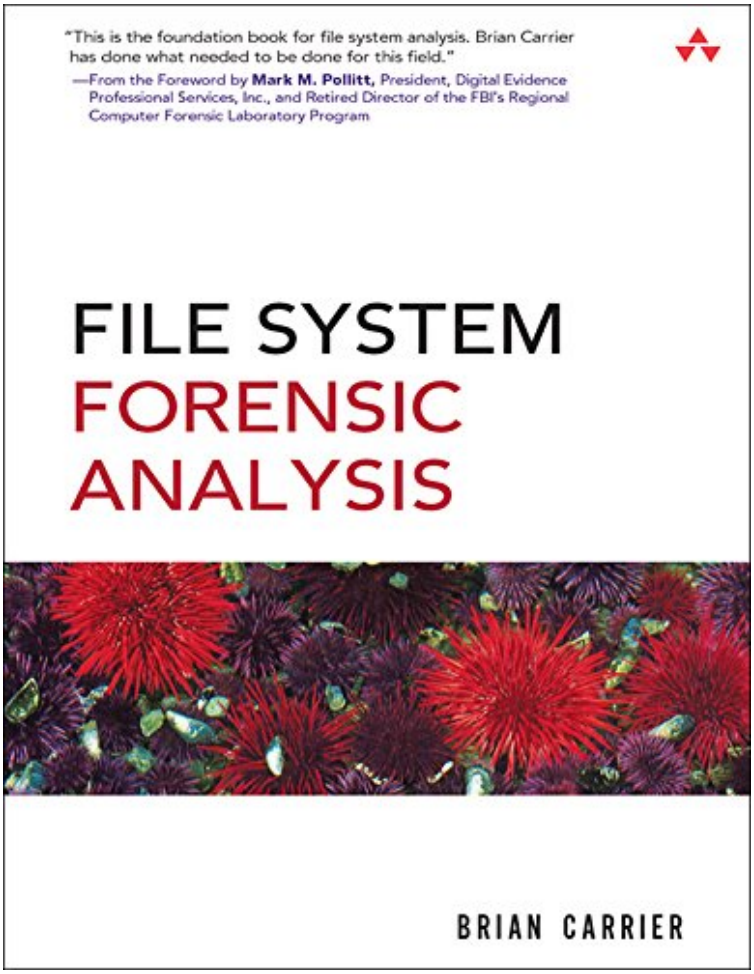
File System Forensic Analysis

Von Brian Carrier
*DOC | *audiobook | ebooks | Download PDF | ePub*



Produktinformation -Verkaufsrang: #422112 in eBooksVerffentlicht am: 2005-03-17Erscheinungsdatum: 2005-03-17File Name: B016N80EZ8 | File size: 50.Mb

Von Brian Carrier : File System Forensic Analysis before purchasing it in order to gage whether or not it would be worth my time, and all praised File System Forensic Analysis:

KundenrezensionenHilfreichste Kundenrezensionen1 von 1 Kunden fanden die folgende Rezension hilfreich. File System ForensicVon Ohne NamenDies Buch kann ich nur empfehlen, sofern mann sich mit Datenrettung beschftigen mchte. Es werden die verschiedenen Filsystem ausfhrlich beschrieben. Ich wrde mir das Buch jederzeit wieder kaufen.

Kurzbeschreibung The Definitive Guide to File System Analysis: Key Concepts and Hands-on Techniques Most digital evidence is stored within the computer'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's most valuable open source file system analysis toolsincluding tools he personally developed. Coverage includes Preserving the digital crime scene and duplicating hard disks for "dead analysis" Identifying hidden data on a disk'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'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. Kurzbeschreibung The Definitive Guide to File System Analysis: Key Concepts and Hands-on Techniques Most digital evidence is stored within the computer'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's most valuable open source file system analysis toolsincluding tools he personally developed. Coverage includes Preserving the digital crime scene and duplicating hard disks for "dead analysis" Identifying hidden data on a disk'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'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. Synopsis This is an advanced cookbook and reference guide for digital forensic practitioners. File System Forensic Analysis focuses on the file system and disk. The file system of a computer is where most files are stored and where most evidence is found; it also the most technically challenging part of forensic analysis. This book offers an overview and detailed knowledge of the file system and disc layout. The overview will allow an investigator to more easily find evidence, recover deleted data, and validate his tools. The cookbook section will show how to use the many open source tools for analysis, many of which Brian Carrier has developed himself.