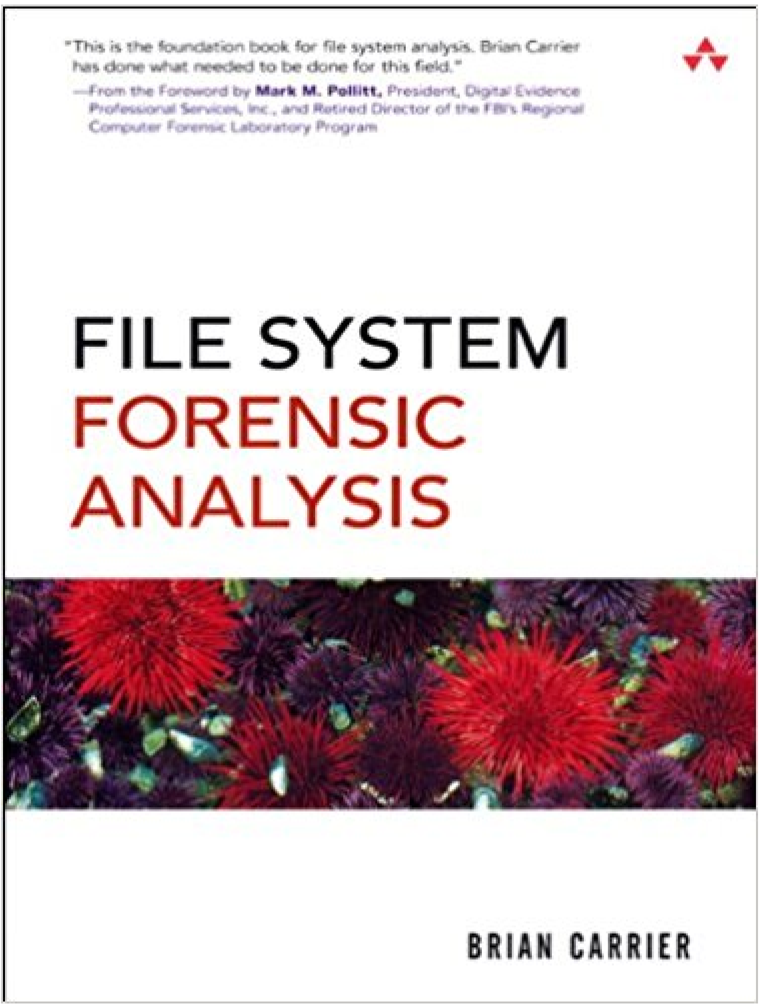
File System Forensic Analysis



"This is the foundation book for file system analysis. Brian Carrier has done what needed to be done for this field."
—From the Foreword by **Mark M. Pollitt,** President, Digital Evidence Professional Services, Inc., and Retired Director of the FBI's Regional Computer Forensic Laboratory Program

FILE SYSTEM
FORENSIC
ANALYSIS

BRIAN CARRIER

Synopsis

The Definitive Guide to File System Analysis: Key Concepts and Hands-on Techniques Ã Â Most digital evidence is stored within the computer&#39;s file system, but understanding how file systems work is one of the most technically challenging concepts for a digital investigator because there exists little documentation. Now, security expert Brian Carrier has written the definitive reference for everyone who wants to understand and be able to testify about how file system analysis is performed. Ã Â Carrier begins with an overview of investigation and computer foundations and then gives an authoritative, comprehensive, and illustrated overview of contemporary volume and file systems: Crucial information for discovering hidden evidence, recovering deleted data, and validating your tools. Along the way, he describes data structures, analyzes example disk images, provides advanced investigation scenarios, and uses today&#39;s most valuable open source file system analysis toolsÃ¢â ¬â •including tools he personally developed. Coverage includes Preserving the digital crime scene and duplicating hard disks for "dead analysis" Identifying hidden data on a disk&#39;s Host Protected Area (HPA) Reading source data: Direct versus BIOS access, dead versus live acquisition, error handling, and more Analyzing DOS, Apple, and GPT partitions; BSD disk labels; and Sun Volume Table of Contents using key concepts, data structures, and specific techniques Analyzing the contents of multiple disk volumes, such as RAID and disk spanning Analyzing FAT, NTFS, Ext2, Ext3, UFS1, and UFS2 file systems using key concepts, data structures, and specific techniques Finding evidence: File metadata, recovery of deleted files, data hiding locations, and more Using The Sleuth Kit (TSK), Autopsy Forensic Browser, and related open source tools When it comes to file system analysis, no other book offers this much detail or expertise. Whether you&#39;re a digital forensics specialist, incident response team member, law enforcement officer, corporate security specialist, or auditor, this book will become an indispensable resource for forensic investigations, no matter what analysis tools you use.

Book Information

Paperback: 600 pages

Publisher: Addison-Wesley Professional; 1 edition (March 27, 2005)

Language: English

ISBN-10: 0321268172

ISBN-13: 978-0321268174

Product Dimensions: 7 x 1.2 x 9 inches

Shipping Weight: 2 pounds (View shipping rates and policies)

Average Customer Review: 4.6 out of 5 stars 62 customer reviews

Best Sellers Rank: #52,666 in Books (See Top 100 in Books) #27 inÃ Â Books > Computers & Technology > Security & Encryption > Privacy & Online Safety #57 inÃ Â Books > Computers & Technology > Networking & Cloud Computing > Network Security #82 inÃ Â Books > Textbooks > Computer Science > Networking

Customer Reviews

The Definitive Guide to File System Analysis: Key Concepts and Hands-on Techniques Most digital evidence is stored within the computer&#039;s file system, but understanding how file systems work is one of the most technically challenging concepts for a digital investigator because there exists little documentation. Now, security expert Brian Carrier has written the definitive reference for everyone who wants to understand and be able to testify about how file system analysis is performed. Carrier begins with an overview of investigation and computer foundations and then gives an authoritative, comprehensive, and illustrated overview of contemporary volume and file systems: Crucial information for discovering hidden evidence, recovering deleted data, and validating your tools. Along the way, he describes data structures, analyzes example disk images, provides advanced investigation scenarios, and uses today&#039;s most valuable open source file system analysis tools&#151;including tools he personally developed. Coverage includes Preserving the digital crime scene and duplicating hard disks for "dead analysis" Identifying hidden data on a disk&#039;s Host Protected Area (HPA) Reading source data: Direct versus BIOS access, dead versus live acquisition, error handling, and more Analyzing DOS, Apple, and GPT partitions; BSD disk labels; and Sun Volume Table of Contents using key concepts, data structures, and specific techniques Analyzing the contents of multiple disk volumes, such as RAID and disk spanning Analyzing FAT, NTFS, Ext2, Ext3, UFS1, and UFS2 file systems using key concepts, data structures, and specific techniques Finding evidence: File metadata, recovery of deleted files, data hiding locations, and more Using The Sleuth Kit (TSK), Autopsy Forensic Browser, and related open source tools When it comes to file system analysis, no other book offers this much detail or expertise. Whether you&#039;re a digital forensics specialist, incident response team member, law enforcement officer, corporate security specialist, or auditor, this book will become an indispensable resource for forensic investigations, no matter what analysis tools you use. Brian Carrier has authored several leading computer forensic tools, including The Sleuth Kit (formerly The @stake Sleuth Kit) and the Autopsy Forensic Browser. He has authored several peer-reviewed conference and journal papers and has created publicly available testing images for forensic tools.

Currently pursuing a Ph.D. in Computer Science and Digital Forensics at Purdue University, he is also a research assistant at the Center for Education and Research in Information Assurance and Security (CERIAS) there. He formerly served as a research scientist at @stake and as the lead for the @stake Response Team and Digital Forensic Labs. Carrier has taught forensics, incident response, and file systems at SANS, FIRST, the @stake Academy, and SEARCH. Brian Carrier&#039;s http://www.digital-evidence.org contains book updates and up-to-date URLs from the book&#039;s references. Ã Â© Copyright Pearson Education. All rights reserved.

Brian Carrier has authored several leading computer forensic tools, including The Sleuth Kit (formerly The @stake Sleuth Kit) and the Autopsy Forensic Browser. He has authored several peer-reviewed conference and journal papers and has created publicly available testing images for forensic tools. Currently pursuing a Ph.D. in Computer Science and Digital Forensics at Purdue University, he is also a research assistant at the Center for Education and Research in Information Assurance and Security (CERIAS) there. He formerly served as a research scientist at @stake and as the lead for the @stake Response Team and Digital Forensic Labs. Carrier has taught forensics, incident response, and file systems at SANS, FIRST, the @stake Academy, and SEARCH. Brian Carrier&#039;s http://www.digital-evidence.org contains book updates and up-to-date URLs from the book&#039;s references. Ã Â© Copyright Pearson Education. All rights reserved.

My understanding is that this book is going to be updated and if so, would be welcome. I read a ton of reviews that praised this book and while I'm sure they are correct, it's not light reading. I also felt that some topics weren't covered too well for someone that isn't a novice but isn't an expert either. It's written very matter-of-factly, so I felt like if you are strong at this topic or have a good solid foundation, you'll be good. If you are a newer person or looking to have a clearer understanding, I feel that this let me down a bit.

This isn't beach reading by any stretch of the imagination. I used the book as a read-along for some online seminars I was doing in digital forensics, and it helped me to understand the concepts better. Brian Carrier is also the author of the Sleuth Kit forensics package. It's a must have if you're doing any kind of digital forensics or data recovery work.

I can't say enough good things about this book and author. The material is beautifully laid out and the writing style is fluid and effortless. The author has a real talent for using metaphors and figures to illustrate elusive concepts.All but the very rarest file systems are covered, and numerous ’screenshots’ show how to use the Linux command prompt and get your hands dirty exploring disks on your own.While this book is a gold standard for digital forensic examiners, it would also be valuable to the computer enthusiast who’s interested in things such as what happens to their hard drive when they format it, exactly what happens during the boot process, etc.I’ve had 3 courses in digital forensics, and this book gives an in-depth discussion of disk level concepts (HPA, FAT, MFT, etc) that were merely glossed over in my formal studies.

I have the pleasure to be working with Dr. Carrier on the Autopsy and Sleuthkit team right now. He’s wonderful to work with, and really knows his stuff. Nowhere is that more present than in this book. If you want to learn about file system analysis the right way, you owe it to yourself to pick this up.

This is an excellent book for an introduction to file systems. This was a required text for a college course in digital forensics and it was a good learning supplement

Great book. Very informative and content is still relevant despite the book’s age.I was able to write a large amount of PowerShell code using the information in this book and correctly parse information from my drive.

Excrutiatingly detailed yet readable and well formatted. THE file system reference for the forensically minded.

OutStanding source. this should be a mandatory book for thoes in digital forensics but also in server administrating and network infrastructure.

Techniques for Forensic Accounting Investigations Forensic Psychological Assessment in Practice: Case Studies (International Perspectives on Forensic Mental Health) Forensic Science: Fundamentals and Investigations (Forensic Science, Fundamentals and Investigations) Practical Homicide Investigation: Tactics, Procedures, and Forensic Techniques, Fifth Edition (Practical Aspects of Criminal and Forensic Investigations) Forensic Pathology, Second Edition (Practical Aspects of Criminal and Forensic Investigations) Forensic Examination of Signatures (Forensic Notes Book 3) Forensic Applications of Gas Chromatography (Analytical Concepts in Forensic Chemistry) Forensic Archaeology: Advances in Theory and Practice (Forensic Science) Forensic Applications of High Performance Liquid Chromatography (Analytical Concepts in Forensic Chemistry) Forensic Anthropology (Inside Forensic Science) Handbook of Forensic Mental Health Services (International Perspectives on Forensic Mental Health)