

Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition

By Eoghan Casey

Download now

Read Online →

Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition By Eoghan Casey

Digital Evidence and Computer Crime, Third Edition provides the knowledge necessary to uncover and use digital evidence effectively in any kind of investigation. The widely-adopted first and second editions introduced thousands of students to this field and helped them deal with digital evidence. This completely updated edition provides the introductory materials that new students require, and also expands on the material presented in previous editions to help students develop these skills. The textbook teaches how computer networks function, how they can be involved in crimes, and how they can be used as a source of evidence. Additionally, this third edition includes updated chapters dedicated to networked Windows, Unix, and Macintosh computers, and Personal Digital Assistants.

Ancillary materials include an Instructor's Manual and PowerPoint slides.

- Named The 2011 Best Digital Forensics Book by *InfoSec Reviews*
- Provides a thorough explanation of how computers & networks function, how they can be involved in crimes, and how they can be used as evidence
- Features coverage of the abuse of computer networks and privacy and security issues on computer networks

 [Download Digital Evidence and Computer Crime: Forensic Scie ...pdf](#)

 [Read Online Digital Evidence and Computer Crime: Forensic Sc ...pdf](#)

Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition

By Eoghan Casey

Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition By Eoghan Casey

Digital Evidence and Computer Crime, Third Edition provides the knowledge necessary to uncover and use digital evidence effectively in any kind of investigation. The widely-adopted first and second editions introduced thousands of students to this field and helped them deal with digital evidence. This completely updated edition provides the introductory materials that new students require, and also expands on the material presented in previous editions to help students develop these skills. The textbook teaches how computer networks function, how they can be involved in crimes, and how they can be used as a source of evidence. Additionally, this third edition includes updated chapters dedicated to networked Windows, Unix, and Macintosh computers, and Personal Digital Assistants.

Ancillary materials include an Instructor's Manual and PowerPoint slides.

- Named The 2011 Best Digital Forensics Book by *InfoSec Reviews*
- Provides a thorough explanation of how computers & networks function, how they can be involved in crimes, and how they can be used as evidence
- Features coverage of the abuse of computer networks and privacy and security issues on computer networks

Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition By Eoghan Casey **Bibliography**

- Sales Rank: #405077 in Books
- Published on: 2011-05-04
- Original language: English
- Number of items: 1
- Dimensions: 1.80" h x 8.00" w x 9.30" l, 4.15 pounds
- Binding: Hardcover
- 840 pages

 [Download Digital Evidence and Computer Crime: Forensic Scie ...pdf](#)

 [Read Online Digital Evidence and Computer Crime: Forensic Sc ...pdf](#)

Editorial Review

Amazon.com Review

Practitioner's Tips from *Digital Evidence and Computer Crime*'s Chapter on Digital Evidence in the Courtroom

- In practice, many searches are conducted with consent. One of the biggest problems with consensual searches is that digital investigators must cease the search when the owner withdraws consent. However, digital investigators may be able to use the evidence gathered from a consensual search to establish probable cause and obtain a search warrant.
- Once a search warrant is obtained, there is generally a limited amount of time to execute the search. Therefore, it is prudent to obtain a search warrant only after sufficient preparations have been made to perform the search in the allotted time period. Any evidence obtained under an expired search warrant may not be admissible.
- Many digital investigators use the terminology “is consistent with” inappropriately to mean that an item of digital evidence might have been due to a certain action or event. For many people, to say that something is consistent with something else means that the two things are identical, without any differences. To avoid confusion, digital investigators are encouraged only to state that something is consistent with something else if the two things are the same and to otherwise use the terminology “is compatible with.”
- Given the complexity of modern computer systems, it is not unusual for digital investigators to encounter unexpected and undocumented behaviors during a forensic analysis of digital evidence. Such behaviors can cause unwary digital investigators to reach incorrect conclusions that can have a significant impact on a case, sometimes leading to false accusations. Thorough testing with as similar an environment to the original as possible can help avoid such mistakes and resolve differences in interpretation of digital evidence. Provided digital investigators can replicate the actions that led to the digital evidence in question, they can generally agree on what the evidence means. When it is not possible to replicate the exact environment or digital evidence under examination, digital investigators may need to rely on their understanding of the systems involved, which is where differences of opinion can arise.
- Careful use of language is needed to present digital evidence and associated conclusions as precisely as possible. Imprecise use of language in an expert report can give decision makers the wrong impression or create confusion. Therefore, digital investigators should carefully consider the level of certainty in their conclusions and should qualify their findings and conclusions appropriately.

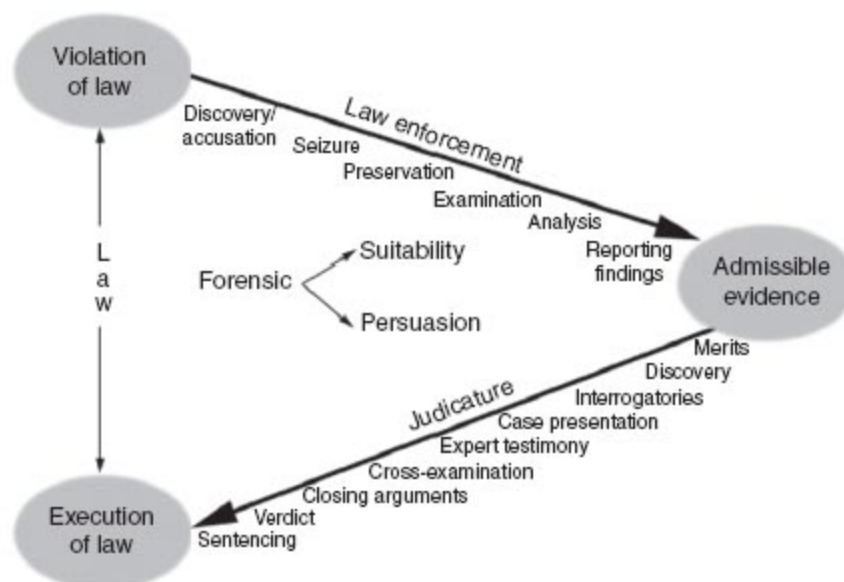


FIGURE 3.1
Overview of case/incident resolution process.

Read a sample chapter on genesis and migration from *Digital Evidence and Computer Crime*

Review

"Throughout the book there are a number of good case studies used to illustrate points which enlivens the text. There are also details of legal cases from various legislative areas and examples of relevant situations that demonstrate the points being made. There are also a number of references to other literature and links to website URLs and tools available to assist the practitioner." --**Best Digital Forensics Book in InfoSecReviews Book Awards**

"Just finished 'Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet' by Eoghan Casey and featuring other contributing authors, and it's quite good. I bought this book because I wanted an all-encompassing book that provided insight on the various aspects of an investigation, especially the legal portion. And in this aspect the book does an excellent job, and is in-depth in area's I have yet to see in other books. The book is divided into five portions digital forensics, digital investigations, apprehending offenders, computers and network forensics. For me the book was worth it for the first three portions; however, the computers and network portions, while a good start, there are more in-depth books that provide better insight... Overall, the book was enjoyable from start to finish and I would recommend it to anyone looking for a great overview of digital forensic investigation process from start to finish. I am happy to add this book to my growing reference library." --**Student of Security**

"This hefty book on forensic evidence obtained from computers dispels the myths propagated by popular television series. It states from the premise that very few people are well versed in the technical, evidential, and legal issues concerning digital evidence. Oftentimes, the useful evidence that may be found in various digital media is overlooked, collected incorrectly, or analyzed ineffectively. It is the goal of the team of contributors to equip readers with the necessary knowledge and skills to be able to make use of digital evidence correctly and effectively.... It is quite obvious that the various authors draw from several fields, such as forensic science, computer science, political science, criminal justice, the law, and behavioral analysis; as such, it is multi- and interdisciplinary. More specifically, the authors tackle the specific crimes of cyber bullying, cyber stalking, identity theft, online sex offenders, fraudsters, and cyber threats. There is extensive use of boxed stories, legal cases, practitioner's tips, tables, the discussion of legislation, flow

charts, treaties and journals, as well as figures, diagrams, pictures, and computer screen shots. The book is comparative in nature: it covers not only cyber law in the US, but also case law in the UK, Ireland, and the Netherlands. Given the ubiquity of the computer and the crimes that it can generate, learning about how other nations handle these issues helps in the formation of our own methods for dealing with crimes domestically, as well as those that cross national boundaries."--**ACM's Computing Reviews.com**

"A better title for *Digital Evidence and Computer Crime* might be the Comprehensive Guide to Everything You Need to Know About Digital Forensics. One is hard pressed to find another book overflowing with so many valuable details and real-world examples."--Ben Rothke on Slashdot.org (Sept 2011)

"The third edition of this comprehensive textbook on forensic science and the Internet is thoroughly updated to reflect the great leaps forward in technology in the six years since the previous printing. The work is divided into five sections covering digital forensics, digital investigations, apprehending offenders, computers and network forensics, and chapters provide practical instruction, case studies and discussions of the theoretical basis for all aspects of digital investigation and the use of computer evidence in forensics and law enforcement. The volume is intended for police, lawyers and forensic analysts and provides a comprehensive look at contemporary methodologies computer crime and crime prevention. Contributors include legal academics as well as computer, networking and forensics professional from around the world."--**Book News, Reference & Research**

"A better title for Digital Evidence and Computer Crime might be the Comprehensive Guide to Everything You Need to Know About Digital Forensics. One is hard pressed to find another book overflowing with so many valuable details and real-world examples. The book is also relevant for those who are new to the field, as it provides a significant amount of introductory material that delivers a broad overview to the core areas of digital forensics. The book progresses to more advanced and cutting-edge topics, including sections on various operating systems, from Windows and Unix to Macintosh. This is the third edition of the book and completely updated and reedited. When it comes to digital forensics, this is the reference guide that all books on the topic will be measured against. With a list price of \$70.00, this book is an incredible bargain given the depth and breadth of topics discussed, with each chapter written by an expert in the field. For those truly serious about digital forensics, Digital Evidence and Computer Crime is an equally serious book."--**Slashdot.com**

From the Back Cover

Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, Third Edition

by Eoghan Casey cmdLabs, Baltimore, Maryland, USA

Technical Editor Brent E. Turvey, Forensic Solutions LLC, Sitka, Alaska, USA

Contributors: Susan W. Brenner (University of Dayton School of Law), Bert-Jaap Koops (Tilburg University, Netherlands), Tessa Robinson (Law Library, Dublin, Ireland), Bradley Schatz (Schatz Forensic Pty. Ltd., Queensland), Terrance Maguire (cmdLabs), Monique M. Ferraro (Technology Forensics, LLC, Connecticut), Michael McGrath, Christopher Daywalt (cmdLabs)

Digital evidence - evidence that is stored on or transmitted by computers - can play a major role in any investigation, including homicide, child exploitation, computer intrusions and corporate malfeasance. The scope of computer crime has expanded further with the proliferation of networks, embedded systems, mobile devices and industrial control systems. Digital evidence from these systems can help establish when events occurred, where victims and suspects were, with whom they communicated, and may even show their intent

to commit a crime.

Despite the ubiquity of computer-facilitated crime, few people are well-versed in the technical, investigative and legal issues related to digital evidence. As a result, digital evidence is often overlooked, collected incorrectly or analyzed ineffectively.

Digital Evidence and Computer Crime, Third Edition is completely updated, providing the knowledge necessary to uncover and use digital evidence effectively in any kind of investigation. The first and second editions introduced thousands of practitioners to this field, and this third edition expands on the material presented in previous editions to help digital forensic practitioners further develop their skills. The textbook teaches digital investigation and forensic methodologies, how computers and networks function, how they can be involved in crimes, and how they can be used as a source of evidence. This book is suitable for incident responders, forensic analysts, police and lawyers. Case examples and practitioner's tips are provided throughout each chapter to emphasize important concepts.

New chapters include coverage of:

- Handling digital crime scenes
- Investigating violent crimes
- Applying the scientific method to digital investigations
- Legal issues from both the U.S. and European perspectives

ISBN: 978-0-12-374268-1

Users Review

From reader reviews:

Claudia Weidner:

The book Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition can give more knowledge and also the precise product information about everything you want. Why must we leave the best thing like a book Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition? A few of you have a different opinion about publication. But one aim this book can give many data for us. It is absolutely suitable. Right now, try to closer along with your book. Knowledge or info that you take for that, you can give for each other; it is possible to share all of these. Book Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition has simple shape however, you know: it has great and big function for you. You can seem the enormous world by available and read a guide. So it is very wonderful.

Donald Scott:

Nowadays reading books be than want or need but also get a life style. This reading habit give you lot of advantages. The huge benefits you got of course the knowledge your information inside the book which improve your knowledge and information. The knowledge you get based on what kind of publication you read, if you want drive more knowledge just go with education and learning books but if you want feel happy read one along with theme for entertaining like comic or novel. The Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition is kind of publication which is giving the reader erratic experience.

Michele Williams:

Reading a publication tends to be new life style in this particular era globalization. With reading you can get a lot of information that could give you benefit in your life. Having book everyone in this world can share their idea. Books can also inspire a lot of people. A great deal of author can inspire their reader with their story as well as their experience. Not only the storyline that share in the books. But also they write about the information about something that you need illustration. How to get the good score toefl, or how to teach your kids, there are many kinds of book that you can get now. The authors on earth always try to improve their talent in writing, they also doing some study before they write on their book. One of them is this Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition.

Daniel Bailey:

As we know that book is significant thing to add our knowledge for everything. By a book we can know everything we would like. A book is a list of written, printed, illustrated or maybe blank sheet. Every year had been exactly added. This publication Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition was filled in relation to science. Spend your spare time to add your knowledge about your scientific disciplines competence. Some people has different feel when they reading any book. If you know how big good thing about a book, you can feel enjoy to read a publication. In the modern era like currently, many ways to get book you wanted.

**Download and Read Online Digital Evidence and Computer Crime:
Forensic Science, Computers and the Internet, 3rd Edition By
Eoghan Casey #WBYQ7RAGNDU**

Read Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition By Eoghan Casey for online ebook

Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition By Eoghan Casey Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition By Eoghan Casey books to read online.

Online Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition By Eoghan Casey ebook PDF download

Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition By Eoghan Casey Doc

Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition By Eoghan Casey Mobipocket

Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition By Eoghan Casey EPub