

# Contents

---

<b><i>Foreword</i></b>		ix
<b><i>Preface</i></b>		xi
<b><i>Acknowledgments</i></b>		xv
<b><i>Author's Note</i></b>		xvii
<b>INTRODUCTION</b>	Investigative Computer Forensics	1
	Changes in Technology	1
	Changes in the Role of the Investigator	2
	What Is Computer Forensics?	4
<b>CHAPTER 1</b>	The Glue	7
	The Relevancy of Truth	8
	Foundations of Digital Evidence	9
	Investigative Objectives	11
	The Investigative Process	11
	Trust	13
	Privacy	14
<b>CHAPTER 2</b>	A Primer on Computers and Networks	17
	The Mechanics of Electronically Stored Information	19
	Optical Drives	25
	The Server	27
	The Router	30
	Application Data	32

	Metadata	35
	Databases	37
	E-mail Mechanics	41
	The IP Address	43
	Computer Time Artifacts	45
	Social Media	45
	Tablets	48
	Cellular Telephones and Smartphones	50
	Audio and Video	52
	The Global Nervous System: Worldwide Data	54
	Fundamentals of Network Traffic	58
	The Firewall	59
	Data- and Traffic-Gathering Applications	61
	Dynamic Data Capture	63
	The Cloud	65
	International Data Security and Privacy Issues	67
<b>CHAPTER 3</b>	Computer Forensic Fundamentals	69
	The Establishment of the Computer Forensic Laboratory	69
	Evidence and Access Controls	73
	The Forensic Workstation	79
	Current Tools and Services	86
	Building a Team and a Process	94
	Computer Forensic Certifications	98
	The Human Quotient	98
	The Devil Is in the Details	124
<b>CHAPTER 4</b>	Investigative Fundamentals	127
	The Investigative Mind-Set	127
	Case Management	128
	Fraud and Investigative Analysis	129
	Information Sources and Records	130
	Investigative Techniques	130
	Surveillance and Interviewing	132
	Trade Secret Theft and IP Investigations	133

---

	Human Resources and Interpersonal Investigations	134
	Reporting and Testifying	136
<b>CHAPTER 5</b>	The Underpinnings of Investigative Computer Forensics	139
	Seizure and Examination of Digital Evidence	140
	Data Classification and Records Management	140
	Deleted Data	143
	Backups and Systems Preservation	145
	Computer Crime Analysis and Reconstruction	147
	The <i>Who, What, Where, How</i> of Data	149
	Contracts Agreements, Third Parties, and Other Headaches	154
	Ethics and Management	155
<b>CHAPTER 6</b>	Tactical Objectives and Challenges in Investigative Computer Forensics	157
	Preparing for the Attack	158
	Early Case Assessment	159
	Investigative Pacing, Timing, and Setting Expectations	160
	Working with Multinational Teams	161
	Collections of Electronic Data in the Cloud and in Social Media	162
	Investigating Internet Service Provider Records	164
	bridging the Actual World with the Cyberworld	165
	Packaging the Findings	165
<b>CHAPTER 7</b>	The Cyber-Firefighters	167
	Incident Response Fundamentals	167
	Data Breaches	170
	Theft and Fraud	172
	Systems Failures	172
	Internal Investigations	173
	The Real-Time Predicament	175
	Building a Global Resource Network	175

	Honeypots and Other Attractive Intel-Gathering Targets	176
	Databases and Structured Data	178
	Organized Crime in the Cyber-Underworld	178
	The Cyber-Underworld in Various Regions	179
	State-Sponsored Cybercrime	181
	Identity Theft	182
	Intellectual Property and Trade Secret Theft	183
	Botnets, Malware, Trojans, and Phishing	184
	Data Breach Vulnerabilities	185
	Hackers and Their Environment	186
<b>CHAPTER 8</b>	E-Discovery Responsibilities	189
	Data Identification	189
	Electronic Discovery Reference Model	190
	E-Discovery Stages	192
	Common E-Discovery and Foreign Data Challenges	196
	Tools, Services, and Technologies	199
	Emerging E-Discovery Realities	202
	European and Asian Observations	205
	Digital Evidence in the Courtroom	207
<b>CHAPTER 9</b>	The Future	209
	Privacy and the Data Ecosystem	209
	Access Controls and the Evolution of Trust	211
	Global Communications Systems in the Cloud	211
	Nanotechnology and Cognitive Computing	212
	Digital Demographics and the Emerging Global Citizen	212
	Extra-National Investigative Networks and the Information Union	214
	Zero Day Forensics	214
	Concluding Thoughts	215
	<b><i>About the Author</i></b>	217
	<b><i>Index</i></b>	219