



SECOND EDITION



# CYBERCRIME AND DIGITAL FORENSICS

AN INTRODUCTION

THOMAS J. HOLT,  
ADAM M. BOSSLER AND  
KATHRYN C. SEIGFRIED-SPELLAR



# Cybercrime and Digital Forensics

This book offers a comprehensive and integrative introduction to cybercrime. It provides an authoritative synthesis of the disparate literature on the various types of cybercrime, the global investigation and detection of cybercrime and the role of digital information, and the wider role of technology as a facilitator for social relationships between deviants and criminals. It includes coverage of:

- key theoretical and methodological perspectives;
- computer hacking and malicious software;
- digital piracy and intellectual theft;
- economic crime and online fraud;
- pornography and online sex crime;
- cyber-bullying and cyber-stalking;
- cyber-terrorism and extremism;
- digital forensic investigation and its legal context around the world;
- the law enforcement response to cybercrime transnationally;
- cybercrime policy and legislation across the globe.

The new edition features two new chapters, the first looking at the law enforcement response to cybercrime and the second offering an extended discussion of online child pornography and sexual exploitation.

This book includes lively and engaging features, such as discussion questions, boxed examples of unique events and key figures in offending, quotes from interviews with active offenders, and a full glossary of terms. This new edition includes QR codes throughout to connect directly with relevant websites. It is supplemented by a companion website that includes further exercises for students and instructor resources. This text is essential reading for courses on cybercrime, cyber-deviancy, digital forensics, cybercrime investigation, and the sociology of technology.

**Thomas J. Holt** is a Professor in the School of Criminal Justice at Michigan State University, USA.

**Adam M. Bossler** is a Professor of Criminal Justice and Criminology at Georgia Southern University, USA.

**Kathryn C. Seigfried-Spellar** is an Assistant Professor in the Department of Computer and Information Technology at Purdue University, USA.

“The second and expanded edition of *Cybercrime and Digital Forensics* is a most welcome update on this popular introductory text that covers the field, from the origins of computer hacking to the seizure and preservation of digital data. Each chapter begins with a useful general overview of the relevant literature on the topic or issue covered, whether economic cybercrimes or online stalking, and then provides coverage of laws, cases, and problems not just in the US but pertinent to other jurisdictions. Additional chapters on child exploitation materials, the role of transnational police and private investigation of cybercrime, and expanded treatment of cyber-terrorism, allow for more in depth treatment of these topics and, importantly, options for streaming or modifying the content of taught courses on cybercrime and digital investigations. The authors have again provided numerous online sources in the text and cases for students to explore, and a supporting website that should help to keep readers and instructors in touch with this rapidly changing field.”

—*Roderic Broadhurst, Professor of Criminology,  
RegNet, Australian National University*

“It is unusual to find a book in this field that does not simply focus on the technical aspects of the subject area. This book brings together a wide range of literature, sources, and real case-studies to provide an in-depth look at this ever-changing subject area. The book is rich in material and is a good read for those just starting to look at cyber-security, all the way through to those living and breathing it.”

—*Emlyn Butterfield, Course Director, School  
of Computing, Creative Technologies and  
Engineering, Leeds Beckett University*

“The style and organization of the book are ideal, not only for the introductory student, but also for the lay reader. What’s more, the timeliness and detail of the issues discussed make it a useful resource for more advanced researchers. In this book, the authors have delivered something for everyone.”

—*Peter Grabosky, Professor Emeritus, RegNet,  
Australian National University*

“*Cybercrime and Digital Forensics* provides an excellent introduction to the theory and practice of cybercrime. This second edition introduces new chapters on law enforcement responses to cybercrime and an extended section on online child pornography and sexual exploitation. The authors have introduced new and recent case material making the subject relevant and accessible to academics and students interested in this new and exciting field of study. I used the first edition of this book extensively in teaching an undergraduate course on cybercrime. This new edition updates and expands on the topic. Both students and teachers will be attracted to the clarity of presentation and extensive use of cases to focus discussion on challenging issues.”

—*Dr Lennon Chang, Lecturer in Criminology, School  
of Social Sciences, Monash University*

# Cybercrime and Digital Forensics

An Introduction

Second Edition

**Thomas J. Holt, Adam M. Bossler  
and Kathryn C. Seigfried-Spellar**

 **Routledge**  
Taylor & Francis Group  
LONDON AND NEW YORK



Second edition published 2018  
by Routledge  
2 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

and by Routledge  
711 Third Avenue, New York, NY 10017

*Routledge is an imprint of the Taylor & Francis Group, an informa business*

© 2018 Thomas J. Holt, Adam M. Bossler and Kathryn C. Seigfried-Spellar

The right of Thomas J. Holt, Adam M. Bossler and Kathryn Seigfried-Spellar to be identified as authors of this work has been asserted by them in accordance with sections 77 and 78 of the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this book may be reprinted or reproduced or utilised in any form or by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying and recording, or in any information storage or retrieval system, without permission in writing from the publishers.

*Trademark notice:* Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

First edition published by Routledge 2015

*British Library Cataloguing-in-Publication Data*

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

*Library of Congress Cataloging-in-Publication Data*

Names: Holt, Thomas J., 1978– author. | Bossler, Adam M., author. | Seigfried-Spellar, Kathryn C., author.

Title: Cybercrime and digital forensics : an introduction / Thomas J. Holt, Adam M. Bossler and Kathryn C. Seigfried-Spellar.

Description: Second edition. | Abingdon, Oxon ; New York, NY : Routledge, 2018. | Includes bibliographical references and index.

Identifiers: LCCN 2017017922 | ISBN 9781138238725 (hardback) | ISBN 9781138238732 (pbk.) | ISBN 9781315296975 (ebook)

Subjects: LCSH: Computer crimes. | Forensic sciences.

Classification: LCC HV6773 .H648 2018 | DDC 363.25/968—dc23

LC record available at <https://lccn.loc.gov/2017017922>

ISBN: 978-1-138-23872-5 (hbk)

ISBN: 978-1-138-23873-2 (pbk)

ISBN: 978-1-315-29697-5 (ebk)

Typeset in Bembo

by Apex CoVantage, LLC

Printed and bound by CPI Group (UK) Ltd, Croydon, CR0 4YY

Visit the companion website: [www.routledge.com/cw/holt](http://www.routledge.com/cw/holt)

# Contents

---

List of figures .....	x
List of tables .....	xii
List of boxes .....	xiii

## 1 TECHNOLOGY AND CYBERCRIME

Introduction .....	2
Technology as a landscape for crime .....	5
A typology of cybercrime .....	22
This text .....	26

## 2 LAW ENFORCEMENT, PRIVACY, AND SECURITY IN DEALING WITH CYBERCRIME

Introduction .....	40
Local police and sheriffs' offices .....	41
State agencies .....	45
Federal law enforcement .....	47
Civil investigation and application of digital evidence .....	48
Extralegal agencies and non-governmental organizations .....	53
International enforcement challenges .....	55
The tension between security and privacy .....	56
Summary .....	60

## 3 COMPUTER HACKERS AND HACKING

Introduction .....	68
Defining computer hacking .....	69
Victims of hacking .....	72

The human aspects of the hacker subculture.....	75
Hacking history .....	78
The modern hacker subculture .....	99
Legal frameworks to prosecute hacking.....	105
Enforcing and investigating hacker activity.....	111
Summary .....	116

**4 MALWARE AND AUTOMATED COMPUTER ATTACKS 127**

Introduction .....	128
The basics of malware.....	129
Viruses, trojans, and worms .....	131
The global impact of malware .....	147
Hackers and malware writers .....	151
The market for malicious software .....	153
Legal challenges in dealing with malware .....	158
Coordination and management in addressing malware.....	162
Summary .....	165

**5 DIGITAL PIRACY AND INTELLECTUAL PROPERTY THEFT 171**

Introduction .....	172
What is intellectual property? .....	175
The evolution of piracy over time .....	177
The subculture of piracy .....	182
The evolution of legislation to deal with piracy.....	184
The law enforcement and industry response .....	191
Summary .....	196

**6 ECONOMIC CRIMES AND ONLINE FRAUD 201**

Introduction .....	202
Fraud and computer-mediated communications .....	205
Identity theft .....	206
Email-based scams.....	210
Romance scams .....	220
The problem of carding and stolen data markets .....	235
Identity theft and fraud laws.....	243
Summary .....	254

**7 PORNOGRAPHY, PROSTITUTION, AND SEX CRIMES 266**

Introduction .....	266
The spectrum of sexuality online.....	268

Pornography in the digital age.....	271
Prostitution and sex work.....	275
Dealing with obscenity and pornography online.....	279
Self-regulation by the pornography industry.....	284
Summary.....	286
<b>8 CHILD PORNOGRAPHY AND SEXUAL EXPLOITATION</b> .....	<b>296</b>
Introduction.....	296
Defining and differentiating child porn from obscene content.....	298
The role of technology in child pornography and exploitation.....	302
Explorations of the pedophile subculture online.....	306
The legal status of child pornography around the globe.....	317
Summary.....	330
<b>9 CYBERBULLYING, ONLINE HARASSMENT, AND CYBERSTALKING</b> .....	<b>340</b>
Online threats, bullying, and harassment.....	340
Defining cyberbullying.....	343
Predictors of bullying online and offline.....	347
Summary.....	370
<b>10 ONLINE EXTREMISM, CYBERTERROR, AND CYBERWARFARE</b> .....	<b>381</b>
Introduction.....	382
Defining terror, hacktivism, and cyberterror.....	385
The role of nation-state vs. non-nation-state attacks.....	390
The use of the Internet in the indoctrination and recruitment of extremist groups.....	394
Electronic attacks by extremist groups.....	402
Cyberwar and the nation-state.....	411
Legislating extremism and cyberterror.....	416
Investigating and securing cyberspace from the threat of terror and war.....	420
Cyberwar and response.....	425
Summary.....	427
<b>11 CYBERCRIME AND CRIMINOLOGICAL THEORIES</b> .....	<b>430</b>
Introduction.....	440
Subcultural theories.....	442

Social learning theory and cybercrime.....	444
General theory of crime.....	449
Agnew's general strain theory .....	453
Techniques of neutralization.....	455
Deterrence theory .....	459
Theories of cybercrime victimization.....	462
Need for new cyberspace theories? .....	470
Summary.....	477
<b>12 EVOLUTION OF DIGITAL FORENSICS</b> .....	<b>491</b>
Introduction .....	492
From computer forensics to digital forensics.....	493
Stages of digital forensic investigation.....	504
The role of digital evidence .....	508
Types of hardware, peripherals, and electronic evidence .....	511
Evidence integrity.....	517
Summary.....	518
<b>13 ACQUISITION AND EXAMINATION OF FORENSIC EVIDENCE</b> .....	<b>527</b>
Introduction .....	528
Data preservation .....	529
Digital forensic imaging tools .....	535
Uncovering digital evidence .....	544
Data analysis .....	557
Data reduction and filtering .....	558
Reporting of findings.....	559
Summary.....	561
<b>14 LEGAL CHALLENGES IN DIGITAL FORENSIC INVESTIGATIONS</b> .....	<b>571</b>
Introduction .....	572
Constitutional issues in digital investigations.....	574
Federal Rules of Evidence 702.....	607
Summary.....	612
<b>15 THE FUTURE OF CYBERCRIME, TERROR, AND POLICY</b> .....	<b>623</b>
Introduction .....	624
Considering the future of cybercrime.....	625

How techniques will shift with new technologies .....	629
Social movements, technology, and social change .....	631
Need for new cyber criminological theories? .....	633
Shifting enforcement strategies in the age of the Internet .....	636
Considering the future of forensics .....	640
The challenge to policy makers globally .....	642
Summary .....	645
<b>Glossary</b> .....	<b>653</b>
<b>Index</b> .....	<b>709</b>

Biblioteka Główna  
Akademii Sztuki Wojennej

26714/III (CB)



03-026714-000-0

Cypt.  
004.056

"The second and expanded edition of *Cybercrime and Digital Forensics* is an introductory text that covers the field, from the basics to the latest data. The authors have again provided numerous examples and a supporting website that should help to keep you up to date." —**Roderic Broadhurst, Professor of Criminology, Monash University**

"It is unusual to find a book in this field that is both accessible and comprehensive. This book brings together a wide range of literature, sources, and real case studies to provide an in-depth look at this ever-changing subject area. The book is rich in material and is a good starting point for anyone interested in cyber-security, all the way through to those living and breathing it." —**Emlyn Butterfield, Course Director, School of Computing, Creative Technology, Beckett University**

"The style and organization of the book are ideal, not only for the introductory student, but also for the lay reader. What's more, the timeliness and detail of the issues discussed make it a useful resource for more advanced researchers. In this book, the authors have delivered something for everyone." —**Peter Grabosky, Professor Emeritus, RegNet, Australian National University**

"*Cybercrime and Digital Forensics* provides an excellent introduction to the theory and practice of cybercrime. Both students and teachers will be attracted to the clarity of presentation and extensive use of cases to focus discussion on challenging issues." —**Dr Lennon Chang, Lecturer in Criminology, School of Social Sciences, Monash University**

This book offers a comprehensive and integrative introduction to cybercrime. It provides an authoritative synthesis of the disparate literature on the various types of cybercrime, the global investigation and detection of cybercrime and the role of digital information, and the wider role of technology as a facilitator for social relationships between deviants and criminals. It includes coverage of:

- key theoretical and methodological perspectives;
- computer hacking and malicious software;
- digital piracy and intellectual theft;
- economic crime and online fraud;
- pornography and online sex crime;
- cyber-bullying and cyber-stalking;
- cyber-terrorism and extremism;
- digital forensic investigation and its legal context around the world;
- the law enforcement response to cybercrime transnationally;
- cybercrime policy and legislation across the globe.

The new edition features two new chapters, the first looking at the law enforcement response to cybercrime and the second offering an extended discussion of online child pornography and sexual exploitation.

This book includes lively and engaging features, such as discussion questions, boxed examples of unique events and key figures in offending, quotes from interviews with active offenders, and a full glossary of terms. This new edition includes QR codes throughout to connect directly with relevant websites. It is supplemented by a companion website that includes further exercises for students and instructor resources. This text is essential reading for courses on cybercrime, cyber-deviancy, digital forensics, cybercrime investigation, and the sociology of technology.

Thomas J. Holt is a Professor in the School of Criminal Justice at Michigan State University, USA.

Adam M. Bossler is a Professor of Criminal Justice and Criminology at Georgia Southern University, USA.

Kathryn C. Seigfried-Spellar is an Assistant Professor in the Department of Computer and Information Technology at Purdue University, USA.

CRIMINOLOGY/SOCIOLOGY



[www.routledge.com/cw/holt](http://www.routledge.com/cw/holt)

Cover image: © Getty

**Routledge**  
Taylor & Francis Group  
[www.routledge.com](http://www.routledge.com)

ISBN 978-1-138-23873-2  
9 781138 238732

Routledge titles are available as eBook editions in a range of digital formats

an informa business