quantities of Jones & Bartlett Learning publications are available to corporations, professional associations, and other qualified organizations. For details and specific discount information, contact the special sales department at Jones & Bartlett Learning via the above contact information or send an email to specialsales@jblearning.com.

Copyright © 2012 by Jones & Bartlett Learning, LLC

All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the copyright owner.

Production Credits

Publisher, Higher Education: Cathleen Sether
Acquisitions Editor: Sean Connelly
Senior Associate Editor: Megan R. Turner
Production Manager: Jenny L. Corriveau
Associate Production Editor: Jill Morton
Associate Marketing Manager: Lindsay White
Manufacturing and Inventory Control Supervisor: Amy Bacus
Composition: DataStream Content Solutions, LLC
Cover Design: Kristin E. Parker
Photo Research and Permissions Supervisor: Christine Myaskovsky
Cover Image: Abstract of fingerprint on monitor, © Saniphot/Dreamstime.com; Abstract of human figures with numbers, © Kts/Dreamstime.com
Chapter Opener Image: © Pixel 4 Images/Shutterstock, Inc.
Printing and Binding: Malloy Incorporated
Cover Printing: Malloy Incorporated

Library of Congress Cataloging-in-Publication Data

Maras, Marie-Helen, 1979–

Computer forensics : cybercriminals, laws, and evidence / by Marie-Helen Maras.
p. cm.

Includes bibliographical references and index.

ISBN-13: 978-1-4496-0072-3

ISBN-10: 1-4496-0072-7

1. Electronic evidence—United States. 2. Computer crimes—Investigation—United States. I. Title.
KF8947.5.M37 2011
363.25'9680973—dc22

2010050880

6048

Printed in the United States of America
15 14 13 12 11 10 9 8 7 6 5 4 3 2 1

COMPUTER FORENSICS

DEDICATION

*Χαίροις της Αιγύπτου θεῖος βλαστός, χαίροις Γερανείων θεοδώρητος θησαυρός,
Χαίροις Λουτρακίου και πάσης Κορινθίας, αντίληψις και κλέος, Ἅγιε Πατάπιε.*



In loving memory of my father, Pete Maras (Petōulis).
Thank you for the best 28 years of my life—of unconditional love, laughter, and adventure.

PREFACE

Computer forensics cannot be divorced from the law. A computer forensics investigator needs knowledge of the law to effectively do his or her job. Meanwhile, legal professionals working on cybercrimes must have knowledge of the hardware, software, and technology involved in computer forensics to effectively do their jobs.

The available textbooks on computer forensics are either too technical, placing too much emphasis on the hardware and software used, or too thick in legal analysis, to the extent that a comprehensive background in law is required for their review. There is currently no textbook in the market that falls somewhere in between these two extremes—a book that is tailored to, and can be used by, the individual who does not have a comprehensive legal and technical background. This textbook seeks to fill this void in the literature.

This book is intended to appeal to a wide range of groups. By steering away from both a thicket of legal terms and realms of technical analysis, it seeks to interest a much broader audience of writers and researchers working on computer forensics. Moreover, by providing a concise yet sufficiently detailed account of the most significant and current developments in computer forensics and their implications for a number of different fields (e.g., computer science, law, public policy and administration, security, and criminology), it is likely to prove an extremely useful resource for academics, practitioners, and graduate and undergraduate students in these areas. Criminal justice and socio-legal scholars and professionals should also find food for thought in this work.

Given that this textbook covers the technology and software currently used in the field, it will be of interest to law enforcement agencies and professionals working as computer forensics specialists.

Specifically, this book is intended for the following audiences:

- Law enforcement agents seeking to expand their knowledge of investigations to the field of computers
- Students and professionals seeking a career in computer forensics investigations
- Computer forensics specialists concerned about the legality of searches and evidence seizure, storage, transport, and evaluation
- Legal professionals seeking to understand computer forensics investigations, rules concerning electronic evidence, and the admissibility of this evidence in court
- Computer specialists in the private sector who may be required by courts or law enforcement agents—sometime in the future—to search, restore, transmit, copy, or store electronic data during a computer forensics investigation

Anyone interested in learning about computer forensics, investigations, and electronic evidence will also benefit from this textbook.

The computer forensics field is gaining prominence because of the current worldwide media coverage of cybercrimes and cybercriminals. This textbook will also be relevant to civil liberties groups and professional associations, as news of extradition of cybercriminals and the acceptance of the use of hearsay evidence in computer crime cases is becoming a more common practice.

Finally, this textbook is intended for students in computer forensics courses. It is also intended for students in legal courses who are seeking an introduction to the technology involved in computer forensics investigations and the technical and legal difficulties involved in searching, extracting, maintaining, and storing electronic evidence, while simultaneously looking at the legal implications of such investigations and the rules of legal procedure relevant to electronic evidence.

Supplements

This textbook is accompanied by a series of valuable supplements. An instructor's manual (with Microsoft® PowerPoint® slides) is available to assist instructors in teaching computer forensics and other cybercrime courses. Additionally, a TestBank containing discussion questions and practical exercises is provided to stimulate the critical thinking skills.

ACKNOWLEDGMENTS

I would like to warmly thank Sean Connelly, Megan Turner, and Jill Morton at Jones & Bartlett Learning for all of their direction and assistance during the development and production of this textbook. Additionally, I am grateful to my former thesis supervisor at the University of Oxford, Dr. Lucia Zedner, for her continuous support and encouragement. I thank you for making my experience at Oxford truly memorable and for continuing to cheer me on long after graduation. I would also like to thank my former professors at the Center for Criminology at the University of Oxford for making my learning experience unforgettable. Last and by no means least, I am especially grateful to John Kostanoski, Chair of the Criminal Justice Department at Farmingdale State College, State University of New York, for his guidance toward my professional development.

On behalf of Jones & Bartlett Learning, we would like to thank the following people for their valuable insight in the review of the text:

Qinghai Gao, Farmingdale State College at SUNY

Camille Gibson, Praire View A&M University

Robert Haack, Suffolk County Community College

Raymond Hsieh, California University of Pennsylvania

Alexander Muentz, Temple University

BRIEF CONTENTS

Chapter 1	Entering the World of Cybercrime.	1
Chapter 2	An Introduction to Computer Forensics Investigations and Electronic Evidence.	27
Chapter 3	Laws Regulating Access to Electronic Evidence	51
Chapter 4	Searches and Seizures of Computers and Electronic Evidence	75
Chapter 5	Cybercrime Laws: Which Statute for Which Crime?	99
Chapter 6	Understanding the Computer-Networking Environment: Beware of the Scam Artists, Bullies, and Lurking Predators!	131
Chapter 7	Where Is the Electronic Evidence and Which Tools Can We Use to Find It?	169
Chapter 8	Crime and Incident Scene: What Should an Investigator Do?	199
Chapter 9	Corporate Crimes and Policy Violations Involving Computers: How to Conduct a Corporate Investigation	223
Chapter 10	E-mail Forensics	247
Chapter 11	Network Forensics: An Introduction	269
Chapter 12	Mobile Phones and PDAs in Computer Forensics Investigations.	293
Chapter 13	The Pretrial and Courtroom Experiences of a Computer Forensics Investigator	321

CONTENTS

Preface	xiii
Acknowledgments	xv

Chapter 1	Entering the World of Cybercrime	1
------------------	---	----------

<i>Cybercrime: Defined</i>	1
<i>Cybercrime Versus Traditional Crime</i>	2
<i>Cybercrime Categories</i>	5
<i>Combating Cybercrime</i>	19
<i>Chapter Summary</i>	19
<i>Key Terms</i>	20
<i>Practical Exercise</i>	20
<i>Critical Thinking Question</i>	20
<i>Review Questions</i>	21
<i>Footnotes</i>	21

Chapter 2	An Introduction to Computer Forensics Investigations and Electronic Evidence	27
------------------	---	-----------

<i>Computer Forensics: What Is It?</i>	27
<i>Computer Forensics Investigations: The Basics</i>	28
<i>Computer Forensics Investigations: A Four-Step Process</i>	32
<i>Electronic Evidence: What Is It?</i>	35
<i>Types of Evidence</i>	36
<i>Authentication of Evidence</i>	43
<i>Standards of Evidence</i>	45
<i>Chapter Summary</i>	45
<i>Key Terms</i>	46
<i>Practical Exercise</i>	46
<i>Review Questions</i>	47
<i>Footnotes</i>	47

Chapter 3	Laws Regulating Access to Electronic Evidence	51
------------------	--	-----------

<i>Telecommunications and Electronic Communications Data</i>	51
<i>The Statutory Background of Privacy Protection and Government Access to Data</i>	53
<i>Chapter Summary</i>	68
<i>Key Terms</i>	69
<i>Practical Exercise</i>	69
<i>Critical Thinking Questions</i>	70
<i>Review Questions</i>	71
<i>Footnotes</i>	71

Chapter 4	Searches and Seizures of Computers and Electronic Evidence	75
	<i>What Is Privacy and Why Is It Important?</i>	75
	<i>Constitutional Source of Privacy Protection:</i> <i>The Fourth Amendment</i>	77
	<i>Search Warrants</i>	81
	<i>Searching the Computer for Evidence</i>	88
	<i>Chapter Summary</i>	92
	<i>Key Terms</i>	93
	<i>Critical Thinking Questions</i>	93
	<i>Review Questions</i>	93
	<i>Footnotes</i>	94
Chapter 5	Cybercrime Laws: Which Statute for Which Crime?	99
	<i>Computer Threats and Intrusions</i>	99
	<i>Financial Crimes and Fraud</i>	106
	<i>Intellectual Property Theft and Economic Espionage</i>	115
	<i>Personal Crimes</i>	119
	<i>Chapter Summary</i>	122
	<i>Key Terms</i>	122
	<i>Critical Thinking Questions</i>	123
	<i>Review Questions</i>	123
	<i>Footnotes</i>	124
Chapter 6	Understanding the Computer-Networking Environment: Beware of the Scam Artists, Bullies, and Lurking Predators!	131
	<i>Scams and Scam Artists</i>	131
	<i>Identity Theft</i>	142
	<i>Cyberbullying</i>	149
	<i>Child Exploitation Online</i>	154
	<i>Chapter Summary</i>	161
	<i>Key Terms</i>	161
	<i>Practical Exercise</i>	162
	<i>Review Questions</i>	162
	<i>Footnotes</i>	163
Chapter 7	Where Is the Electronic Evidence and Which Tools Can We Use to Find It?	169
	<i>The Location of Electronic Evidence</i>	169
	<i>Tools Used to Search and Collect Electronic Evidence</i>	190
	<i>Chapter Summary</i>	193
	<i>Key Terms</i>	194
	<i>Practical Exercises</i>	194
	<i>Critical Thinking Question</i>	194

<i>Review Questions</i>	195
<i>Footnotes</i>	195

Chapter 8	Crime and Incident Scene: What Should an Investigator Do?	199
------------------	--	------------

<i>Conducting an Investigation</i>	199
<i>Special Considerations for Cybercrime Investigations</i>	204
<i>Identifying Evidence</i>	206
<i>Analysis of Evidence</i>	207
<i>How to Handle Evidence in an Investigation</i>	208
<i>Hypothetical Criminal Investigation</i>	210
<i>Extracting Electronic Evidence</i>	214
<i>Chapter Summary</i>	219
<i>Key Terms</i>	219
<i>Critical Thinking Questions</i>	220
<i>Review Questions</i>	220
<i>Footnotes</i>	220

Chapter 9	Corporate Crimes and Policy Violations Involving Computers: How to Conduct a Corporate Investigation	223
------------------	---	------------

<i>Corporate Investigations</i>	223
<i>Corporate Criminal Activities and Policy Violations</i>	224
<i>Preparing for the Investigation</i>	233
<i>Conducting the Investigation</i>	234
<i>Chapter Summary</i>	241
<i>Key Terms</i>	242
<i>Review Questions</i>	242
<i>Footnotes</i>	243

Chapter 10	E-mail Forensics	247
-------------------	-------------------------	------------

<i>The Importance of E-mail Investigations</i>	247
<i>E-mail: The Basics</i>	249
<i>How to Conduct an E-mail Investigation</i>	255
<i>Problems Encountered by Computer Forensics Investigators</i>	261
<i>Chapter Summary</i>	264
<i>Key Terms</i>	265
<i>Practical Exercise</i>	266
<i>Critical Thinking Question</i>	266
<i>Review Questions</i>	266
<i>Footnotes</i>	266

Chapter 11	Network Forensics: An Introduction	269
-------------------	---	------------

<i>Stand-alone Versus Networked Devices</i>	269
<i>Computer Networks</i>	269
<i>Network Components</i>	271

<i>Where Can Network-Related Evidence Be Found?</i>	274
<i>Network Forensics Analysis Tools</i>	280
<i>Special Issues When Conducting Investigations in a Networked Environment</i>	282
<i>Preliminary Analysis</i>	283
<i>Documentation and Collection</i>	283
<i>Analysis and Preservation</i>	285
<i>Chapter Summary</i>	288
<i>Key Terms</i>	288
<i>Review Questions</i>	289
<i>Footnotes</i>	290

Chapter 12 Mobile Phones and PDAs in Computer Forensics Investigations 293


<i>Role of Mobile Phones and PDAs</i>	293
<i>Mobile Phones and PDAs Versus Other Electronic Devices</i>	300
<i>Which Tools Can Be Used to Retrieve Evidence?</i>	302
<i>Mobile Phone and PDA Investigations</i>	307
<i>Chapter Summary</i>	313
<i>Key Terms</i>	313
<i>Practical Exercise</i>	314
<i>Critical Thinking Questions</i>	314
<i>Review Questions</i>	314
<i>Footnotes</i>	315

Chapter 13 The Pretrial and Courtroom Experiences of a Computer Forensics Investigator 321

<i>Pretrial Procedures</i>	321
<i>Testimony and Rules of Evidence</i>	324
<i>The Role of the Computer Forensics Investigator in Pretrial Proceedings and Court</i>	330
<i>Chapter Summary</i>	335
<i>Key Terms</i>	336
<i>Critical Thinking Question</i>	336
<i>Review Questions</i>	336
<i>Footnotes</i>	337

<i>Glossary</i>	339
---------------------------	-----

<i>Index</i>	361
------------------------	-----



Chapter 1

Entering the World of Cybercrime

During 2006 and 2007, inmates at the Plymouth County, Massachusetts, correctional facility were provided with computer privileges to conduct legal research. Stringent security measures were put in place that prevented inmates from accessing e-mail, the Internet, and other computer programs—at least that is what prison officials thought.

Francis G. Janosko, an inmate at the correctional facility at that time, managed to hack into the computer network. Specifically, he gained unauthorized access to the computer system to send e-mails and provide inmates in the facility with access to the personal information (names, Social Security numbers, home addresses, and telephone numbers, among other items) of more than 1000 current and former correctional facility workers.¹

Janosko's actions put the lives of these employees and their families in harm's way. This case is but one example of how the technology and information age has provided criminals with the means to cause catastrophic harm or damage with just a few presses on a keyboard—harm or damage that one could accurately say would not have been possible without the existence of such technology. It also raises a troubling question: Which other types of crimes have the Internet, computers, and related technologies made possible? To answer this question, this chapter focuses on what cybercrime is, how it differs from traditional forms of crime, which types of cybercrimes are distinguished, and which crimes are considered “cybercrimes.”

Cybercrime: Defined

The exponential expansion of computer technologies and the Internet have spawned a variety of new criminal behaviors and provided criminals with a new environment within

which to operate. **Cybercrime** involves the use of the Internet, computers, and related technologies in the commission of a crime. It includes technologically specific crimes that would not be possible without the use of computer technology as well as traditional crimes committed with the assistance of a computer.² The range of criminal activities has also been increasing as a result of the advent of cybercrime, as many more crimes were created and have been the exclusive product of technology and the Internet.

Cybercrime Versus Traditional Crime

Cybercrime differs from traditional crime in several ways. One important difference is that cybercrime knows no physical, geographic boundaries because the Internet provides criminals with access to people, institutions, and businesses around the globe. Consider the crime of fraud. Normally, fraud involves face-to-face communication with the victim or lengthy conversations over the phone to gain the target's trust. In today's world, however, fraudulent e-mails and websites can be used to con victims worldwide. For instance, from 2004 to 2009, Icarus Dakota Ferris manufactured and sold counterfeit postage stamps online by claiming that they were discontinued. He made approximately \$345,000 in profits by defrauding victims globally.³ As this example suggests, cybercrimes can be committed on a far broader scale than their traditional, real-world counterparts.

The Internet has augmented the ease and speed with which criminal activities are conducted. Prior to the advent of the Internet, if someone wanted to steal money from the bank, he or she would either rob the bank during its daily operation or steal the money after business hours. Either way, the thief would have to physically remove the money from the bank. As such, bank robbers were restricted to taking as much money as they could possibly carry outside the bank. In the online environment, such physical restrictions no longer apply. Larger monetary rewards can be gained without expending any physical energy. Billions of dollars can be stolen from a bank in the online environment within minutes.

The Internet also affords perpetrators with the opportunity to expend less effort in defrauding someone. Consider mail fraud, which has changed a great deal since the advent of computers. The amount of correspondence between individuals has increased exponentially as a result of technology because it takes significantly less time to send and receive a letter. Instead of individuals sending out fake letters through regular mail, criminals now do so electronically. In the past, regular mail might contain vital information, such as credit card and financial information, which nefarious individuals might steal. Now, criminals are using electronic mail (e-mail) to obtain the same kind of information. Criminals can also send bulk amounts of e-mail without paying; in the practice known as spamming, huge numbers of e-mails are sent out to multiple recipients almost instantaneously.

Another crime affected by computer and information technology is the theft of proprietary information and trade secrets from businesses. In the past, businesses might use spies, tap into phone wires, or set up cameras or voice recorders to obtain information on

their rivals. They would steal paperwork or sift through the trash for valuable documents that might have been discarded carelessly. Often, stealing this information was relatively difficult for the criminal. With the advent of computers, however, once someone has gained unauthorized access to a computer system, he or she has all of the information desired at their fingertips.

Social networking sites such as Facebook, MySpace, and Twitter have also made the burglar's job much easier. Today, burglars no longer need to stake out someone's home to determine whether the individual (target) is at home. Instead, they can simply request to be the target's friend on Facebook or MySpace or a follower of the subject on Twitter. Given that many people accept friend and follower requests from strangers, such a request is very likely to give the would-be thief access to the subject's profile page. On these sites, the targets are usually more than happy to share with the rest of the world their comings and goings—to such an extent that they normally declare when they are leaving their homes and where they are going. Individuals also like to share information about their homes and purchases. In California, a group of teenagers—mostly girls—were accused of burglarizing the homes of celebrities such as Orlando Bloom, Brian Austin Green, Megan Fox, Paris Hilton, and Lindsay Lohan using this information. More than \$3 million in jewelry, clothes, and accessories was stolen from these celebrities.⁴ The group tracked their victims' whereabouts online through sites such as Twitter to determine when the celebrities would be away from their homes.

Perhaps the National Academy of Sciences said it best: "The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."⁵

New Crimes, New Tactics

Crimes that would not have been possible without the use of technology include threats against software and networks such as **hacking** (defined as unauthorized intrusion into computers) and **malware** (malicious software), which includes computer viruses, worms, and Trojan horses (each of which is explored in this chapter in further detail).

Cyberterrorism is another example.⁶ **Cyberterrorism** may be defined "as the politically motivated use of computers as weapons or as targets, by sub-national groups or clandestine agents intent on violence, to influence an audience or cause a government to change its policies."⁷ A cyberterrorist may hack into U.S. critical infrastructure in an attempt to cause grave harm such as loss of life or significant economic damage. Such attacks are aimed at wreaking havoc on information technology systems that are an integral part of public safety, traffic control, medical and emergency services, and public works. While this type of wide-scale disruption has not yet come to fruition in real life, film has depicted it (for example, *Live Free or Die Hard*) and academicians, practitioners, researchers, law enforcement agencies, and politicians have entertained the possibility of such events occurring. Additionally, computer security experts have created mock cyberterrorism attacks to expose weaknesses in the United States' critical infrastructure during a war

game titled “Digital Pearl Harbor” hosted by the U.S. Naval War College in 2002.⁸ These attacks illustrated that the most vulnerable systems were the Internet and computer infrastructure systems of financial institutions.

Old Crimes, New Tactics

Cybercrime also includes crimes that put a twist on traditional crimes. Extortion can occur online. **Cyberextortion** occurs when someone uses a computer to attack or threaten to attack an individual, business, or organization if money is not provided to prevent or stop the attack. In Long Island, for example, two teenagers attempted to extort MySpace by threatening to post a method for stealing MySpace users’ personal information online, unless the site’s operators paid the teenagers \$150,000. In 2010, Anthony Digati tried to extort money from a New York-based life insurance company. In particular, Digati, via e-mail, threatened to damage the reputation of the insurance company and cost it millions of dollars in revenue if the company did not pay him approximately \$200,000.⁹

Crimes of **vandalism** can also occur online, although they take a different form from physical vandalism, such as graffiti on the walls. Online vandalism can occur by defacing websites, for example. Web defacement involves the unauthorized access to a website and the alteration or replacement of its content without causing permanent damage. A group of U.S. hackers (known as “Team Spl0it”) broke into government websites during the conflict in Kosovo in 1999 and posted antiwar messages.¹⁰ A more recent example concerns the Red Eye Crew. In January 2010, this group of hackers (allegedly from Brazil) defaced more than 30 websites owned by various U.S. House of Representatives and House Committee members. The hackers left an offensive message on the compromised websites that was aimed at the President of the United States, Barack Obama.¹¹

Even certain public order crimes, which include—among other things—victimless crimes that threaten the general well-being of society and challenge its accepted moral principles, can be committed online. One such example is prostitution. Prostitutes provide a range of sexual behaviors (e.g., sadism, masochism, and sexual intercourse) in exchange for remuneration. They may provide their services through brothels or escort services or search for potential customers on the streets. Nowadays, their services can be offered and arranged over the Internet. Specifically, prostitutes (or their pimps) may set up websites through which customers may solicit sexual services or post ads on online forums, wait for clients to answer the ads, and arrange meetings with their customers in hotels or other locations. This has come to be known as **cyberprostitution**. There have been many cases on Craigslist (a website that provides, among other things, forums for housing, jobs, personals, services, and events) where prostitutes have been soliciting sex in the “Casual Encounters” section (other sections as well). In fact, in 2009, undercover police officers in Worcester, Massachusetts, posted false offers of prostitution on Craigslist’s “Causal Encounters” section that resulted in the arrests of 50 people.¹²