

Contents

	Preface	<i>xv</i>
	List of Contributors	<i>xvii</i>
	List of Figures	<i>xxi</i>
	List of Tables	<i>xxv</i>
	List of Examples	<i>xxvii</i>
	List of Definitions	<i>xxix</i>
	List of Abbreviations	<i>xxxi</i>
1	Introduction	1
	<i>André Årnes</i>	
1.1	Forensic Science	1
1.1.1	History of Forensic Science	2
1.1.2	Locard's Exchange Principle	2
1.1.3	Crime Reconstruction	3
1.1.4	Investigations	3
1.1.5	Evidence Dynamics	4
1.2	Digital Forensics	4
1.2.1	Crimes and Incidents	5
1.2.2	Digital Devices, Media, and Objects	5
1.2.3	Forensic Soundness and Fundamental Principles	5
1.2.4	Crime Reconstruction in Digital Forensics	6
1.3	Digital Evidence	7
1.3.1	Layers of Abstraction	7
1.3.2	Metadata	7
1.3.3	Error, Uncertainty, and Loss	7
1.3.4	Online Bank Fraud – A Real-World Example	8
	1.3.4.1 Modus Operandi	8
	1.3.4.2 The SpyEye Case	8
1.4	Further Reading	9
1.5	Chapter Overview	10
1.6	Comments on Citation and Notation	10

2	The Digital Forensics Process	13
	<i>Anders O. Flaglien</i>	
2.1	Introduction	13
2.1.1	Why Do We Need a Process?	14
2.1.2	Principles of a Forensics Process	15
2.1.3	Finding the Digital Evidence	15
2.1.4	Introducing the Digital Forensics Process	16
2.2	The Identification Phase	17
2.2.1	Preparations and Deployment of Tools and Resources	18
2.2.2	The First Responder	19
2.2.3	At the Scene of the Incident	21
2.2.3.1	Preservation Tasks	22
2.2.4	Dealing with Live and Dead Systems	22
2.2.5	Chain of Custody	23
2.3	The Collection Phase	24
2.3.1	Sources of Digital Evidence	26
2.3.2	Systems Physically Tied to a Location	28
2.3.3	Multiple Evidence Sources	28
2.3.4	Reconstruction	28
2.3.5	Evidence Integrity and Cryptographic Hashes	29
2.3.6	Order of Volatility	30
2.3.7	Dual-Tool Verification	32
2.3.8	Remote Acquisition	32
2.3.9	External Competency and Forensics Cooperation	33
2.4	The Examination Phase	33
2.4.1	Initial Data Source Examination and Preprocessing	34
2.4.2	Forensic File Formats and Structures	35
2.4.3	Data Recovery	35
2.4.4	Data Reduction and Filtering	36
2.4.5	Timestamps	37
2.4.6	Compression, Encryption and Obfuscation	37
2.4.7	Data and File Carving	38
2.4.8	Automation	39
2.5	The Analysis Phase	39
2.5.1	Layers of Abstraction	40
2.5.2	Evidence Types	40
2.5.3	String and Keyword Searches	41
2.5.4	Anti-Forensics	42
2.5.4.1	Computer Media Wiping	42
2.5.4.2	Analysis of Encrypted and Obfuscated Data	42
2.5.5	Automated Analysis	43
2.5.6	Timelining of Events	43
2.5.7	Graphs and Visual Representations	43
2.5.8	Link Analysis	44

2.6	The Presentation Phase	45
2.6.1	The Final Reports	46
2.6.2	Presentation of Evidence and Work Conducted	46
2.6.3	The Chain of Custody Circle Closes	47
2.7	Summary	47
2.8	Exercises	48
3	Cybercrime Law	51
	<i>Inger Marie Sunde</i>	
3.1	Introduction	51
3.2	The International Legal Framework of Cybercrime Law	54
3.2.1	The Individuals Involved in Criminal Activity and in Crime-Preventing Initiatives	54
3.2.2	The National Legal System versus the International Legal Framework	55
3.2.3	Fundamental Rights Relating to Cybercrime Law – The ECHR	56
3.2.3.1	The ECtHR as a Driving Force for Development of Human Rights	57
3.2.3.2	The Right to Bring a Case before the ECtHR	57
3.2.3.3	A Special Note on Transborder Search and Surveillance	58
3.2.3.4	The Connection between Fundamental Rights and the Rule of Law	60
3.2.3.5	The Principle of Legality in the Context of Crime	60
3.2.3.6	The Principle of Legality in the Context of a Criminal Investigation	61
3.2.3.7	The Positive Obligation of the Nation State	63
3.2.3.8	The Right to Fair Trial	64
3.2.3.9	A Special Note on Evidence Rules in Different Legal Systems	68
3.2.3.10	Possible Outcomes of a Violation of Fundamental Rights	69
3.2.4	Special Legal Framework: The Cybercrime Convention	69
3.2.5	Interpretation of Cybercrime Law	72
3.2.5.1	Interpretation of Substantive Criminal Law	72
3.2.5.2	Application of Old Criminal Provisions to New Modes of Conduct	74
3.2.5.3	Interpretation of Procedural Provisions Authorizing Coercive Measures	75
3.3	Digital Crime – Substantive Criminal Law	76
3.3.1	General Conditions for Criminal Liability	77
3.3.2	Real-Life Modus Operandi	80
3.3.3	Offenses against the Confidentiality, Integrity, and Availability of Computer Data and Systems	81
3.3.3.1	Illegal Access and Illegal Interception	82
3.3.3.2	Data and System Interference	85
3.3.3.3	Misuse of Devices	88

3.3.4	Computer-Related Offenses	89
3.3.5	Content-Related Offenses	91
3.3.6	Offenses Related to Infringements of Copyright and Related Rights	93
3.3.7	Racist and Xenophobic Speech	94
3.4	Investigation Methods for Collecting Digital Evidence	95
3.4.1	The Digital Forensic Process in the Context of Criminal Procedure	95
3.4.2	Computer Data That Are Publicly Available	97
3.4.2.1	Transborder Access to Stored Computer Data Where Publicly Available	98
3.4.2.2	Online Undercover Operations	98
3.4.3	Scope and Safeguards of the Investigation Methods	99
3.4.3.1	Suspicion-Based Investigation Methods	99
3.4.3.2	The Scope of the Investigation Methods (Article 14)	99
3.4.3.3	Conditions and Safeguards (Article 15)	100
3.4.3.4	Considerations Relating to Third Parties	102
3.4.4	Search and Seizure (Article 19)	103
3.4.4.1	Main Rules	103
3.4.4.2	Special Issues	104
3.4.5	Production Order	106
3.4.6	Expedited Preservation and Partial Disclosure of Traffic Data	107
3.4.6.1	Real-Time Investigation Methods (Articles 20 and 21)	107
3.5	International Cooperation in Order to Collect Digital Evidence	109
3.5.1	Narrowing the Focus	109
3.5.2	A Special Note on Transborder Access to Digital Evidence	110
3.5.3	Mutual Legal Assistance	111
3.5.3.1	Basic Principles and Formal Steps of the Procedure	111
3.5.3.2	International Conventions Concerning Mutual Legal Assistance	112
3.5.4	International Police Cooperation and Joint Investigation Teams	114
3.6	Summary	115
3.7	Exercises	115
4	Digital Forensic Readiness	117
	<i>Ausra Dilijonaite</i>	
4.1	Introduction	117
4.2	Definition	117
4.3	Law Enforcement versus Enterprise Digital Forensic Readiness	118
4.4	Why? A Rationale for Digital Forensic Readiness	119
4.4.1	Cost	119
4.4.2	Usefulness of Digital Evidence	120
4.4.2.1	Existence of Digital Evidence	121
4.4.2.2	Evidentiary Weight of Digital Evidence	121

4.5	Frameworks, Standards, and Methodologies	123
4.5.1	Standards	124
4.5.1.1	ISO/IEC 27037	124
4.5.1.2	ISO/IEC 17025	124
4.5.1.3	NIST SP 800-86	124
4.5.2	Guidelines	124
4.5.2.1	IOCE Guidelines	124
4.5.2.2	Scientific Working Group on Digital Evidence (SWGDE)	125
4.5.2.3	ENFSI Guidelines	125
4.5.3	Research	125
4.5.3.1	Rowlingson's Ten-Step Process	125
4.5.3.2	Grobler <i>et al.</i> 's Forensic Readiness Framework	125
4.5.3.3	Endicott-Popovsky <i>et al.</i> 's Forensic Readiness Framework	126
4.6	Becoming "Digital Forensic" Ready	126
4.7	Enterprise Digital Forensic Readiness	127
4.7.1	Legal Aspects	127
4.7.2	Policy, Processes, and Procedures	128
4.7.2.1	Risk-Based Approach	128
4.7.2.2	Incident Response versus Digital Forensics	130
4.7.2.3	Policy	130
4.7.2.4	Processes and Procedures	131
4.7.3	People	132
4.7.3.1	Roles and Responsibilities	132
4.7.3.2	Skills, Competencies, and Training	134
4.7.3.3	Awareness Training	134
4.7.4	Technology: Digital Forensic Laboratory	135
4.7.4.1	Accreditation and Certification	135
4.7.4.2	Organizational Framework	136
4.7.4.3	Security Policy or Framework	136
4.7.4.4	Control of Records	136
4.7.4.5	Processes, Procedures, and Lab Routines	137
4.7.4.6	Methodology and Methods	138
4.7.4.7	Personnel	138
4.7.4.8	Code of Conduct	138
4.7.4.9	Tools	138
4.7.5	Technology: Tools and Infrastructure	139
4.7.5.1	Sources of the Digital Evidence	139
4.7.5.2	Validation and Verification of Digital Forensic Tools	140
4.7.5.3	Preparation of Infrastructure	141
4.7.6	Outsourcing Digital Forensic Capabilities	142
4.7.6.1	Continuous Improvement	143
4.8	Considerations for Law Enforcement	144
4.9	Summary	145
4.10	Exercises	145

5 Computer Forensics 147

Jeff Hamm

5.1 Introduction 147

5.2 Evidence Collection 148

5.2.1 Data Acquisition 149

5.2.1.1 Live Data (Including Memory) 150

5.2.1.2 Forensic Image 152

5.2.2 Forensic Copy 152

5.3 Examination 152

5.3.1 Disk Structures 153

5.3.1.1 Physical Disk Structures 153

5.3.1.2 Logical Disk Structures 156

5.3.2 File Systems 159

5.3.2.1 NTFS (New Technology File System) 163

5.3.2.2 INDX (Index) 173

5.3.2.3 Orphan Files 174

5.3.2.4 EXT2/3/4 (Second, Third, and Fourth Extended Filesystems) 176

5.3.2.5 Operating System Artifacts 177

5.3.2.6 Linux Distributions 183

5.4 Analysis 185

5.4.1 Analysis Tools 185

5.4.2 Timeline Analysis 186

5.4.3 File Hashing 187

5.4.4 Filtering 187

5.4.5 Data Carving 188

5.4.5.1 Files 188

5.4.5.2 Records 188

5.4.5.3 Index Search 189

5.4.6 Memory Analysis 189

5.5 Summary 189

5.6 Exercises 190

6 Mobile and Embedded Forensics 191

Jens-Petter Sandvik

6.1 Introduction 192

6.1.1 Embedded Systems and Consumer Electronics 192

6.1.2 Mobile Phones 194

6.1.2.1 UICC (Formerly Known as a SIM Card) 195

6.1.3 Telecommunication Networks 196

6.1.3.1 GSM Network 196

6.1.3.2 UMTS Networks 198

6.1.3.3 Evolved Packet System (EPS)–Long-Term Evolution (LTE) Networks 198

6.1.3.4 Evidence in the Mobile Network 199

6.1.4 Mobile Devices and Embedded Systems as Evidence 200

6.1.5 Malware and Security Considerations 201

6.1.6	Ontologies for Mobile and Embedded Forensics	202
6.1.6.1	An Acquisition Method Ontology	202
6.1.6.2	Technical Qualities	207
6.1.6.3	Tools Used for Acquisition	207
6.1.6.4	Data Acquisition Methods	208
6.2	Collection Phase	208
6.2.1	Special Considerations for Embedded Systems and Mobile Devices	209
6.2.1.1	Functionality	210
6.2.1.2	Stored Data	210
6.2.1.3	Storage Media	210
6.2.1.4	Security Measures	210
6.2.1.5	Communication Ports and Protocols	210
6.2.2	Handling Electronics – ESD	210
6.2.3	First Contact	212
6.2.3.1	Hazards	212
6.2.3.2	Preservation of Other Traces	213
6.2.3.3	Damages and Unique Characteristics	213
6.2.3.4	State and Information	213
6.2.3.5	Clock Setting	213
6.2.3.6	Investigative Value of Information	213
6.2.4	Physical Acquisition	214
6.2.4.1	Two Approaches to Physical Acquisition	215
6.2.4.2	Chip-Off/In Vitro Acquisition	216
6.2.4.3	JTAG/In-System Acquisition	222
6.2.5	Logical Acquisition of Data	225
6.2.5.1	Manual Inspection	225
6.2.5.2	SIM Acquisition	225
6.2.5.3	SIM Replacement	228
6.2.5.4	Device Backup	228
6.2.5.5	USB Mass Storage	229
6.2.5.6	Media Transfer Protocol	230
6.2.5.7	OBEX	230
6.2.5.8	AT Commands	231
6.2.5.9	Vendor-Specific Protocols	233
6.2.5.10	Android Debug Bridge (ADB)	233
6.2.6	Somewhere between Physical and Logical	234
6.2.6.1	Root Access	235
6.2.6.2	Boot Access	235
6.2.6.3	Encryption Keys	237
6.2.6.4	Flasher Tools	237
6.2.6.5	Chip-Off Continued	238
6.2.7	Commercial Forensic Products	240
6.2.8	What about RAM?	241
6.2.9	Damaged Devices	241
6.2.9.1	External Force	242
6.2.9.2	Water, Liquids, and Blood	243

6.2.10	Wrapping It Up	243
6.2.10.1	Matrix of Information Availability	243
6.2.10.2	Cheat Sheet	245
6.2.10.3	On or Off?	245
6.3	Examination Phase	247
6.3.1	Top-Down: Flash Translation Layer (FTL)	247
6.3.2	Top-Down: Flash File Systems	249
6.3.3	Bottom-Up: Carving	250
6.3.4	Bottom-Up: Keyword Search	250
6.3.5	Technical Deep-Dive: FTL from Nokia 7610 Supernova	251
6.3.6	Technical Deep-Dive: Flash File System – YAFFS	252
6.3.7	Technical Deep-Dive: Structure – SMS PDU	255
6.3.8	Technical Deep-Dive: Structure – SQLite3 Database	261
6.3.9	Technical Deep-Dive: Timestamps	265
6.4	Reverse Engineering and Analysis of Applications	267
6.4.1	Methods	267
6.4.1.1	Black Box Testing	267
6.4.1.2	Static Code Analysis	268
6.4.1.3	Runtime Analysis	268
6.4.2	Targets	269
6.4.2.1	Program Functionality	269
6.4.2.2	Data Structures	269
6.4.2.3	Protocols	269
6.4.2.4	Encryption	269
6.5	Summary	270
6.6	Exercises	271
7	Internet Forensics	275
	<i>Petter Christian Bjelland</i>	
7.1	Introduction	275
7.2	Computer Networking	276
7.3	Layers of Network Abstraction	277
7.3.1	The Physical Layer	277
7.3.2	The Data Link, Network, and Transport Layers	277
7.3.2.1	IP Addresses	278
7.3.3	The Session, Presentation, and Application Layers	278
7.4	The Internet	279
7.4.1	Internet Backbone	279
7.4.1.1	Autonomous System (AS)	279
7.4.1.2	Border Gateway Protocol (BGP)	280
7.4.1.3	Internet Service Providers (ISPs)	281
7.4.2	Common Applications	281
7.4.2.1	Domain Name System (DNS)	281
7.4.2.2	Email	283
7.4.2.3	World Wide Web (WWW)	284
7.4.2.4	Peer-to-Peer Networks	285
7.4.2.5	Other Media	285

7.4.3	Caveats	286
7.4.3.1	Network Address Translation (NAT)	286
7.4.3.2	Onion Routing	287
7.4.3.3	Web Shells	288
7.5	Tracing Information on the Internet	289
7.5.1	DNS and Reverse DNS	289
7.5.2	Whois and Reverse Whois	290
7.5.3	Ping and Port Scan	290
7.5.4	Traceroute	291
7.5.5	IP Geolocation	291
7.5.6	Tracing BitTorrent Peers	292
7.5.7	Bitcoin Unconfirmed Transaction Tracing	293
7.6	Collection Phase – Local Acquisition	294
7.6.1	Browser History	295
7.6.2	Browser Cache	295
7.6.3	Browser Cookies	296
7.6.4	Email	297
7.6.5	Messaging and Chats	297
7.6.6	Internet of Things	297
7.7	Collection Phase – Network Acquisition	298
7.7.1	tcpdump and pcap	298
7.7.1.1	Netflow	299
7.7.2	DHCP Logs	299
7.8	Collection Phase – Remote Acquisition	300
7.8.1	Server	300
7.8.1.1	Web Server Logs	300
7.8.1.2	Web Application Logs	300
7.8.1.3	Virtual Hosts	301
7.8.2	Cloud Services	301
7.8.3	Open Sources	302
7.8.3.1	Personal Information	302
7.8.3.2	User Accounts	303
7.8.3.3	Contact Lists	303
7.8.3.4	Publication of Content	303
7.8.3.5	Interaction with Content	303
7.8.3.6	Public Interaction	304
7.8.3.7	Association with Groups and Communities	304
7.9	Other Considerations	304
7.9.1	Application Programming Interfaces (APIs)	304
7.9.1.1	Accessing User Accounts	304
7.9.2	Integrity of Remote Artifacts	305
7.10	The Examination and Analysis Phases	306
7.10.1	Finding Interesting Nodes in Large Networks	306
7.10.2	Divide and Conquer Large Networks	307
7.10.2.1	Clustering	307
7.10.2.2	Community Detection	307

7.10.3	Making Sense of Millions of Events	308
7.10.3.1	Aggregated Timelines	308
7.10.3.2	Temporal Networks	309
7.10.3.3	Heat Maps	310
7.11	Summary	311
7.12	Exercises	312
8	Challenges in Digital Forensics	313
	<i>Katrin Franke and André Årnes</i>	
8.1	Computational Forensics	313
8.1.1	The Objectives of Computational Forensics	314
8.1.1.1	Large-Scale Investigations	314
8.1.1.2	Automation	314
8.1.1.3	Analysis	315
8.1.1.4	Forensic Soundness	315
8.1.2	Disciplines of Computational Forensics	316
8.2	Automation and Standardization	316
8.3	Research Agenda	317
8.4	Summary	317
9	Educational Guide	319
	<i>Stefan Axelsson</i>	
9.1	Teacher's Guide	319
9.2	Student's Guide	320
9.2.1	Journals	320
9.2.2	Conferences and Organizations	321
9.2.3	Professional and Training Organizations	322
9.2.4	Tools	323
9.2.5	Corpuses	323
9.3	Summary	324
	References	325
	Index	333