

# DIGITAL FORENSICS PROCESSING AND PROCEDURES

Meeting the Requirements of ISO 17020, ISO 17025,  
ISO 27001 and Best Practice Requirements

David Watson  
Andrew Jones



# Digital Forensics Processing and Procedures

Meeting the Requirements of  
ISO 17020, ISO 17025, ISO 27001 and  
Best Practice Requirements

David Watson

Andrew Jones

Frank Thornton, Technical Editor



AMSTERDAM • BOSTON • HEIDELBERG • LONDON  
NEW YORK • OXFORD • PARIS • SAN DIEGO  
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Syngress is an Imprint of Elsevier

**SYNGRESS**

**Acquiring Editor:** *Chris Katsaropoulos*  
**Editorial Project Manager:** *Heather Scherer*  
**Project Manager:** *Priya Kumaraguruparan*  
**Designer:** *Russell Purdy*

Syngress is an imprint of Elsevier  
225 Wyman Street, Waltham, MA 02451, USA

Copyright © 2013 Elsevier, Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: [www.elsevier.com/permissions](http://www.elsevier.com/permissions).

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

## Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods or professional practices, may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

## Library of Congress Cataloging-in-Publication Data

Watson, David (David Lilburn)

Digital forensics processing and procedures : meeting the requirements of ISO 17020, ISO 17025, ISO 27001 and best practice requirements / David Watson, Andrew Jones.

pages cm

Includes bibliographical references and index.

1. Computer crimes—Investigation. 2. Evidence preservation—Standards. 3. Forensic sciences—Standards. 4. Computer science. I. Title.

HV8079.C65W38 2013

363.250285—dc23

2013021249

## British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

ISBN: 978-1-59749-742-8

Printed in the United States of America

13 14 15 10 9 8 7 6 5 4 3 2 1



Working together  
to grow libraries in  
developing countries

[www.elsevier.com](http://www.elsevier.com) • [www.bookaid.org](http://www.bookaid.org)

**David Lilburn Watson** heads up Forensic Computing Ltd., a specialist digital forensic recovery and investigation company. He is responsible for the coordination and efficient delivery of the digital forensic evidence recovery services and digital investigations, and provides support for a broad range of investigative, information security and risk consulting assignments. He holds the following certifications and degrees:

- Certificate in Governance of Enterprise IT Systems (CGEIT);
- Certificate of Cloud Security Knowledge (CSSK);
- Certified Computer Crime Investigator (CCCI);
- Certified Computer Forensics Technician—Advanced (CCFT);
- Certified Fraud Examiner (CFE);
- Certified Identity Risk Manager (CIRM);
- Certified in Risk and Information System Control (CRISC);
- Certified Information Forensics Investigator (CIFI);
- Certified Information Security Manager (CISM);
- Certified Information System Security Professional (CISSP);
- Certified Information Systems Auditor (CISA);
- Certified Management Consultant (CMC);
- Certified Software Manager (CSM);
- Chartered Fellow (BCS—UK);
- Chartered IT Professional (BCS—UK);
- MSc—Distributed Computer Networks (University of Greenwich);
- MSc—IT Security (University of Westminster)—Distinction;
- MSc—Fraud Risk Management (Nottingham Trent University)—Distinction.

David has also led Forensic Computing Ltd. to ISO 27001, ISO 9001, and BS 25999 (now ISO 22301) certification. Forensic Computing Ltd. complies with ISO 17020 and ISO 17025 but has not sought accreditation. This makes Forensic Computing Ltd. one of the very few consultancies to hold such important credentials in the field of digital forensic services.

Among other achievements, David was the HTCIA Chapter President in the UK and a member of the Metropolitan Police Computer Crime Unit—Expert Advisors Panel.

**Andy Jones** served for 25 years in the British Army's Intelligence Corps. After this he became a manager and a researcher and analyst in the area of information warfare and computer crime at a defense research establishment. In 2002, he left the defense environment to take up a post as a principal lecturer at the University of Glamorgan in the subjects of network security and computer crime and as a researcher on the threats to information systems and computer forensics. At the university, he developed and managed a well-equipped Computer Forensics Laboratory and took the lead on a large number of computer investigations and data recovery tasks. He holds a PhD in the area of threats to information systems. In January 2005, he joined the Security Research Centre at BT where he became a chief researcher and the head of information security research. From BT he went on sabbatical to Khalifa University in the UAE to establish a post graduate programme in Information Security and computer crime and to create a research capability. Andy holds posts as a visiting professor at Edith Cowan University in Perth, Australia, and the University of South Australia in Adelaide.

**Frank Thornton** runs his own technology consulting firm, Blackthorn Information Security, which specializes in digital forensics, network penetration testing, and e-discovery. He holds certifications as a Certified Computer Examiner for the International Association of Forensic Computer Examiners, and as an AccessData Certified Examiner.

Frank's past experiences have been in the fields of Law Enforcement, Forensics, and Computer Sciences. As a detective and forensics expert, he has investigated over

one hundred homicides and thousands of other crime scenes.

Combining both professional interests, he was a member of the workgroup to establish ANSI Standard "ANSI/NIST-CSL 1-1993 Data Format for the Interchange of Fingerprint Information."

Frank has been the author, co-author, contributor, or technical editor for 12 books covering police procedures, digital forensic processes, and information security.

---

## Acknowledgments

The writing of this book has been an epic endeavor that went far beyond what was originally conceived. A large number of people have either knowingly or unknowingly helped, and provided knowledge, inspiration, support, coffee, and sympathy at the right time.

To this end, we would particularly like to thank the following individuals who have helped us in achieving our goal:

Prof. Craig Valli, Frank Thornton, Clive Blake, Matthew Pemble, Phil Swinburne, Bill Millar, Paul Wright, and Steve Anson.

We would also like to thank the project team and the publishing professionals at Elsevier—Heather Scherer,

Chris Katsaropoulos, and Priya Kumaraguruparan for their patience and support during the rather lengthy process.

In addition, we would like to acknowledge our wives and partners, Kath Jones and Pat Sims, for their ongoing tolerance, and editorial and inspirational support when the writing (and sometimes the authors) became difficult.

David would like to thank J. M. M., who was never sure he would make it and M. J. W. R., who said, “He will do well” (Summer 1975)—it just took some time.

Finally, we would like to thank all of you that have taken the trouble to use this book. We hope that the information that we have provided contributes to the smooth running of your laboratories.

Anyone who has been involved in working in or managing a digital forensic laboratory will be aware of the large number of processes and procedures that are essential for the efficient and safe running of the laboratory. If the laboratory also aspires to achieve an accreditation from one of the accreditation bodies such as American Society of Crime Laboratory Directors/Laboratory Crediting Board (ASCLD/LAB) or the International Standards Organization (ISO), then additional processes and procedures will have to be implemented and followed.

This book has been written as a follow-on from the book *Building a Digital Forensic Laboratory*, which, as the name suggests, was aimed at providing guidance for creating and managing the Forensic Laboratory. When that book was written, the aim was to guide the user through the issues that needed to be addressed when a laboratory was created and on the issues of managing it. This book is written to provide the reader with guidance on the policies and procedures that need to be adopted in order to run the Forensic Laboratory in a professional manner and also to allow the Forensic Laboratory to be conformant with the standards that apply to the Forensic Laboratory. The book has not been designed to address the legal issues of any specific jurisdiction, but

instead to provide advice and guidance on good practice in the broader aspects of management of a digital forensic laboratory.

As part of this book, a large number of templates and checklists have been included to provide a “one-stop shop” for the reader. These in themselves have been produced as the result of best practice and an understanding of the requirements from running a number of different forensic laboratories (collectively referred to as the “Forensic Laboratory”). The scope of the policies and procedures that are covered in this book go into a great deal of detail in some areas where it is considered necessary and in other areas less so.

This book is divided into three logical areas: policies and procedures for setting up the Forensic Laboratory, policies and procedures that will be required during the normal running of the Forensic Laboratory, and the policies and procedures that are required for gaining and maintaining accreditation and accredited certification.

As the requirements for the running of the Forensic Laboratory develop, the policies and procedures will inevitably change. In order to address this problem, the following Web site has been created and will contain the most up-to-date material: <http://www.forensic-computing.ltd.uk>.

About the Authors	xv	4.5 Planning	46
Technical Editor Bio	xvii	4.6 Implementation and Operation	47
Acknowledgments	xix	4.7 Performance Assessment	57
Preface	xxi	4.8 Continuous Improvement	62
		4.9 Management Reviews	65
<b>1. Introduction</b>	<b>1</b>	Appendix 1 - Mapping ISO Guide 72 Requirements to PAS 99	66
1.1 Introduction	1	Appendix 2 - PAS 99 Glossary	66
Appendix 1 - Some Types of Cases Involving Digital Forensics	11	Appendix 3 - PAS 99 Mapping to IMS Procedures	67
Appendix 2 - Growth of Hard Disk Drives for Personal Computers	11	Appendix 4 - The Forensic Laboratory Goal Statement	68
Appendix 3 - Disk Drive Size Nomenclature	12	Appendix 5 - The Forensic Laboratory Baseline Measures	68
<b>2. Forensic Laboratory Accommodation</b>	<b>13</b>	Appendix 6 - Environment Policy	68
2.1 The Building	13	Appendix 7 - Health and Safety Policy	68
2.2 Protecting Against External and Environmental Threats	14	Appendix 8 - Undue Influence Policy	69
2.3 Utilities and Services	15	Appendix 9 - Business Continuity Policy	70
2.4 Physical Security	18	Appendix 10 - Information Security Policy	71
2.5 Layout of the Forensic Laboratory	20	Appendix 11 - Access Control Policy	72
Appendix 1 - Sample Outline for a Business Case	21	Appendix 12 - Change or Termination Policy	73
Appendix 2 - Forensic Laboratory Physical Security Policy	22	Appendix 13 - Clear Desk and Clear Screen Policy	73
<b>3. Setting up the Forensic Laboratory</b>	<b>25</b>	Appendix 14 - Continuous Improvement Policy	74
3.1 Setting up the Forensic Laboratory	25	Appendix 15 - Cryptographic Control Policy	74
Appendix 1 - The Forensic Laboratory ToR	33	Appendix 16 - Document Retention Policy	75
Appendix 2 - Cross Reference between ISO 9001 and ISO 17025	35	Appendix 17 - Financial Management Policy	77
Appendix 3 - Conflict of Interest Policy	36	Appendix 18 - Mobile Devices Policy	77
Appendix 4 - Quality Policy	36	Appendix 19 - Network Service Policy	78
<b>4. The Forensic Laboratory Integrated Management System</b>	<b>39</b>	Appendix 20 - Personnel Screening Policy	79
4.1 Introduction	41	Appendix 21 - Relationship Management Policy	80
4.2 Benefits	42	Appendix 22 - Release Management Policy	80
4.3 The Forensic Laboratory IMS	42	Appendix 23 - Service Management Policy	80
4.4 The Forensic Laboratory Policies	43	Appendix 24 - Service Reporting Policy	81
		Appendix 25 - Third-Party Access Control Policy	81
		Appendix 26 - Acceptable use Policy	81
		Appendix 27 - Audit Committee	88
		Appendix 28 - Business Continuity Committee	90
		Appendix 29 - Environment Committee	92



Appendix 30 - Health and Safety Committee	93	Appendix 13 - Likelihood of Occurrence	141
Appendix 31 - Information Security Committee	94	Appendix 14 - Risk Appetite	142
Appendix 32 - Quality Committee	95	Appendix 15 - Security Controls from CobIT and NIST 800-53	142
Appendix 33 - Risk Committee	97	Appendix 16 - Information Classification	150
Appendix 34 - Service Delivery Committee	98	Appendix 17 - The Corporate Risk Register	150
Appendix 35 - Whistle Blowing Policy	99	Appendix 18 - Comparison between Qualitative and Quantitative Methods	150
Appendix 36 - Management Review Agenda	100	Appendix 19 - Mapping Control Functions to ISO 27001	151
Appendix 37 - Document Control Checklist	101	Appendix 20 - Mapping Security Concerns to ISO 27001	155
Appendix 38 - Document Metadata	101	Appendix 21 - SoA Template	161
Appendix 39 - File-Naming Standards	103	Appendix 22 - The Forensic Laboratory's Security Metrics Report	162
Appendix 40 - Watermarks in Use in the Forensic Laboratory	104	Appendix 23 - Mapping ISO 31000 and ISO 27001 to IMS Procedures	175
Appendix 41 - Document Review Form	104		
Appendix 42 - IMS Calendar	105		
Appendix 43 - Audit Plan Letter	105		
Appendix 44 - Audit Reporting Form	106		
Appendix 45 - CAR/PAR Form	106		
Appendix 46 - Opening Meeting Agenda	106		
Appendix 47 - Closing Meeting Agenda	107		
Appendix 48 - Audit Report Template	107		
Appendix 49 - Root Causes for Non-Conformity	107		
<b>5. Risk Management</b>	<b>109</b>	<b>6. Quality in the Forensic Laboratory</b>	<b>177</b>
5.1 A Short History of Risk Management	110	6.1 Quality and Good Laboratory Practice	178
5.2 An Information Security Risk Management Framework	111	6.2 Management Requirements for Operating the Forensic Laboratory	179
5.3 Framework Stage 1—ISMS Policy	114	6.3 ISO 9001 for the Forensic Laboratory	181
5.4 Framework Stage 2: Planning, Resourcing, and Communication	116	6.4 The Forensic Laboratory's QMS	183
5.5 Framework Stage 3: Information Security Risk Management Process	120	6.5 Responsibilities in the QMS	183
5.6 Framework Stage 4: Implementation and Operational Procedures	129	6.6 Managing Sales	185
5.7 Framework Stage 5: Follow-up Procedures	130	6.7 Product and Service Realization	189
Appendix 1 - Sample Communication Plan	132	6.8 Reviewing Deliverables	192
Appendix 2 - Sample Information Security Plan	132	6.9 Signing Off a Case	194
Appendix 3 - Asset Type Examples	133	6.10 Archiving a Case	194
Appendix 4 - Asset Values	133	6.11 Maintaining Client Confidentiality	194
Appendix 5 - Consequences Table	134	6.12 Technical Requirements for the Forensic Laboratory	194
Appendix 6 - Some Common Business Risks	134	6.13 Measurement, Analysis, and Improvement	200
Appendix 7 - Some Common Project Risks	136	6.14 Managing Client Complaints	201
Appendix 8 - Security Threat Examples	137	Appendix 1 - Mapping ISO 9001 to IMS Procedures	203
Appendix 9 - Common Security Vulnerabilities	138	Appendix 2 - Mapping ISO 17025 to IMS Procedures	205
Appendix 10 - Risk Management Policy	139	Appendix 3 - Mapping SWGDE Quality Requirements to IMS Procedures	208
Appendix 11 - The IMS and ISMS Scope Document	139	Appendix 4 - Mapping NIST-150 Quality Requirements to IMS Procedures	212
Appendix 12 - Criticality Ratings	141	Appendix 5 - Mapping ENFSI Quality Requirements to IMS Procedures	213
		Appendix 6 - Mapping FSR Quality Requirements to IMS Procedures	215
		Appendix 7 - Quality Manager, Job Description	218
		Appendix 8 - Business Plan Template	219
		Appendix 9 - Business KPIs	220
		Appendix 10 - Quality Plan Contents	220
		Appendix 11 - Induction Checklist Contents	221

Appendix 12 - Induction Feedback	222	Appendix 8 - Service Desk Manager, Job Description	296
Appendix 13 - Standard Proposal Template	223	Appendix 9 - Incident Manager, Job Description	297
Appendix 14 - Issues to Consider for Case Processing	223	Appendix 10 - Incident Status Levels	298
Appendix 15 - Standard Quotation Contents	223	Appendix 11 - Incident Priority Levels	299
Appendix 16 - Standard Terms and Conditions	224	Appendix 12 - Service Desk Feedback Form	299
Appendix 17 - ERMS Client Areas	224	Appendix 13 - Problem Manager, Job Description	300
Appendix 18 - Cost Estimation Spreadsheet	224	Appendix 14 - Contents of the Forensic Laboratory SIP	301
Appendix 19 - Draft Review Form	225	Appendix 15 - Change Categories	301
Appendix 20 - Client Sign-Off and Feedback Form	225	Appendix 16 - Change Manager, Job Description	301
Appendix 21 - Information Required for Registering a Complaint	225	Appendix 17 - Standard Requirements of a Request for Change	302
Appendix 22 - Complaint Resolution Timescales	225	Appendix 18 - Emergency Change Policy	303
Appendix 23 - Complaint Metrics	226	Appendix 19 - Release Management Policy	303
Appendix 24 - Laboratory Manager, Job Description	226	Appendix 20 - Release Manager, Job Description	303
Appendix 25 - Forensic Analyst, Job Description	227	Appendix 21 - Configuration Management Plan Contents	305
Appendix 26 - Training Agenda	228	Appendix 22 - Configuration Management Policy	305
Appendix 27 - Some Individual Forensic Certifications	229	Appendix 23 - Configuration Manager, Job Description	305
Appendix 28 - Minimum Equipment Records Required by ISO 17025	230	Appendix 24 - Information Stored in the DSL and DHL	306
Appendix 29 - Reference Case Tests	230	Appendix 25 - Capacity Manager, Job Description	307
Appendix 30 - ISO 17025 Reporting Requirements	231	Appendix 26 - Capacity Management Plan	308
Appendix 31 - Standard Forensic Laboratory Report	231	Appendix 27 - Service Management Policy	309
<b>7. IT Infrastructure</b>	<b>233</b>	Appendix 28 - Service Level Manager, Job Description	309
7.1 Hardware	235	Appendix 29 - Service Reporting Policy	310
7.2 Software	238	Appendix 30 - Policy for Maintaining and Servicing IT Equipment	310
7.3 Infrastructure	239	Appendix 31 - ISO 17025 Tool Test Method Documentation	311
7.4 Process Management	241	Appendix 32 - Standard Forensic Tool Tests	311
7.5 Hardware Management	273	Appendix 33 - Forensic Tool Test Report Template	311
7.6 Software Management	281	Appendix 34 - Overnight Backup Checklist	312
7.7 Network Management	285	<b>8. Incident Response</b>	<b>313</b>
Appendix 1 - Some Forensic Workstation Providers	293	8.1 General	314
Appendix 2 - Some Mobile Forensic Workstation Providers	293	8.2 Evidence	316
Appendix 3 - Standard Build for a Forensic Workstation	294	8.3 Incident Response as a Process	317
Appendix 4 - Some Case Processing Tools	294	8.4 Initial Contact	317
Appendix 5 - Policy for Securing IT Cabling	294	8.5 Types of First Response	319
Appendix 6 - Policy for Siting and Protecting IT Equipment	295	8.6 The Incident Scene	323
Appendix 7 - ISO 20000-1 Mapping	295		

8.7 Transportation to the Forensic Laboratory	347	9.16 Statements, Depositions, and Similar	407
8.8 Crime Scene and Seizure Reports	348	9.17 Forensic Software Tools	407
8.9 Postincident Review	348	9.18 Backing up and Archiving a Case	408
Appendix 1 - Mapping ISO 17020 to IMS Procedures	349	9.19 Disclosure	408
Appendix 2 - First Response Briefing Agenda	351	9.20 Disposal	409
Appendix 3 - Contents of the Grab Bag	351	Appendix 1 - Some International Forensic Good Practice	409
Appendix 4 - New Case Form	353	Appendix 2 - Some International and National Standards Relating to Digital Forensics	410
Appendix 5 - First Responder Seizure Summary Log	353	Appendix 3 - Hard Disk Log Details	411
Appendix 6 - Site Summary Form	353	Appendix 4 - Disk History Log	411
Appendix 7 - Seizure Log	354	Appendix 5 - Tape Log Details	411
Appendix 8 - Evidence Locations in Devices and Media	355	Appendix 6 - Tape History Log	411
Appendix 9 - Types of Evidence Typically Needed for a Case	356	Appendix 7 - Small Digital Media Log Details	411
Appendix 10 - The On/Off Rule	356	Appendix 8 - Small Digital Media Device Log	412
Appendix 11 - Some Types of Metadata That may be Recoverable from Digital Images	359	Appendix 9 - Forensic Case Work Log	412
Appendix 12 - Countries with Different Fixed Line Telephone Connections	360	Appendix 10 - Case Processing KPIs	412
Appendix 13 - Some Interview Questions	360	Appendix 11 - Contents of Sample Exhibit Rejection Letter	412
Appendix 14 - Evidence Labeling	362	Appendix 12 - Sample Continuity Label Contents	413
Appendix 15 - Forensic Preview Forms	362	Appendix 13 - Details of the Forensic Laboratory Property Log	413
Appendix 16 - A Traveling Forensic Laboratory	363	Appendix 14 - Exhibit Acceptance Letter Template	413
Appendix 17 - Movement Sheet	363	Appendix 15 - Property Special Handling Log	414
Appendix 18 - Incident Response Report	363	Appendix 16 - Evidence Sought	414
Appendix 19 - Postincident Review Agenda	364	Appendix 17 - Request for Forensic Examination	414
Appendix 20 - Incident Processing Checklist	364	Appendix 18 - Client Virtual Case File Structure	414
<b>9. Case Processing</b>	<b>367</b>	Appendix 19 - Computer Details Log	415
9.1 Introduction to Case Processing	368	Appendix 20 - Other Equipment Details Log	415
9.2 Case Types	372	Appendix 21 - Hard Disk Details Log	415
9.3 Precase Processing	377	Appendix 22 - Other Media Details Log	416
9.4 Equipment Maintenance	381	Appendix 23 - Cell Phone Details Log	416
9.5 Management Processes	384	Appendix 24 - Other Device Details Log	417
9.6 Booking Exhibits in and out of the Secure Property Store	385	Appendix 25 - Some Evidence Found in Volatile Memory	417
9.7 Starting a New Case	387	Appendix 26 - Some File Metadata	417
9.8 Preparing the Forensic Workstation	389	Appendix 27 - Case Progress Checklist	418
9.9 Imaging	389	Appendix 28 - Meeting the Requirements of HB 171	418
9.10 Examination	399	Appendix 29 - Internal Case Report Template	420
9.11 Dual Tool Verification	405	Appendix 30 - Forensic Laboratory Exhibit Log	420
9.12 Digital Time Stamping	405	Appendix 31 - Report Production Checklist	420
9.13 Production of an Internal Case Report	405		
9.14 Creating Exhibits	406		
9.15 Producing a Case Report for External Use	406		

<b>10. Case Management</b>	<b>421</b>		
10.1 Overview	429	Appendix 40 - Tapes by Assignment Report	491
10.2 Hard Copy Forms	430	Appendix 41 - Tapes by Reference Number Report	492
10.3 MARS	430	Appendix 42 - Wiped Tapes Report	492
10.4 Setting up a New Case	445	Appendix 43 - Disposed Tapes Report	492
10.5 Processing a Forensic Case	450	Appendix 44 - Tape History Report	493
10.6 Reports General	459	Appendix 45 - Small Digital Media by Assignment Report	493
10.7 Administrator's Reports	460	Appendix 46 - Small Digital Media by Reference Number Report	493
10.8 User Reports	465	Appendix 47 - Wiped Small Digital Media Report	494
Appendix 1 - Setting up Organisational Details	465	Appendix 48 - Disposed Small Digital Media Report	494
Appendix 2 - Set up the Administrator	467	Appendix 49 - Small Digital Media History Report	494
Appendix 3 - Audit Reports	468	Appendix 50 - Wipe Methods Report	495
Appendix 4 - Manage Users	469	Appendix 51 - Disposal Methods Report	495
Appendix 5 - Manage Manufacturers	470	Appendix 52 - Imaging Methods Report	495
Appendix 6 - Manage Suppliers	470	Appendix 53 - Operating Systems Report	495
Appendix 7 - Manage Clients	471	Appendix 54 - Media Types Report	496
Appendix 8 - Manage Investigators	471	Appendix 55 - Exhibit Type Report	496
Appendix 9 - Manage Disks	471	Appendix 56 - Case Setup Details Report	496
Appendix 10 - Manage Tapes	473	Appendix 57 - Case Movement Report	497
Appendix 11 - Manage Small Digital Media	474	Appendix 58 - Case Computers Report	497
Appendix 12 - Exhibit Details	476	Appendix 59 - Case Non-Computer Evidence Report	498
Appendix 13 - Evidence Sought	477	Appendix 60 - Case Disks Received Report	498
Appendix 14 - Estimates	477	Appendix 61 - Case Other Media Received	499
Appendix 15 - Accept or Reject Case	477	Appendix 62 - Case Exhibits Received Report	500
Appendix 16 - Movement Log	478	Appendix 63 - Case Work Record	500
Appendix 17 - Examination Log	479	Appendix 64 - Cases Rejected Report	500
Appendix 18 - Computer Hardware Details	480	Appendix 65 - Cases Accepted	501
Appendix 19 - Non-Computer Exhibit Details	481	Appendix 66 - Case Estimates Report	501
Appendix 20 - Hard Disk Details	482	Appendix 67 - Cases by Forensic Analyst	501
Appendix 21 - Other Media Details	483	Appendix 68 - Cases by Client Report	502
Appendix 22 - Work Record Details	485	Appendix 69 - Cases by Investigator Report	502
Appendix 23 - Updating Case Estimates	485	Appendix 70 - Case Target Dates Report	503
Appendix 24 - Create Exhibit	486	Appendix 71 - Cases Within "x" Days of Target Date Report	503
Appendix 25 - Case Result	486	Appendix 72 - Cases Past Target Date Report	503
Appendix 26 - Case Backup	486	Appendix 73 - Cases Unassigned Report	503
Appendix 27 - Billing and Feedback	487	Appendix 74 - Case Exhibits Produced Report	504
Appendix 28 - Feedback Received	487	Appendix 75 - Case Results Report	504
Appendix 29 - Organization Report	487	Appendix 76 - Case Backups Report	505
Appendix 30 - Users Report	488	Appendix 77 - Billing Run Report	505
Appendix 31 - Manufacturers Report	488	Appendix 78 - Feedback Letters	505
Appendix 32 - Supplier Report	489	Appendix 79 - Feedback Forms Printout	506
Appendix 33 - Clients Report	489		
Appendix 34 - Investigator's Report	489		
Appendix 35 - Disks by Assignment Report	490		
Appendix 36 - Disks by Reference Number Report	490		
Appendix 37 - Wiped Disks Report	490		
Appendix 38 - Disposed Disks Report	491		
Appendix 39 - Disk History Report	491		

Appendix 80 - Feedback Reporting Summary by Case	506	Appendix 2 - Meeting the Requirements of GAISP	597
Appendix 81 - Feedback Reporting Summary by Forensic Analyst	506	Appendix 3 - Software License Database Information Held	597
Appendix 82 - Feedback Reporting Summary by Client	507	Appendix 4 - Information Security Manager, Job Description	597
Appendix 83 - Complete Case Report	507	Appendix 5 - Logon Banner	599
Appendix 84 - Processed Report	508	Appendix 6 - The Forensic Laboratory's Security Objectives	599
Appendix 85 - Insurance Report	508	Appendix 7 - Asset Details to be Recorded in the Asset Register	599
<b>11. Evidence Presentation</b>	<b>509</b>	Appendix 8 - Details Required for Removal of an Asset	600
11.1 Overview	510	Appendix 9 - Handling Classified Assets	600
11.2 Notes	510	Appendix 10 - Asset Disposal Form	601
11.3 Evidence	510	Appendix 11 - Visitor Checklist	601
11.4 Types of Witness	513	Appendix 12 - Rules of the Data Center	602
11.5 Reports	514	Appendix 13 - User Account Management Form Contents	603
11.6 Testimony in Court	516	Appendix 14 - Teleworking Request Form Contents	604
11.7 Why Cases Fail	518	<b>13. Ensuring Continuity of Operations</b>	<b>605</b>
Appendix 1 - Nations Ratifying the Budapest Convention	519	13.1 Business Justification for Ensuring Continuity of Operations	606
Appendix 2 - Criteria for Selection an Expert Witness	519	13.2 Management Commitment	608
Appendix 3 - The Forensic Laboratory Code of Conduct for Expert Witnesses	520	13.3 Training and Competence	609
Appendix 4 - Report Writing Checklist	521	13.4 Determining the Business Continuity Strategy	613
Appendix 5 - Statement and Deposition Writing Checklist	521	13.5 Developing and Implementing a Business Continuity Management Response	617
Appendix 6 - Non-Verbal Communication to Avoid	522	13.6 Exercising, Maintaining, and Reviewing Business Continuity Arrangements	622
Appendix 7 - Etiquette in Court	522	13.7 Maintaining and Improving the BCMS	626
Appendix 8 - Testimony Feedback Form	523	13.8 Embedding Business Continuity Forensic Laboratory Processes	626
<b>12. Secure Working Practices</b>	<b>525</b>	13.9 BCMS Documentation and Records—General	627
12.1 Introduction	527	Appendix 1 - Supplier Details Held	628
12.2 Principles of Information Security within the Forensic Laboratory	528	Appendix 2 - Headings for Financial and Security Questionnaire	628
12.3 Managing Information Security in the Forensic Laboratory	528	Appendix 3 - Business Continuity Manager, Job Description	628
12.4 Physical Security in the Forensic Laboratory	550	Appendix 4 - Contents of the Forensic Laboratory BIA Form	630
12.5 Managing Service Delivery	559	Appendix 5 - Proposed BCMS Development and Certification Timescales	630
12.6 Managing System Access	560	Appendix 6 - Incident Scenarios	631
12.7 Managing Information on Public Systems	570	Appendix 7 - Strategy Options	631
12.8 Securely Managing IT Systems	571		
12.9 Information Processing Systems Development and Maintenance	576		
Appendix 1 - The Forensic Laboratory SoA	583		

Appendix 8 - Standard Forensic Laboratory BCP Contents	631	15.3 Record Characteristics	670
Appendix 9 - Table of Contents to the Appendix to a BCP	632	15.4 A Records Management Policy	671
Appendix 10 - BCP Change List Contents	633	15.5 Defining the Requirements for Records Management in the Forensic Laboratory	672
Appendix 11 - BCP Scenario Plan Contents	633	15.6 Determining Forensic Laboratory Records to be Managed by the ERMS	675
Appendix 12 - BCP Review Report Template Contents	633	15.7 Using Metadata in the Forensic Laboratory	676
Appendix 13 - Mapping IMS Procedures to ISO 22301	633	15.8 Record Management Procedures	679
Appendix 14 - Differences between ISO 22301 and BS 25999	635	15.9 Business Continuity	686
<b>14. Managing Business Relationships</b>	<b>637</b>	Appendix 1 - MoReq2 Functional Requirements	686
14.1 The Need for Third Parties	638	Appendix 2 - Mapping of ISO 15489 Part 1 to Forensic Laboratory Procedures	686
14.2 Clients	638	Appendix 3 - Types of Legislation and Regulation that will Affect Record Keeping	688
14.3 Third Parties Accessing the Forensic Laboratory	643	Appendix 4 - Forensic Laboratory Record Keeping Policy	688
14.4 Managing Service Level Agreements	644	Appendix 5 - Record Management System Objectives	690
14.5 Suppliers of Office and IT Products and Services	645	Appendix 6 - Business Case Contents	690
14.6 Utility Service Providers	649	Appendix 7 - Outline of the ERMS Project	690
14.7 Contracted Forensic Consultants and Expert Witnesses	649	Appendix 8 - Selection Criteria for an ERMS	691
14.8 Outsourcing	651	Appendix 9 - Initial ERMS Feedback Questionnaire	692
14.9 Use of Sub-Contractors	656	Appendix 10 - Metadata Required in the ERMS	692
14.10 Managing Complaints	657	Appendix 11 - Sample E-mail Metadata	693
14.11 Reasons for Outsourcing Failure	657	Appendix 12 - Forensic Case Records Stored in the ERMS	694
Appendix 1 - Contents of a Service Plan	657	Appendix 13 - Dublin Core Metadata Elements	695
Appendix 2 - Risks to Consider with Third Parties	658	Appendix 14 - National Archives of Australia Metadata Standard	695
Appendix 3 - Contract Checklist for Information Security Issues	658	Appendix 15 - Responsibilities for Records Management in the Forensic Laboratory	696
Appendix 4 - SLA Template for Products and Services for Clients	660	Appendix 16 - Metadata for Records Stored Off-Site	697
Appendix 5 - RFx Descriptions	660	Appendix 17 - Records Classification System	698
Appendix 6 - The Forensic Laboratory RFx Template Checklist	661	Appendix 18 - Disposition Authorization	698
Appendix 7 - RFx Timeline for Response, Evaluation, and Selection	662	Appendix 19 - Additional Requirements for Physical Record Recovery	698
Appendix 8 - Forensic Consultant's Personal Attributes	662	Appendix 20 - Specialized Equipment Needed for Inspection and Recovery of Damaged Records	699
Appendix 9 - Some Tips for Selecting an Outsourcing Service Provider	663		
Appendix 10 - Areas to Consider for Outsourcing Contracts	663		
<b>15. Effective Records Management</b>	<b>665</b>		
15.1 Introduction	666		
15.2 Legislative, Regulatory, and Other Requirements	669		

<b>16. Performance Assessment</b>	<b>701</b>	Appendix 2 - Employee Security Screening Policy Checklist	772
16.1 Overview	701	Appendix 3 - Employment Application Form	773
16.2 Performance Assessment	701	Appendix 4 - Employment Application Form Notes	773
<b>17. Health and Safety Procedures</b>	<b>705</b>	Appendix 5 - Some Documents that can Verify Identity	774
17.1 General	706	Appendix 6 - Document Authenticity Checklist	774
17.2 Planning for OH&S	709	Appendix 7 - Verifying Addresses	775
17.3 Implementation and Operation of the OH&S Management System	719	Appendix 8 - Right to Work Checklist	775
17.4 Checking Compliance with OH&S Requirements	722	Appendix 9 - Reference Authorization	775
17.5 Improving the OH&S Management System	725	Appendix 10 - Statutory Declaration	776
Appendix 1 - OH&S Policy Checklist	725	Appendix 11 - Employer Reference Form	776
Appendix 2 - The Forensic Laboratory OH&S Policy	726	Appendix 12 - Employer's Oral Reference Form	777
Appendix 3 - Health and Safety Manager Job Description	726	Appendix 13 - Confirmation of an Oral Reference Letter	777
Appendix 4 - Some Examples of OH&S Drivers	728	Appendix 14 - Qualification Verification Checklist	777
Appendix 5 - The Forensic Laboratory OH&S Objectives	728	Appendix 15 - Criminal Record Declaration Checklist	778
Appendix 6 - Sample Hazards in the Forensic Laboratory	728	Appendix 16 - Personal Reference Form	778
Appendix 7 - Hazard Identification Form	729	Appendix 17 - Personal Oral Reference Form	779
Appendix 8 - Some Areas for Inspection for Hazards	729	Appendix 18 - Other Reference Form	779
Appendix 9 - Inputs to the Risk Assessment Process	730	Appendix 19 - Other Reference Form	780
Appendix 10 - OH&S Risk Rating	730	Appendix 20 - Employee Security Screening File	780
Appendix 11 - DSE Initial Workstation Self-Assessment Checklist	730	Appendix 21 - Top Management Acceptance of Employment Risk	782
Appendix 12 - DSE Training Syllabus	732	Appendix 22 - Third-Party Employee Security Screening Provider Checklist	782
Appendix 13 - DSE Assessors Checklist	732	Appendix 23 - Recruitment Agency Contract Checklist	782
Appendix 14 - Measurement of OH&S Success	736	Appendix 24 - Investigation Manager, Job Description	783
Appendix 15 - Specific OH&S Incident Reporting Requirements	738	Appendix 25 - Forensic Laboratory System Administrator, Job Description	784
Appendix 16 - OH&S Investigation Checklist and Form Contents	738	Appendix 26 - Employee, Job Description	785
Appendix 17 - OH&S Incident Review	739	Appendix 27 - Areas of Technical Competence	786
Appendix 18 - OHSAS 18001 Mapping to IMS Procedures	740	Appendix 28 - Some Professional Forensic and Security Organizations	787
<b>18. Human Resources</b>	<b>741</b>	Appendix 29 - Training Specification Template	787
18.1 Employee Development	743	Appendix 30 - Training Proposal Evaluation Checklist	788
18.2 Development	759	Appendix 31 - Training Supplier Interview and Presentation Checklist	788
18.3 Termination	769	Appendix 32 - Training Reaction Level Questionnaire	788
Appendix 1 - Training Feedback Form	772	Appendix 33 - The Forensic Laboratory Code of Ethics	789
		Appendix 34 - Termination Checklist	790

<b>19. Accreditation and Certification for a Forensic Laboratory</b>	<b>795</b>	<b>20. Emerging Issues</b>	<b>825</b>
19.1 Accreditation and Certification	796	20.1 Introduction	825
19.2 Accreditation for a Forensic Laboratory	800	20.2 Specific Challenges	826
19.3 Certification for a Forensic Laboratory	812		
Appendix 1 - Typical Conditions of Accreditation	823	Acronyms	835
Appendix 2 - Contents of an Audit Response	823	Bibliography	839
Appendix 3 - Management System Assessment		Index	841
Non-Conformance Examples	823	Glossary (e-only)	e1
Appendix 4 - Typical Closeout Periods	824		



# Introduction

## Table of Contents

<b>1.1 Introduction</b>	<b>1</b>	1.1.8 The Principles of Electronic Evidence	10
1.1.1 What is Digital Forensics?	1	1.1.9 Nomenclature Used in This Book	10
1.1.2 The Need for Digital Forensics	2	<b>Appendix 1 - Some Types of Cases Involving Digital Forensics</b>	<b>11</b>
1.1.3 The Purpose of This Book	3	<b>Criminal Cases</b>	<b>11</b>
1.1.4 Book Structure	3	<b>Civil Cases</b>	<b>11</b>
1.1.5 Who Should Read This Book?	3	<b>Appendix 2 - Growth of Hard Disk Drives for Personal Computers</b>	<b>11</b>
1.1.6 The Need for Procedures in Digital Forensics	4	<b>Appendix 3 - Disk Drive Size Nomenclature</b>	<b>12</b>
1.1.7 Problems with Electronic Evidence	5		

## 1.1 INTRODUCTION

### 1.1.1 What is Digital Forensics?

Digital forensics is a highly specialized and fast-growing field of forensic science relating to the recovery of evidence from digital storage media. Digital forensics applies traditional forensics processes and procedures to this new evidential source.

It can also be referred to as computer forensics, but technically speaking, the term only relates to recovery of evidence from a computer, and not the whole range of digital storage devices that may store digital data to be used as evidence. Computer forensics is also often referred to as cyber forensics.

In this book, as in the case of Forensic Laboratory, the term digital forensics is used.

Digital forensics can be used in civil and criminal cases or any other area of dispute. Each has its own set of handling requirements relevant to the jurisdiction in which the case is being investigated.

Typically, digital forensics involves the recovery of data from digital storage media that may have been lost, hidden, or otherwise concealed or after an incident that has affected the operation of an information processing system. This could be an accidental or deliberate act, carried out by an employee or outsider, or after a malware attack of any type.

No matter what the specific details of the case, the overview of processing a digital forensic case by the Forensic Laboratory follows the same series of processes, interpreted

for the jurisdiction according to case requirements. The processes are as follows:

- preserving the evidence;
- identifying the evidence;
- extracting the evidence;
- documenting the evidence recovered and how it was recovered;
- interpreting the evidence;
- presenting the evidence (either to the client or a court).

Inspection of numerous sources gives differing definitions of "Digital (or Computer) Forensics," depending on the organization and its jurisdiction. They all contain some or all of the elements mentioned above (explicitly defined or implied). The Forensic Laboratory uses the following definition:

The use of scientifically derived, proved, and repeatable methods for:

- preserving the evidence;
- identifying the evidence;
- extracting the evidence;
- documenting the evidence recovered and how it was recovered;
- interpreting the evidence;
- presenting the evidence.

to reconstruct relevant events relating to a given case.

The same processes and techniques are used for any digital media, whether it is a hard disk drive, a SIM card from a