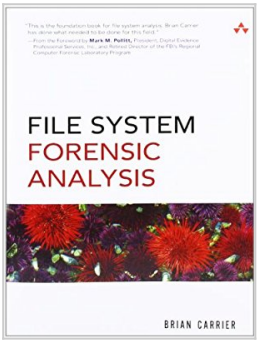

File System Forensic Analysis

By Brian Carrier

File System Forensic Analysis By Brian Carrier

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 tools—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'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.

File System Forensic Analysis

By Brian Carrier

File System Forensic Analysis By Brian Carrier

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 tools—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'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.

File System Forensic Analysis By Brian Carrier Bibliography

- Sales Rank: #303184 in Books
- Published on: 2005-03-27
- Ingredients: Example Ingredients
- Original language: English
- Number of items: 1
- Dimensions: 9.00" h x 1.20" w x 7.00" l,
- Binding: Paperback
- 600 pages

Foreword

Computer forensics is a relatively new field, and over the years it has been called many things: "computer forensics," "digital forensics," and "media analysis" to name a few. It has only been in the past few years that we have begun to recognize that all of our digital devices leave digital breadcrumbs and that these breadcrumbs are valuable evidence in a wide range of inquiries. While criminal justice professionals were some of the first to take an interest in this digital evidence, the intelligence, information security, and civil law fields have enthusiastically adopted this new source of information.

Digital forensics has joined the mainstream. In 2003, the American Society of Crime Laboratory Directors–Laboratory Accreditation Board (ASCLD–LAB) recognized digital evidence as a full-fledged forensic discipline. Along with this acceptance came increased interest in training and education in this field. The Computer Forensic Educator's Working Group (now known as the Digital Forensic Working Group) was formed to assist educators in developing programs in this field. There are now over three-dozen colleges and universities that have, or are, developing programs in this field. More join their ranks each month.

I have had the pleasure of working with many law enforcement agencies, training organizations, colleges, and universities to develop digital forensic programs. One of first questions that I am asked is if I can recommend a good textbook for their course or courses. There have been many books written about this field. Most take a targeted approach to a particular investigative approach, such as incident response or criminal investigation. Some tend to be how-to manuals for specific tools. It has been hard to find a book that provides a solid technical and process foundation for the field...That is, until now.

This book is the foundational book for file system analysis. It is thorough, complete, and well organized. *Brian Carrier has done what needed to be done for this field*. This book provides a solid understanding of both the structures that make up different file systems and how these structures work. Carrier has written this book in such a way that the reader can use what they know about one file system to learn another. This book will be invaluable as a textbook and as a reference and needs to be on the shelf of every digital forensic practitioner and educator. It will also provide accessible reading for those who want to understand subjects such as data recovery.

When I was first approached about writing this Foreword, I was excited! I have know Brian Carrier for a number of years and I have always been impressed with his wonderful balance of incredible technical expertise and his ability to clearly explain not just what he knows but, more importantly, what you need to know. Brian's work on Autopsy and The Sleuth Kit (TSK) has demonstrated his command of this field—his name is a household name in the digital forensic community. I have been privileged to work with Brian in his current role at Purdue University, and he is helping to do for the academic community what he did for the commercial sector: He set a high standard.

So, it is without reservation that I recommend this book to you. It will provide you with a solid foundation in digital media.

Mark M. Pollitt
Former Director of the FBI's Regional Computer Forensic Laboratory Program

Read File System Forensic Analysis By Brian Carrier for online ebook

File System Forensic Analysis By Brian Carrier 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 File System Forensic Analysis By Brian Carrier books to read online.

Online File System Forensic Analysis By Brian Carrier ebook PDF download

File System Forensic Analysis By Brian Carrier Doc

File System Forensic Analysis By Brian Carrier Mobipocket

File System Forensic Analysis By Brian Carrier EPub