1.

Record Nr.	UNINA9910782363803321
Autore	Wiles Jack
Titolo	Techno security's guide to e-discovery and digital forensics [[electronic resource] /] / Jack Wiles, lead author ; Tammy Alexander ... [et al.]
Pubbl/distr/stampa	Burlington, Mass., : Syngress Publishing, c2007
ISBN	1-281-76292-X 9786611762926 0-08-055881-X
Edizione	[1st edition]
Descrizione fisica	1 online resource (434 p.)
Disciplina	363.25/968
Soggetti	Computer crimes - Investigation Computer networks - Security measures Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"A comprehensive handbook for investigators, examiners, IT security managers, lawyers, and academia". Includes index.
Nota di contenuto	Cover; Contents; Foreword; Chapter 1: Authentication: Are You Investigating the Right Person?; Introduction; Authentication: What Is It?; An Authentication War Story from 20 Years Ago: The Outside Job; A Second Authentication War Story; Let's Do Something about This Authentication Problem; A Third Authentication War Story; Security Threats in the Future; The Inside Job; A Final Authentication War Story; Key Loggers 101; Some 21st Century Solutions to Authentication; Security Awareness Training; The Rest of the Book; Chapter 2: Digital Forensics: An Overview; Introduction Digital Forensic PrinciplesDigital Environments; Digital Forensic Methodologies; Chapter 3: Working with Other Agencies; Introduction; Building the Relationship; Building Your Package of Information; Don't Shop Your Cases; A Discussion of Agencies; The Big Two: The U.S. Secret Service and the FBI; Other Federal Cyber Crime Investigations Agencies; Chapter 4: Developing an Enterprise Digital Investigative/ Electronic Discovery Capability; Introduction; Identifying Requirements for an Enterprise Digital Investigative/ Electronic Discovery Capability

Administrative Considerations for an Enterprise Digital Investigative/Electronic Discovery CapabilityIdentifying Resources (Software/Hardware/Facility) for Your Team; Chapter 5: Forensic Examination in a Terabyte World; Introduction; Volume Challenges; Network and Hardware Challenges; Future Digital Forensic Solutions; The FTK 2.x Model; Chapter 6: Selecting Equipment for a Computer Forensic Laboratory; Introduction; Forensic Workstations for the Laboratory; Forensic Workstations for the Mobile or Field Laboratory; Hardware Write-Protection Devices; Data Storage; Miscellaneous Items
Chapter 7: Integrating a Quality Management System in a Digital Forensic LaboratoryIntroduction; Quality Planning, Quality Reviews, and Continuous Quality Improvement; Other Challenges: Ownership, Responsibility, and Authority; Chapter 8: Balancing E-discovery Challenges with Legal and IT Requirements; Introduction; Drivers of E-discovery Engineering; Locations, Forms, and Preservation of Electronically Stored Information; Legal and IT Team Considerations for Electronic Discovery; Are You Litigation Ready?; E-discovery Tools; Chapter 9: E-mail Forensics; Introduction; Where to Start
Forensic AcquisitionProcessing Local Mail Archives; Chapter 10: Murder and Money: The Story of Standards, Accreditation, and Certification in Computer Forensics; Introduction; Standards; Accreditation; Certification; Rough Beginnings; Money to the Rescue; Standards and Computer Forensics; Certification Options for the Digital Evidence Analyst; Another Standards Option; Chapter 11: Starting a Career in the Field of Techno Forensics; Introduction; Occupations; Professional Organizations; Professional Certifications; Degree Programs
Appendix A: Death by a Thousand Cuts By Johnny Long with Anthony Kokocinski

Sommario/riassunto

This book provides IT security professionals with the information (hardware, software, and procedural requirements) needed to create, manage and sustain a digital forensics lab and investigative team that can accurately and effectively analyze forensic data and recover digital evidence, while preserving the integrity of the electronic evidence for discovery and trial.IDC estimates that the U.S. market for computer forensics will be grow from 252 million in 2004 to 630 million by 2009. Business is strong outside the United States, as well. By 2011, the estimated international market w