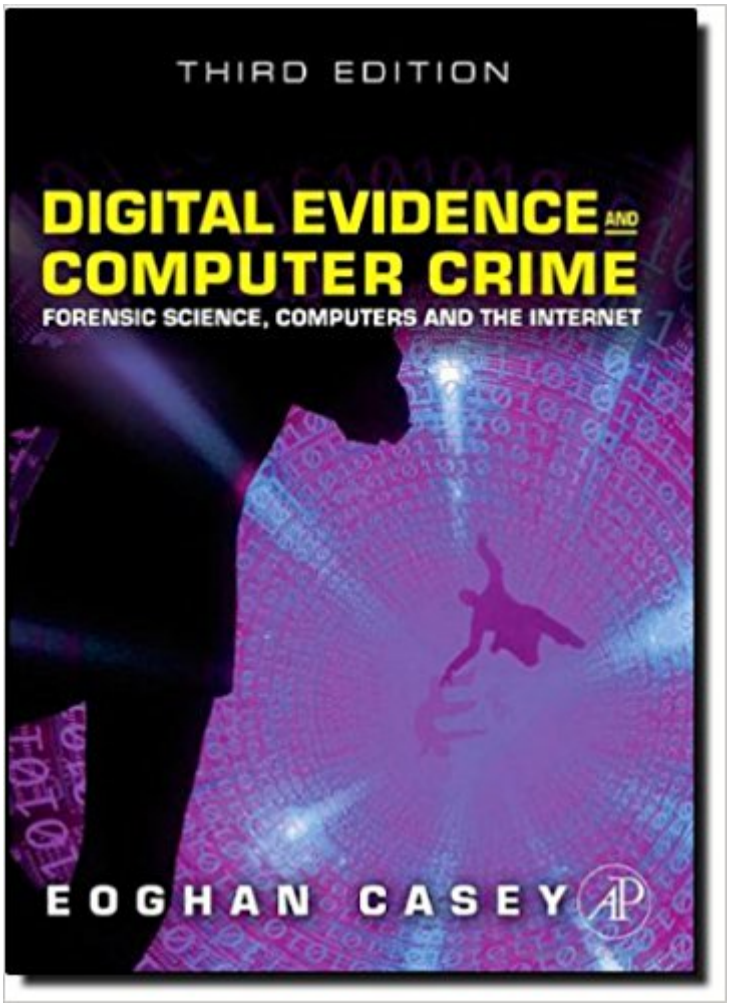
Digital Evidence And Computer Crime: Forensic Science, Computers And The Internet, 3rd Edition



Synopsis

Digital Evidence and Computer Crime, Third Edition, provides the knowledge necessary to uncover and use digital evidence effectively in any kind of investigation. It offers a thorough explanation of how computer networks function, how they can be involved in crimes, and how they can be used as a source of evidence. In particular, it addresses the abuse of computer networks as well as privacy and security issues on computer networks. This updated edition is organized into five parts. Part 1 is about digital forensics and covers topics ranging from the use of digital evidence in the courtroom to cybercrime law. Part 2 explores topics such as how digital investigations are conducted, handling a digital crime scene, and investigative reconstruction with digital evidence. Part 3 deals with apprehending offenders, whereas Part 4 focuses on the use of computers in digital investigation. The book concludes with Part 5, which includes the application of forensic science to networks. New to this edition are updated information on dedicated to networked Windows, Unix, and Macintosh computers, as well as Personal Digital Assistants; coverage of developments in related technology and tools; updated language for search warrant and coverage of legal developments in the US impacting computer forensics; and discussion of legislation from other countries to provide international scope. There are detailed case examples that demonstrate key concepts and give students a practical/applied understanding of the topics, along with ancillary materials that include an Instructor's Manual and PowerPoint slides. This book will prove valuable to computer forensic students and professionals, lawyers, law enforcement, and government agencies (IRS, FBI, CIA, CCIPS, etc.). Named The 2011 Best Digital Forensics Book by InfoSec ReviewsProvides 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

Book Information

Hardcover: 840 pages
Publisher: Academic Press; 3rd edition (May 4, 2011)
Language: English
ISBN-10: 0123742684
ISBN-13: 978-0123742681
Product Dimensions: 9.3 x 8 x 1.8 inches
Shipping Weight: 4.2 pounds (View shipping rates and policies)
Average Customer Review: 4.0 out of 5 stars 26 customer reviews

Best Sellers Rank: #38,422 in Books (See Top 100 in Books) #12 inÃ Â Books > Law > Criminal Law > Evidence #17 inÃ Â Books > Medical Books > Psychology > Forensic Psychology #17 inÃ Â Books > Health, Fitness & Dieting > Psychology & Counseling > Forensic Psychology

Customer Reviews

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 Ã¢â ¬Å“is consistent withÃ¢â ¬Â• 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 Ã¢â ¬Å“is compatible with.Ã¢â ¬Â• 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. Read a sample chapter on genesis and migration

from Digital Evidence and Computer Crime

"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 Ã¢â ¬ËœDigital Evidence and Computer Crime: Forensic Science, Computers and the InternetÃ¢â ¬â„¢ by Eoghan Casey and featuring other contributing authors, and itÃ¢â ¬â„¢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 areaÃ¢â ¬â„¢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 insightÃ¢â ¬Â¦ 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 effectivelyÃ¢â ¬Â¦. Ã Â 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, practitionerÃ¢â ¬â„¢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."--ACMÃ¢â ¬â„¢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

Required for a graduate level digital forensics course. I had taken another one before in the Information Assurance major and that class used the Bill Nelson textbook. While Nelson’s book delivered more lab exercises for actually harvesting digital data, Casey’s book focuses more on the elements inherent in the field of digital forensics.Chain of custody and legal procedure are critical to success if digital "evidence" is to be accepted in court. The TV shows where the detective looks at a suspect’s cell phone and finds a clue immediately is not proper procedure. Accessing a suspect’s computer as shown on TV also does not happen since a bit by bit forensic copy must be made first

and all operations occur using the copy thereby preserving the original.There have been strides made in laws regarding digital evidence, however, judges deciding cases involving digital evidence also need to be equipped to comprehend the significance of data on digital devices and how it all works. One flaming example of a judge out of her depth is Judge Lucy Koh during the Samsung tablet v. Apple iPad case. While holding up the two tablets, Koh asked Samsung attorneys to identify which table was Samsung. The patent infringement lawsuit had little to do with the exterior hard case of the tablets and everything to do with its operating system and how data was processed. Casey makes it clear that digital forensics is more about the appropriate processing & handling of digital device evidence, according to venue, and less about whether there is a treasure trove of data clues staring police detectives/federal agents in the face like tempting fruit on a forbidden tree. He also presents the tricky navigating that needs to occur since laws regarding digital device evidence processing & use in court vary widely across the globe.I like Casey’s use of language. I like that he seldom uses "for example" and substitutes "for instance." I like the in-depth and meticulous material. It is the hallmark of a person who knows so much and wants to impart as much of it as possible. Thank you Eoghan Casey for sharing your wealth of knowledge with the community of potential digital forensic investigators.

Did Casey get paid by the page?!? It’s obvious that Casey knows his stuff, but this book is way too long for what it offers.It is repetitive from chapter to chapter. This may be good for those people who only learning through repetition, but it’s wasted effort for anyone else.There is an entire chapter on European cybercrime law, but the only relevant national legislation reviewed is from England, Ireland, and the Netherlands. This is probably because those are the countries he could get an expert from, but again, it’s a waste of space. As a reader, if you need to cover specific national legislation, then you’ll need more than this chapter, if you don’t then again, this chapter is a waste. 100 pages to basically say, "Europe is different than the US". Wow, thanks, I would’ve never guessed.This book is not specific enough (no technical details or procedures within) for more than an overview of digital forensic principles, but yet it’s too long to be a good overview for people just getting started.3 stars, because other than the length, there is nothing particularly wrong with the content, but yet, I can’t recommend it to anyone. I can’t see a reason to need this book except as mandatory reading for a class.

This is roughly the format of this book:Simple concepts explained in excruciating detail that can rarely be applied.Simple case studies that almost have something to do with the concepts but, on

the whole, distract from the concepts.Amalgams of concepts and case studies that leave you wondering what the purpose is of all these things you're reading.If you're looking into getting into digital forensics I can't say this is a good way to start.Though, to be fair, a few of my classmates seemed to love it.

A very confusing and jumbled up text book. I don't know why the professor recommended this book.

Very good quality. Huge and heavy book. May reccommend the EBook! Great service, fast shipping.

Required reading for one of my course's in computer forensics. Liked the price over what was being charged int he local bookstore.

Purchased as a gift. Required textbook for master's program in cybersecurity.

This book really is focused on legal aspects of computer crime and does not give a lot of detail about how to actually do any type of digital forensics. Great book for understanding some of the history and regulations on computer crime and would recommend for that reason. But if you want to know how to perform any type of digital forensics, get another book.

Practice in Neuropsychology) Computers in Medicine (Applications of computer science series) True Crime Stories Volume 7: 12 Shocking True Crime Murder Cases (True Crime Anthology) True Crime Stories: 3 True Crime Books Collection (True Crime Novels Anthology) True Crime Stories: 12 Shocking True Crime Murder Cases (True Crime Anthology) True Crime: Homicide & True Crime Stories of 2016 (Annual True Crime Anthology) Forensic Analysis and DNA in Criminal Investigations and Cold Cases Solved: Forensic Science Forensic Archaeology: Advances in Theory and Practice (Forensic Science) Forensic Anthropology (Inside Forensic Science) Computer Science for the Curious: Why Study Computer Science? (The Stuck Student's Guide to Picking the Best College Major and Career) Extremal Combinatorics: With Applications in Computer Science (Texts in Theoretical Computer Science. An EATCS Series)