

# Contents

---

Preface	xvii
Acknowledgments	xviii
Introduction	xix
Author	xxi

## *Section I*

### ENABLING DIGITAL FORENSICS

<b>1</b>	<b>Understanding Digital Forensics</b>	<b>2</b>
	Introduction	2
	The Role of Technology in Crime	2
	History of Digital Crime and Forensics	4
	Prologue (1960s–1980s)	4
	Infancy (1980–1995)	5
	Childhood (1995–2005)	6
	Adolescence (2005–2015)	7
	The Future (2015 and Beyond)	8
	Evolutionary Cycle of Digital Forensics	9
	“Ad Hoc” Phase	9
	“Structured” Phase	10
	“Enterprise” Phase	11
	Principles of Digital Forensics	11
	Evidence Exchange	11
	Forensics Soundness	12
	Authenticity and Integrity	13
	Chain of Custody	14
	Types of Forensics Investigations	15
	Legal Aspects	16
	Jurisdiction	16
	Digital Forensics Resources	17
	Summary	17

<b>2</b>	<b>Investigative Process Methodology</b>	<b>18</b>
	Introduction	18
	Existing Process Models	18
	Digital Forensics Readiness Model	22
	Summary	23
<b>3</b>	<b>Digital Evidence Management</b>	<b>24</b>
	Introduction	24
	Types of Digital Evidence	24
	Common Sources of Digital Evidence	26
	Log Files	27
	Computer Systems	28
	Infrastructure Devices	29
	Virtual Systems	29
	Cloud Computing	30
	Mobile Devices	31
	External Sources	31
	Federal Rules of Evidence	32
	Investigative Process Methodology	34
	Preparation	35
	Information Security Management	35
	Lab Environment	39
	Hardware and Software	43
	Gathering	45
	Operating Procedures	45
	Processing	50
	Presentation	50
	Evidence Storage Networks	51
	Summary	52
<b>4</b>	<b>Ethics and Conduct</b>	<b>53</b>
	Introduction	53
	Importance of Ethics	53
	Principles of Ethics	53
	Personal Ethics	54
	Professional Ethics	54
	Computer Ethics	54
	Business Ethics	55
	Ethics in Digital Forensics	56
	Certifications and Professional Organizations	56
	Digital Forensics Certification Board (DFCB)	57

	International Association of Computer Investigative Specialists (IACIS)	58
	International Society of Forensics Computer Examiners (ISFCE)	58
	Principles for Digital Forensics	59
	Impartiality and Objectivity	60
	Openness and Disclosure	60
	Confidentiality and Trust	60
	Due Diligence and Duty of Care	60
	Certifications and Accreditations	61
	Summary	61
<b>5</b>	<b>Digital Forensics as a Business</b>	<b>62</b>
	Introduction	62
	The Role of Digital Forensics in an Enterprise	62
	Starting a Digital Forensics Program	63
	Step #1: Understand Business Risks	63
	Step #2: Outline Business Scenarios	64
	Step #3: Establish Governance Framework	66
	Step #4: Enable Technical Execution	69
	Step #5: Define Service Offerings	70
	Maintaining a Digital Forensics Program	70
	Educational Roadmap	71
	Forensics Toolkit Maintenance	71
	Key Performance Indicators (KPI)	72
	Resource Capacity	73
	Challenges and Strategies	75
	Team Placement	75
	Industry Regulation	76
	Political Influences	77
	Summary	77

## Section II

### ENHANCING DIGITAL FORENSICS

<b>6</b>	<b>Understanding Digital Forensic Readiness</b>	<b>80</b>
	Introduction	80
	What Is Digital Forensics Readiness?	80
	Costs and Benefits of Digital Forensics Readiness	82
	Cost Assessment	82

Benefits Analysis	83
Implementing Forensics Readiness	85
Summary	86
<b>7 Defining Business Risk Scenarios</b>	<b>87</b>
Introduction	87
What Is Business Risk?	87
Forensics Readiness Scenarios	88
Scenario #1: Reduce the Impact of Cybercrime	89
Scenario #2: Validate the Impact of Cybercrime or Disputes	90
Mitigating Control Logs	90
Overhead Time and Effort	91
Indirect Business Loss	91
Recovery and Continuity Expenses	92
Scenario #3: Produce Evidence to Support Organizational	
Disciplinary Issues	92
Scenario #4: Demonstrating Compliance with Regulatory	
or Legal Requirements	93
Scenario #5: Effectively Manage the Release of Court-	
Ordered Data	94
Scenario #6: Support Contractual and Commercial	
Agreements	94
Scenario Assessment	95
Summary	95
<b>8 Identify Potential Data Sources</b>	<b>96</b>
Introduction	96
What Is a Data Source?	96
Background Evidence	97
Foreground Evidence	97
Cataloguing Data Sources	98
Phase #1: Prepare an Action Plan	98
Phase #2: Identify Data Sources	99
Phase #3: Document Deficiencies	101
Insufficient Data Availability	101
Unidentified Data Sources	104
External Data Considerations	104
Data Exposure Concerns	105
Forensic Architectures	105
Systems Lifecycle	106
Waterfall and Agile Models	106
Summary	108

<b>9 Determine Collection Requirements</b>	<b>109</b>
Introduction	109
Pre-collection Questions	109
Evidence Collection Factors	112
Best Evidence Rule	112
Time	112
Metadata	113
Cause and Effect	114
Correlation and Association	115
Corroboration and Redundancy	117
Storage Duration	117
Storage Infrastructure	118
Data Security Requirements	119
Summary	120
<b>10 Establishing Legal Admissibility</b>	<b>121</b>
Introduction	121
Legal Admissibility	121
Preservation Challenges	123
Preservation Strategies	124
Administrative Controls	124
Policies	124
Guidelines	124
Standards	124
Procedures	125
Technical Controls	125
Storage Security	125
Integrity Monitoring	126
Cryptographic Algorithms	126
Remote Logging	127
Secure Delivery	128
Physical Controls	128
Deter	128
Detect	129
Deny	129
Delay	130
Summary	130
<b>11 Establish Secure Storage and Handling</b>	<b>131</b>
Introduction	131
Secure Storage Attributes	131

Least Privilege Access	132
End-to-End Cryptography	132
Integrity Checking	133
Physical Security	134
Administrative Governance Foundations	135
Personnel	136
Evidence Storage	137
Evidence Handling	137
Incident and Investigative Response	137
Assurance Controls	138
Backup and Restoration Strategies	138
Near Real-Time Data Replication	139
Data Replication	139
Data Restoration from On-line Backup Media	139
Data Restoration from Off-line Backup Media	140
Summary	140

## 12 Enabling Targeted Monitoring 141

Introduction	141
What Is (un)acceptable Activity?	141
Digital Forensics in Enterprise Security	142
Information Security vs. Cyber Security	144
Defense-in-Depth	145
Traditional Security Monitoring	145
Modern Security Monitoring	146
Positive Security	148
Australian Signal Directorate (ASD)	149
Analytical Techniques	150
Misuse Detection	150
Anomaly Detection	151
Specification-Based Detection	152
Machine Learning	152
Extractive Forensics	153
Inductive Forensics	154
Deductive Forensics	154
Implementation Concerns	156
Summary	156

## 13 Mapping Investigative Workflows 157

Introduction	157
Incident Management Lifecycle	157
Integrating the Digital Forensic Readiness Model	158

Incident Handling and Response	159
Phase #1: Preparation	159
“Event” versus “Incident”	160
Policies, Plans, and Procedures	160
Team Structure and Models	161
Communication and Escalation	163
Escalation Management	164
Phase #2: Respond	166
Detection	166
Analysis	166
Prioritization	168
Phase #3: Restore	169
Containment	169
Eradication and Recovery	170
Phase #4: Learn	171
The Incident Response Team (IRT)	172
The Role of Digital Forensics During an Incident	174
Practitioner	174
Advisor	174
Investigation Workflow	175
Types of Security Investigations	175
Summary	176

## 14 Establish Continuing Education 177

Introduction	177
Types of Education and Training	177
Awareness	178
Basic Knowledge	179
Functional Knowledge	180
Professional Certification	180
Specialized Knowledge	180
Organizational Roles and Responsibilities	182
The Digital Forensics Team	183
Roles	183
Titles	184
An Educational Roadmap	185
Technical Knowledge	186
Introductory	186
Intermediate	187
Advanced	188
Non-Technical Knowledge	189
Introductory	189

	Intermediate	190
	Advanced	191
	Digital Forensics Experts	192
	Summary	194
<b>15</b>	<b>Maintaining Evidence-Based Reporting</b>	<b>195</b>
	Introduction	195
	Importance of Factual Reports	195
	Types of Reports	196
	Creating Understandable Reports	197
	Arranging Written Reports	198
	Inculpatory and Exculpatory Evidence	199
	Summary	200
<b>16</b>	<b>Ensuring Legal Review</b>	<b>201</b>
	Introduction	201
	The Role of Technology in Crime	201
	Laws and Regulations	203
	Information Technology (IT) Law	203
	Cyberlaw or Internet Law	204
	Computer Law	205
	Legal Precedence	207
	Brady Rule: Inculpatory and Exculpatory Evidence	207
	Frye versus Daubert Standard: General Acceptance Testing	208
	Jurisdiction	209
	Technology Counselling	209
	Obtaining Legal Advice	210
	Constraints	210
	Disputes	210
	Employees	211
	Liabilities	211
	Prosecution	211
	Communication	211
	Involving Law Enforcement	212
	Summary	212
<b>17</b>	<b>Accomplishing Digital Forensic Readiness</b>	<b>213</b>
	Introduction	213
	Maintain a Business-Centric Focus	213
	Don't Reinvent the Wheel	214
	Understand Costs and Benefits	214
	Summary	215

## Section III

### INTEGRATING DIGITAL FORENSICS

<b>18</b>	<b>Forensics Readiness in Cloud Environments</b>	<b>218</b>
	Introduction	218
	Brief History of Cloud Computing	218
	What Is Cloud Computing?	219
	Characteristics	220
	Service Models	221
	Delivery Models	221
	Isolation Models	222
	Challenges with Cloud Environments	223
	Mobility	223
	Hyper-Scaling	223
	Containerization	224
	First Responders	224
	Evidence Gathering and Processing	224
	Forensics Readiness Methodology	225
	Step #1: Define Business Risk Scenarios	225
	Step #2: Identify Potential Data Sources	226
	Step #3: Determine Collection Requirements	227
	Enterprise Management Strategies	228
	Cloud Computing Governance	228
	Security and Configuration Standards	229
	Reference Architectures	229
	Step #4: Establish Legal Admissibility	232
	Layers of Trust	232
	Step #5: Establish Secure Storage and Handling	234
	Step #6: Enable Targeted Monitoring	235
	Step #7: Map Investigative Workflows	236
	Phase #1: Preparation	236
	Phase #2: Gathering	237
	Phase #3: Processing	238
	Phase #4: Presentation	238
	Step #8: Establish Continuing Education	238
	General Awareness	239
	Basic Training	239
	Formal Education	239
	Step #9: Maintain Evidence-Based Presentations	240
	Step #10: Ensure Legal Review	240
	Contractual Agreements	241
	Summary	242

<b>19</b>	<b>Forensics Readiness with Mobile Devices</b>	<b>243</b>
	Introduction	243
	Brief History of Mobile Devices	243
	Challenges with Mobile Devices	245
	Loss	245
	Theft	245
	Replacement	246
	Local Storage	246
	Cloud Storage	246
	Encryption	246
	“Burner” Phones	247
	Forensics Readiness Methodology	248
	Step #1: Define Business Risk Scenarios	248
	Step #2: Identify Potential Data Sources	249
	Step #3: Determine Collection Requirements	251
	Enterprise Management Strategies	251
	Step #4: Establish Legal Admissibility	256
	Step #5: Establish Secure Storage and Handling	257
	Step #6: Enable Targeted Monitoring	258
	Step #7: Map Investigative Workflows	260
	Phase #1: Preparation	260
	Phase #2: Gathering	261
	Phase #3: Processing	263
	Phase #4: Presentation	264
	Step #8: Establish Continuing Education	265
	General Awareness	265
	Basic Training	265
	Formal Education	266
	Step #9: Maintain Evidence-Based Presentation	266
	Step #10: Ensure Legal Review	267
	Summary	267
<b>20</b>	<b>Forensics Readiness and the Internet of Things</b>	<b>268</b>
	Introduction	268
	Brief History of the Internet of Things (IoT)	268
	What Is the Internet of Things (IoT)?	269
	Challenges with the Internet of Things (IoT)	270
	Form Factor	271
	Security	271
	Privacy	271

Evidence Gathering and Processing	271
Forensics Toolkits	272
Forensics Readiness Methodology	272
Step #1: Define Business Risk Scenarios	273
Step #2: Identify Potential Data Sources	273
Step #3: Determine Collection Requirements	274
Step #4: Establish Legal Admissibility	275
Zones of Trust	275
Step #5: Establish Secure Storage and Handling	276
Step #6: Enable Targeted Monitoring	277
Step #7: Map Investigative Workflows	278
Phase #1: Preparation	278
Phase #2: Gathering	279
Phase #3: Processing	281
Phase #4: Presentation	283
Step #8: Establish Continuing Education	284
General Awareness	284
Basic Training	285
Formal Education	285
Step #9: Maintain Evidence-Based Presentation	285
Step #10: Ensure Legal Review	286
Discrimination	286
Privacy	287
Security	287
Consent	287
Summary	287

## Section IV

### ADDENDUMS

Addendum A: Tool and Equipment Validation Program	290
Addendum B: Service Catalog	297
Addendum C: Cost-Benefit Analysis	301
Addendum D: Building a Taxonomy	313
Addendum E: Risk Assessment	320
Addendum F: Threat Modeling	336
Addendum G: Data Warehousing Introduction	344
Addendum H: Requirements Analysis	355

## ***Section V***

### **APPENDIXES**

<b>Appendix A: Investigative Process Models</b>	<b>362</b>
<b>Appendix B: Education and Professional Certifications</b>	<b>383</b>
<b>Appendix C: Investigative Workflow</b>	<b>394</b>

## ***Section VI***

### **TEMPLATES**

<b>Template 1: Test Case</b>	<b>400</b>
<b>Template 2: Logbook</b>	<b>404</b>
<b>Template 3: Chain of Custody</b>	<b>405</b>
<b>Template 4: Investigative Final Report</b>	<b>408</b>
<b>Template 5: Service Catalog</b>	<b>411</b>
<b>Template 6: Business Case</b>	<b>412</b>
<b>Template 7: Net Present Value (NPV)</b>	<b>420</b>
<b>Template 8: Threat Risk Assessment</b>	<b>421</b>
<b>Template 9: Data Source Inventory Matrix</b>	<b>426</b>
<b>Template 10: Project Charter</b>	<b>427</b>
<b>Template 11: Requirement Analysis Report</b>	<b>437</b>
<b>Bibliography</b>	<b>444</b>
<b>Resources</b>	<b>456</b>
<b>Glossary</b>	<b>461</b>
<b>Index</b>	<b>469</b>