

1. Record Nr.	UNINA9910452749303321
Autore	Watson David (David Lilburn)
Titolo	Digital forensics processing and procedures : meeting the requirements of ISO 17020, ISO 17025, ISO 27001 and best practice requirements // David Watson, Andrew Jones
Pubbl/distr/stampa	Amsterdam : , : Syngress, , [2013] ©2013
ISBN	1-59749-745-2
Edizione	[1st edition]
Descrizione fisica	1 online resource (914 p.)
Altri autori (Persone)	JonesAndrew
Disciplina	363.250285
Soggetti	Computer crimes - Investigation Evidence preservation - Standards Forensic sciences - Standards Computer science Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Front Cover; Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practices ...; Copyright; Contents; About the Authors; Technical Editor Bio; Acknowledgments; Preface; Chapter 1: Introduction; 1.1. Introduction; 1.1.1. What is Digital Forensics?; 1.1.2. The Need for Digital Forensics; 1.1.3. The Purpose of This Book; 1.1.4. Book Structure; 1.1.5. Who Should Read This Book?; 1.1.6. The Need for Procedures in Digital Forensics; 1.1.7. Problems with Electronic Evidence; 1.1.8. The Principles of Electronic Evidence 1.1.9. Nomenclature Used in This Book Appendix 1 - Some types of cases involving Digital Forensics; Criminal cases; Civil cases; Appendix 2 - Growth of hard disk drives for personal computers; Appendix 3 - Disk drive size nomenclature; Chapter 2: Forensic Laboratory Accommodation; 2.1. The building; 2.1.1. General; 2.1.2. Business Case; 2.1.3. Standards; 2.2. Protecting against external and environmental threats; 2.3. Utilities and services; 2.3.1. Signage; 2.3.2. Power and Cabling; 2.3.3. Heating, Ventilation, and Air Conditioning;

2.3.4. Fire Detection and Quenching
2.3.5. Close Circuit Television and Burglar Alarms 2.3.6.
Communications; 2.3.7. Water; 2.4. Physical security; 2.4.1. General;
2.4.2. Building Infrastructure; 2.4.3. Access Control; 2.4.4. On-Site
Secure Evidence Storage; 2.4.5. Clean Room; 2.4.6. Fire Safes; 2.4.7.
Secure Off-Site Storage; 2.5. Layout of the Forensic Laboratory; 2.5.1.
Separation of Space for Specific Roles and Tasks; 2.5.2. Ergonomics;
2.5.3. Personal Workspace; 2.5.4. Size Estimating; 2.5.5. Infrastructure
Rooms; Appendix 1 - Sample outline for a business case; Appendix 2 -
Forensic Laboratory Physical Security Policy
Introduction Purpose; Definitions; Scope; Audience; Policy statements;
Responsibilities; Enforcement, monitoring, and breaches; Ownership;
Review and maintenance; Approval; Chapter 3: Setting up the Forensic
Laboratory; 3.1. Setting up the Forensic Laboratory; 3.1.1. Forensic
Laboratory Terms of Reference; 3.1.2. The Status of the Forensic
Laboratory; 3.1.3. The Forensic Laboratory Principles; 3.1.3.1.
Responsibilities; 3.1.3.2. Integrity; 3.1.3.3. Quality; 3.1.3.4. Efficiency;
3.1.3.5. Productivity; 3.1.3.6. Meet Organizational Expectations;
3.1.3.7. Health and Safety
3.1.3.8. Information Security 3.1.3.9. Management Information
Systems; 3.1.3.10. Qualifications; 3.1.3.11. Training; 3.1.3.12.
Maintaining Employee Competency; 3.1.3.13. Employee Development;
3.1.3.14. Environment; 3.1.3.15. Supervision; 3.1.3.16. Conflicts of
Interest; 3.1.3.17. Legal Compliance; 3.1.3.18. Accountability; 3.1.3.19.
Disclosure and Discovery; 3.1.3.20. Work Quality; 3.1.3.21.
Accreditation and Certification; 3.1.3.22. Membership of Appropriate
Organizations; 3.1.3.23. Obtain Appropriate Personal Certifications;
3.1.4. Laboratory Service Level Agreements
3.1.5. Impartiality and Independence

Sommario/riassunto

This is the first digital forensics book that covers the complete life cycle of digital evidence and the chain of custody. This comprehensive handbook includes international procedures, best practices, compliance, and a companion web site with downloadable forms. Written by world-renowned digital forensics experts, this book is a must for any digital forensics lab. It provides anyone who handles digital evidence with a guide to proper procedure throughout the chain of custody--from incident response through analysis in the lab. A step-by-step guide to designing, building a
