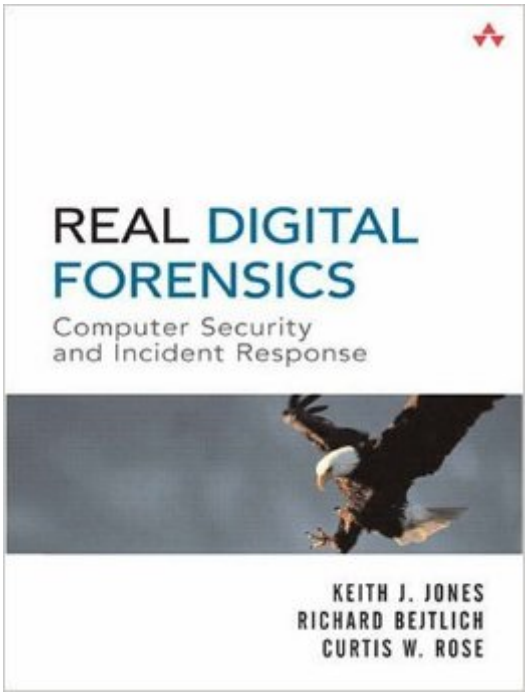
Real Digital Forensics: Computer Security And Incident Response



Synopsis

This is a book and DVD set providing an interactive experience that helps readers master the tools and techniques of forensic analysis by investigating real cases. Offers practical hands-on approach to solving problems encountered when performing computer-related investigations. It’s authors are well known and well respected in the industry, speak widely, and teach forensics classes. The motto of this book and DVD set is learn by doing. Many people understand the basics of computer forensics and incident response, but lack the necessary skills and direct experience to tackle a case on their own. Organized around case studies, this book offers a comprehensive introduction to the methods, techniques, and tools of forensic investigations through direct contact with real cases. All of the material is introduced within the context of a complete forensic investigation, and the book’s companion DVD allows readers to immediately test their skills by working with real data.

Book Information

Paperback: 688 pages

Publisher: Addison-Wesley Professional (October 3, 2005)

Language: English

ISBN-10: 9780321240699

ISBN-13: 978-0321240699

ASIN: 0321240693

Product Dimensions: 7 x 1.7 x 9.2 inches

Shipping Weight: 2.2 pounds (View shipping rates and policies)

Average Customer Review: 4.3 out of 5 starsÂ Â See all reviewsÂ (17 customer reviews)

Best Sellers Rank: #222,440 in Books (See Top 100 in Books) #47 inÂ Books > Computers & Technology > Certification > CompTIA #135 inÂ Books > Computers & Technology > Security & Encryption > Privacy & Online Safety #170 inÂ Books > Computers & Technology > Internet & Social Media > Hacking

Customer Reviews

There have been several authoritative books on computer forensics. (Including "Tao of Network Security Monitoring" by Bejtlich.) But this "Real Digital Forensics" book breaks new ground. Not in the theoretical modelling of an attack or countermeasures against it. Instead, there are several indepth case studies, that key off data given in the book’s DVD. And the latter is a DVD, not a CD. The authors needed the multigigabyte capacity to store the provided data. Even then, these are compressed. This should give you some feeling of the book’s emphasis.The authors address a

serious lack in this field. How does someone [you] gain experience analysing a real attack? Without already being employed at a company experiencing such an event? In response, the authors made several scenarios that, they claim, reflect what actual attackers would likely have done.This is an experimental book. There is no overarching elegant theory. You are meant to roll up your sleeves and tackle each case. En route, the book shows how, as a defender, you can use several open source packages to dissect the attack, as well as impose countermeasures. Which is another nice feature. Those packages are free. It makes your forensics education very cheap, in terms of explicit capital outlay.Which is not to say that the book ignores commercial forensic tools. But the authors have a clear preference for open source, with which you might well concur.

There is a real lack of well written books in this category, and this one stands out because it is comprehensive, yet easy to digest and carefully laid out, including case studies to understand data capture and analysis techniques.The progression of the chapters mirror an investigative process; there is discussion of how to properly handle digital evidence, how to make a duplicate of the source data, and how to make sense of what you have collected. There are many real-world type case studies in the beginning of the book that could easily read off the front of any newspaper, and the captured evidence is on the included DVD for you to search to find the "smoking gun". Very well done.The book takes the unusual role of discussing not only the more popular commercial tools like EnCase or Forensic Tool Kit, but also all the open source tools available for free, which is a real plus if you don’t have the deep pockets required for the retail products. The book also does an excellent job of explaining the advantages and shortcomings of all the products discussed, something not often seen in technical books. Along with the open source discussion are source web sites for downloading the tools. The accompanying DVD is packed with stuff to get you started. The book is filled with well illustrated screen shots to help you orient yourself when trying the programs yourself.Be forewarned, this book assumes a pretty reasonable amount of technical knowledge and while it addresses the commercial products available on the Win32 platform, a lot of tools and utilities referenced are written for Linux. While a novice investigator can certainly find value in the book, there is a lot of "meat" that even a seasoned professional will find useful.This is definitely the best book currently available on data forensic investigations.

Bejtlich, Jones and Rose ’Real Digital Forensics’ is as practical as a printed book can be. In a very methodical fashion, the authors cover live response (Unix, Windows), network-based forensics following the NSM model (Unix, Windows), forensics duplication, common forensics analysis

techniques (such as file recovery and Internet history review), hostile binary analysis (Unix, Windows), creating a forensics toolkit and PDA, flash and USB drive forensics. Is that it? :-)Well, there is some other fun stuff too. In other words, the book is both comprehensive and in-depth; following the text and trying the investigations using the enclosed DVD definitely presents an effective way to learn forensic techniques. I would recommend the book to all security professionals (even those not directly involved with forensics on a daily basis).Anton Chuvakin, Ph.D., GCIA, GCIH, GCFA is a Security Strategist with a major security company. He is an author of the book "Security Warrior" and a contributor to "Know Your Enemy II" and the upcoming "Hacker's Challenge III". In his spare time, he maintains his security portal info-secure.org and his blog at O'Reilly. His next book will be about security log analysis.

As an author and instructor, I tend to be pretty picky about the books I choose to read and use in my classes. The authors present the material in a good logical progression. I especially like that it also provides sample evidence on the DVD. Most of the computer forensic books that currently exist contain mostly theory. This is the first good hands-on text that I have seen.The authors have captured a good cross section of scenarios and then guide you through each case in-depth, offering practical solutions when faced with obstacles. The content provides methodologies, techniques, and tools that anyone can use. In addition it covers a variety of media such as USB memory and Palm devices.This is a book that I will definitely keep. It is one of the best forensic investigations books currently on the market and would be a great asset to anyone wishing to enhance their skills.

Estate Investment & House Flipping (Real Estate income, investing, Rental Property) HACKING: Beginner's Crash Course - Essential Guide to Practical: Computer Hacking, Hacking for Beginners, & Penetration Testing (Computer Systems, Computer Programming, Computer Science Book 1) Host Response to Biomaterials: The Impact of Host Response on Biomaterial Selection Social Security: Time for a Life of Leisure - The Guide of Secrets to Maximising Social Security Retirement Benefits and Planning Your Retirement (social ... disability, social security made simple) Android Forensics: Investigation, Analysis and Mobile Security for Google Android Hacking: How to Hack Computers, Basic Security and Penetration Testing (Hacking, How to Hack, Hacking for Dummies, Computer Hacking, penetration testing, basic security, arduino, python) Practical UNIX and Internet Security (Computer Security) Network Security: Private Communications in a Public World (Radia Perlman Series in Computer Networking and Security) Principles of Computer Security: CompTIA Security+ and Beyond [With CDROM] (Official Comptia Guide) Security, Rights, & Liabilities in E-Commerce (Artech House Computer Security Series)