1. Record Nr. UNINA9910828815903321

Autore	Cohen Tyler
Titolo	Alternate data storage forensics / / Amber Schroader, Tyler Cohen
Pubbl/distr/stampa	Burlington, MA, : Syngress Pub., c2007
ISBN	1-281-07709-7 9786611077099 0-08-055475-X
Edizione	[1st edition]
Descrizione fisica	1 online resource (337 p.)
Altri autori (Persone)	SchroaderAmber
Disciplina	363.25968
Soggetti	Information storage and retrieval systems Computer crimes
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di contenuto	Front Cover; Alternate Data Storage Forensics; Copyright Page; Contents; Chapter 1. Digital Forensics and Analyzing Data; Introduction; The Evolution of Computer Forensics; Phases of Digital Forensics; Summary; References; Solutions Fast Track; Frequently Asked Questions; Chapter 2. Seizure of Digital Information; Introduction; Defining Digital Evidence; Digital Evidence Seizure Methodology; Factors Limiting the Wholesale Seizure of Hardware; Other Options for Seizing Digital Evidence; Common Threads within Digital Evidence Seizure; Determining the Most Appropriate Seizure Method; Summary Works CitedSolutions Fast Track; Frequently Asked Questions; Chapter 3. Introduction to Handheld Forensics; Digital Forensics; What Is the Handheld Forensic Impact?; Cellular Handling; Evidence Preservation; Maintain a Forensic Data Connection; Analysis and Reporting; Chapter 4. PDA, Blackberry, and iPod Forensic Analysis; Introduction; PDA Forensics; PDA Investigative Tips; Expansion Sleeve Removed; Deploying PDA Forensic Tools; Introduction to the Blackberry; Security for Stored Data; Forensic Examination of a Blackberry; Attacking The Blackberry; Securing the Blackberry (RIM) iPod ForensicsMisuse of an iPod; iPod Investigation; The iPod and Windows; The iPod and Linux; User Accounts; Deleted Files; iPod Time

Issues; Registry Key Containing the iPod's USB/Firewire Serial Number; iPod Tools; Summary; Notes; Solutions Fast Track; Frequently Asked Questions; Chapter 5. E-mail Forensics; Introduction; Where to Start?; Forensic Acquisition; Processing Local Mail Archives; Using Paraben's Network E-mail Examiner (NEMX); Chapter 6. Router Forensics; Introduction; Network Forensics; Searching for Evidence; An Overview of Routers; Hacking Routers; Investigating Routers
Incident ResponseSummary; Solutions Fast Track; Frequently Asked Questions; Chapter 7. Legal Issues of Intercepting WiFi Transmissions; Introduction; WiFi Technology; Understanding WiFi RF; Scanning RF; Eavesdropping on WiFi; Fourth Amendment Expectation of Privacy in WLANs; Summary; Works Cited; Solutions Fast Track; Freyuently Asked Questions; Chapter 8. CD and DVD Forensics; Physical Characteritics of CD and DVD Media; CD Features; CD and DVD Logical Structure; Space Allocation by CD and DVD File Systems; Disc Accessibility Problems; Forensic Binary Images; Collecting CD and DVD Evidence
Preparing for Disc ExaminationChapter 9. MP3 Forensics; Introduction; History; Why Is an iPod Considered Alternative Media?; Imaging and Hashing; Hardware vs . Nonhardware Imaging; Types of iPods; File Systems; "Hacking Tools" and Encrypted Home Directories; Evidence: Normal vs . Not Normal; Analysis Tools; Summary; Index

Sommario/riassunto

Learn to pull "digital fingerprints? from alternate data storage (ADS) devices including: iPod, Xbox, digital cameras and more from the cyber sleuths who train the Secret Service, FBI, and Department of Defense in bleeding edge digital forensics techniques. This book sets a new forensic methodology standard for investigators to use.This book begins by describing how alternate data storage devices are used to both move and hide data. From here a series of case studies using bleeding edge forensic analysis tools demonstrate to readers how to perform forensic investigations on a variety of AD