

Contents at a Glance

<i>Introduction</i>	1
<i>Part I: Digging Out and Documenting Electronic Evidence</i>	7
Chapter 1: Knowing What Your Digital Devices Create, Capture, and Pack Away — Until Revelation Day	9
Chapter 2: Suiting Up for a Lawsuit or Criminal Investigation.....	23
Chapter 3: Getting Authorized to Search and Seize	39
Chapter 4: Documenting and Managing the Crime Scene	55
<i>Part II: Preparing to Crack the Case</i>	71
Chapter 5: Minding and Finding the Loopholes.....	73
Chapter 6: Acquiring and Authenticating E-Evidence	95
Chapter 7: Examining E-Evidence	117
Chapter 8: Extracting Hidden Data	135
<i>Part III: Doing Computer Forensic Investigations</i>	151
Chapter 9: E-Mail and Web Forensics.....	153
Chapter 10: Data Forensics.....	175
Chapter 11: Document Forensics.....	201
Chapter 12: Mobile Forensics.....	219
Chapter 13: Network Forensics	241
Chapter 14: Investigating X-Files: eXotic Forensics.....	265
<i>Part IV: Succeeding in Court</i>	275
Chapter 15: Holding Up Your End at Pretrial	277
Chapter 16: Winning a Case Before You Go to Court	287
Chapter 17: Standing Your Ground in Court	295
<i>Part V: The Part of Tens</i>	311
Chapter 18: Ten Ways to Get Qualified and Prepped for Success.....	313
Chapter 19: Ten Tactics of an Excellent Investigator and a Dangerous Expert Witness.....	319
Chapter 20: Ten Cool Tools for Computer Forensics.....	325

<i>Glossary</i>	331
<i>Index</i>	345

Table of Contents



<i>Introduction</i>	1
Who Should Read This Book?	1
About This Book	2
How to Use This Book	3
What You Don't Need to Read	3
Foolish Assumptions	3
How This Book Is Organized	4
Part I: Digging Out and Documenting Electronic Evidence	4
Part II: Preparing to Crack the Case	4
Part III: Doing Computer Forensic Investigations	4
Part IV: Succeeding in Court	5
Part V: The Part of Tens	5
Glossary	5
About the Web Site and Blog	5
Icons Used in This Book	6
Where to Go from Here	6

Part I: Digging Out and Documenting Electronic Evidence..... **7**

Chapter 1: Knowing What Your Digital Devices Create, Capture, and Pack Away — Until Revelation Day	9
Living and Working in a Recorded World	10
Deleting is a misnomer	10
Getting backed up	12
Delusions of privacy danced in their headsets	13
Giving the Third Degree to Computers, Electronics, and the Internet	13
Answering the Big Questions	14
What is my computer doing behind my back?	15
How does my data get out there?	18
Why can data be discovered and recovered easily?	19
Examining Investigative Methods	20
Getting permission	20
Choosing your forensic tools	20
Knowing what to look for and where	21
Gathering evidence properly	21
Revealing Investigation Results	21
Preparing bulletproof findings	22
Making it through trial	22

Chapter 2: Suiting Up for a Lawsuit or Criminal Investigation 23

Deciphering the Legal Codes	24
Learning about relevancy and admissibility	24
Getting started with electronic discovery.....	26
Deciding what's in and what's not.....	26
Playing by the rules	27
Managing E-Discovery.....	28
Understanding that timing is everything.....	29
Grasping ESI discovery problems.....	30
Avoiding overbroad requests.....	31
Shaping the request.....	32
Stepping through the response.....	32
Conducting the Investigation in Good Faith	34
Deciding Who's Paying the Bill	35

Chapter 3: Getting Authorized to Search and Seize. 39

Getting Authority: Never Start Without It	40
Acknowledging who's the boss (not you!).....	40
Putting together your team	40
Involving external sources.....	42
No warrant, no problem (if it's done legally).....	43
Criminal Cases: Papering Your Behind (CYA)	43
Learning about the case and the target	44
Drafting an affidavit for a search warrant.....	45
Presenting an affidavit for judicial processing.....	48
Civil Cases: Verifying Company Policy	50
Searching with verbal permission (without a warrant).....	51
Obtaining a subpoena	52

Chapter 4: Documenting and Managing the Crime Scene 55

Obsessing over Documentation.....	56
Keeping the chain complete.....	56
Dealing with carbon memories	57
Deciding who gets the evidence first	57
Getting to the truth.....	58
Directing the Scene	59
Papering the trail	59
Recording the scene: Video.....	60
Recording the sounds: Audio	62
Getting the lead out	62
Managing Evidence Behind the Yellow Tape.....	63
Arriving ready to roll: Bringing the right tools	63
Minimizing your presence	64
Stepping Through the Scene	66
Securing the area.....	67
Surveying the scene.....	68
Transporting the e-evidence	69

Part II: Preparing to Crack the Case 71

Chapter 5: Minding and Finding the Loopholes 73

Deciding to Take On a Client..... 74
 Learning about the case and the theory 74
 Finding out the client’s priorities 76
 Timing your work..... 77
 Defining the scope of work 78
 Determining Whether You Can Help the Case 79
 Serving as a resource for the lawyer 79
 Taking an active role 80
 Answering big, blunt questions 81
 Signing on the dotted line..... 82
 Passing the Court’s Standard As a Reliable Witness 82
 Getting your credentials accepted 83
 Impressing opinions on the jury 84
 Going Forward with the Case..... 84
 Digging into the evidence 84
 Organizing and documenting your work 86
 Researching and digging for intelligence..... 87
 Keeping a Tight Forensic Defense 89
 Plugging loopholes 90

Chapter 6: Acquiring and Authenticating E-Evidence 95

Acquiring E-Evidence Properly 95
 Step 1: Determine the Type of Media You’re Working With 97
 Step 2: Find the Right Tool 101
 Finding all the space..... 101
 A write-protect device..... 103
 Sterile media..... 104
 Step 3: Transfer Data..... 105
 Transferring data in the field..... 105
 From computer to computer 110
 From storage device to computer 111
 Step 4: Authenticate the Preserved Data..... 113
 Step 5: Make a Duplicate of the Duplicate..... 116

Chapter 7: Examining E-Evidence 117

The Art of Scientific Inquiry 118
 Gearing Up for Challenges..... 119
 Getting a Handle on Search Terms..... 122
 Defining your search list 123
 Using forensic software to search 124
 Assuming risks 126
 Challenging Your Results: Plants and Frames and Being
 in the Wrong Place..... 128
 Knowing what can go wrong 128
 Looking beyond the file..... 129

Finding No Evidence.....	130
No evidence of who logged in	130
No evidence of how it got there.....	131
Reporting Your Analysis.....	131

Chapter 8: Extracting Hidden Data 135

Recognizing Attempts to Blind the Investigator.....	136
Encryption and compression	137
Data hiding techniques	139
Defeating Algorithms, Hashes, and Keys.....	143
Finding Out-of-Sight Bytes	145
Cracking Passwords	146
Knowing when to crack and when not to crack.....	147
Disarming passwords to get in.....	147
Circumventing passwords to sneak in	149
Decrypting the Encrypted	149
Sloppiness cracks PGP	149
Desperate measures	150

Part III: Doing Computer Forensic Investigations 151

Chapter 9: E-Mail and Web Forensics 153

Opening Pandora's Box of E-Mail	154
Following the route of e-mail packets	154
Becoming Exhibit A	154
Tracking the biggest trend in civil litigation	156
Scoping Out E-Mail Architecture	157
E-mail structures.....	157
E-mail addressing.....	158
E-mail lingo	158
E-mail in motion	159
Seeing the E-Mail Forensics Perspective	160
Dissecting the message.....	160
Expanding headers	160
Checking for e-mail extras	163
Examining Client-Based E-Mail.....	163
Extracting e-mail from clients	164
Getting to know e-mail file extensions	164
Copying the e-mail	166
Printing the e-mail.....	167
Investigating Web-Based Mail.....	167
Searching Browser Files	170
Temporary files	170
Internet history	172
Looking through Instant Messages	173

Chapter 10: Data Forensics	175
Delving into Data Storage	176
The anatomy of a disk drive	176
Microsoft operating systems	178
Apple: HFS	183
Linux/Unix	184
Finding Digital Cavities Where Data Hides	185
Deleted files	185
Non-accessible space	191
RAM	192
Windows Registry	194
Search filtering	195
Extracting Data	196
Rebuilding Extracted Data	199
Chapter 11: Document Forensics	201
Finding Evidential Material in Documents: Metadata	202
Viewing metadata	203
Extracting metadata	206
Honing In on CAM (Create, Access, Modify) Facts	207
Discovering Documents	208
Luring documents out of local storage	209
Finding links and external storage	213
Rounding up backups	215
Chapter 12: Mobile Forensics	219
Keeping Up with Data on the Move	220
Shifting from desktop to handhelds	221
Considering mobile devices forensically	222
Recognizing the imperfect understanding of the technology	223
Making a Device Seizure	225
Mobile phones and SIM cards	225
Personal digital assistants	230
Digital cameras	230
Digital audio recorders	231
Cutting-Edge Cellular Extractions	232
Equipping for mobile forensics	232
Mobile forensic hardware	233
Securing the mobile device	234
Finding mobile data	235
Examining a smart phone step-by-step	236
Chapter 13: Network Forensics	241
Mobilizing Network Forensic Power	242
Identifying Network Components	242
Looking at the Open Systems Interconnection Model (OSI)	244
Cooperating with secret agents and controlling servers	245

Saving Network Data	248
Categorizing the data	248
Figuring out where to store all those bytes.....	250
Re-Creating an Event from Traffic	253
Analyzing time stamps	253
Putting together a data sequence.....	256
Spotting different data streams	258
Looking at Network Forensic Tools	259
Test Access Port (TAP).....	259
Mirrors	261
Promiscuous NIC.....	261
Wireless.....	262
Discovering Network Forensic Vendors	263
Chapter 14: Investigating X-Files: eXotic Forensics	265
Taking a Closer Look at Answering Machines	266
Examining Video Surveillance Systems	266
Cracking Home Security Systems	267
Tracking Automobiles.....	268
Extracting Information from Radio Frequency	
Identification (RFID)	270
Examining Copiers.....	272
Taking a Look On the Horizon	273
 Part IV: Succeeding in Court	 275
Chapter 15: Holding Up Your End at Pretrial	277
Pretrial Motions	278
Motion to suppress evidence	279
Motion in limine	279
Motion to dismiss	279
Other motions	279
Handling Pretrial Hearings	280
Giving a Deposition	281
Swearing to tell truthful opinions	282
Surviving a deposition.....	284
Bulletproofing your opinions	285
Checking your statements	286
Fighting stage fright.....	286
 Chapter 16: Winning a Case Before You Go to Court.....	 287
Working Around Wrong Moves	288
Responding to Opposing Experts.....	289
Dealing with counterparts	289
Formatting your response	289
Responding to affidavits	292
Hardening your testimony.....	294

Chapter 17: Standing Your Ground in Court. 295

- Making Good on Deliverables 296
- Understanding Barroom Brawls in the Courtroom..... 297
 - Managing challenging issues 297
 - Sitting on the stand..... 298
 - Instructing jurors about expert testimony 303
- Presenting E-Evidence to Persuade..... 304
 - Staging a disaster 304
 - Exhibiting like an expert 305
- Communicating to the Court..... 306
 - Giving testimony about the case 306
 - Answering about yourself..... 307
 - Getting paid without conflict..... 309

Part V: The Part of Tens 311

Chapter 18: Ten Ways to Get Qualified and Prepped for Success 313

- The Front Ten: Certifications 313
 - ACE: AccessData 313
 - CCE: Certified Computer Examiner..... 314
 - CFCE: Certified Forensic Computer Examiner..... 314
 - CECS: Certified Electronic Evidence Collection Specialist 314
 - Cisco: Various certifications..... 314
 - CISSP: Certified Information Systems Security Professional..... 315
 - CompTia: Various certifications 315
 - EnCE: Guidance Software..... 315
 - Paraben training..... 315
 - SANS and GCFA: GIAC Certified Forensics Analyst..... 316
- The Back Ten: Journals and Education 316

Chapter 19: Ten Tactics of an Excellent Investigator and a Dangerous Expert Witness 319

- Stick to Finding and Telling the Truth 320
- Don't Fall for Counsel's Tricks in Court..... 320
- Be Irrefutable 321
- Submit a Descriptive, Complete Bill..... 321
- Prepare a Clear, Complete Report..... 322
- Understand Nonverbal Cues 322
- Look 'Em Straight in the Eye 323
- Dress for Your Role As a Professional 323
- Stay Certified and Up-to-Date..... 323
- Know When to Say No..... 324

Chapter 20: Ten Cool Tools for Computer Forensics	325
Computer Forensic Software Tools.....	325
EnCase.....	326
Forensic ToolKit (FTK).....	326
Device Seizure	326
Computer Forensic Hardware.....	327
FRED	327
WiebeTech Forensic Field Kit.....	327
Logicube.....	328
Computer Forensic Laboratories	328
Computer forensic data server	328
Forensic write blockers.....	329
Media wiping equipment.....	330
Recording equipment.....	330
 <i>Glossary</i>	 331
 <i>Index</i>	 345

