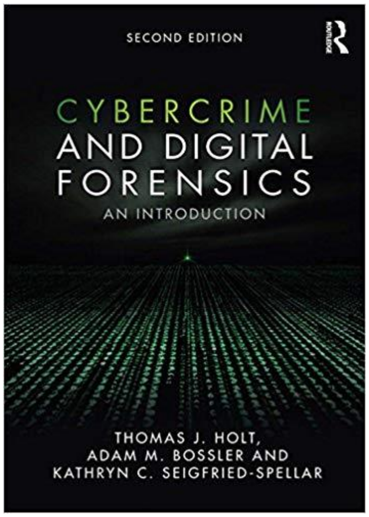
Text Review: Cybercrime and Digital Forensics: An Introduction

ROGER NEBEL, University of Alaska Fairbanks

rjnebel@alaska.edu


SECOND EDITION
CYBERCRIME AND DIGITAL FORENSICS
AN INTRODUCTION
THOMAS J. HOLT, ADAM M. BOSSLER AND KATHRYN C. SEIGFRIED-SPELLAR

TEXT AND AUTHOR INFORMATION

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.

Paperback: 754 pages
Publisher: Routledge; 2 edition (October 20, 2017)
Language: English
ISBN-10: 1138238732
ISBN-13: 978-1138238732
List Price: $57.17 (Paperback)
eReader: $54.88 (Kindle Edition)

TABLE OF CONTENTS REVIEW

Cybercrime and Digital Forensics is structured as 15 more or less independent chapters that reflect the authors obvious backgrounds and expertise in criminal matters. For this 2nd edition two new chapters have also been added. The book offers a comprehensive overview of the range of digital cybercrimes, related investigations, forensics, and some legal issues. The text also includes discussion questions, boxed examples of unique events and key figures, quotes from interviews with offenders, and a glossary of terms. It is supplemented by a companion website that includes further exercises for students and instructor resources, as well as a list of related acronyms, a glossary, and an index. Each chapter includes endnotes and reference documentation.

TEXT REVIEW

The book focuses on crimes and law enforcement, important subjects to be sure, and bound to be enlightening for many readers. The book is necessarily somewhat technical in nature, but not so much that it faces being too outdated by technology before it's even printed. In addition, law and technology are changing rapidly as courts are interpreting issues and technology quickly adds new issues requiring interpretation. Having said that one is cautioned that technology and related law is constantly changing in some key areas, and so up to date information should always be consulted. The book also mentions contracts and civil actions, and as pointed out disputes are often settled between the parties in private agreements, so public information is scant. However, the book fails to mention that most computer security law and digital forensics is in fact outside any law enforcement at all and while not a negative criticism per se, future editions should expand on the role of litigation and legal precedent in both crimes and in civil actions.

What to look for. Highlights include:

- Computer Hackers and Hacking Chapter 3 has a good summary of the hacker ethic and The Hacker Manifesto. There is also a discussion of Capture the Flag type competitions. There is also a lengthy description of the Computer Fraud and Abuse Act (CFAA).
- Chapters 7, 8, and 9 are especially helpful as the whole area of sexual crimes, cyberbullying, and technology is rapidly changing in the era of social media and the perceived anonymity provided by the Internet.
- Cybercrime and Criminological Theories Chapter 11 is very well written and adds to the student's knowledge in this area.

What else. I have yet to come across a cybercrime and digital forensics text that is both comprehensive and sufficiently covers all the necessary topics. My sense is that the disciplines are necessarily too large and varied to allow a definitive, one-stop publication. However, there are some areas that I would like to see in the next edition:

- An explanation of what Responsible Disclosure is, and how the trend towards Bug Bounties and Crowdsourcing has greatly expanded, and how that influences the fields of crime and forensics. For example, anti-forensics techniques are not mentioned at all.
- Expanded section or a chapter on civil litigation, contract law, and precedent, and how the law changes over time based on trends in this area. A re-write may be needed of Chapters 2 and 14 to clearly differentiate between criminal, contract, and civil law and how they interact. For example, most non-law enforcement forensic experts (sometimes called e-discovery) are considerably more talented and already self-regulate through efforts such as the Sedona Conference.
- A section on the psychology of cyber miscreants beyond criminological theories is needed for an understanding of digital behavior that is not criminal per se but is clearly not productive to society. An example of this is the whole area of gaming and betting. While the book calls some of this behavior "deviant" from societal norms, more is needed in this area.

Cybercrime and Digital Forensics is a solid effort, and one that lends itself to satisfying the need to fill the void in how technology affects crime today. While all the chapters are essentially correct, they don't depend on each other and one is able to pick and choose the chapters that add value or supplement your reading list.