TABLE OF CONTENTS

1. Introduction: Purpose and Scope *1*

Purpose 1
Scope 3
What Is Not Covered....................3
Defining Digital Evidence....................4

2. Hard Drive Technology, File Systems, and Computer Forensics *5*

Hard Drive Technology 5
Platters....................6
Low-Level Formatting: Tracks and Sectors 6
High-Level Formatting....................8
Clusters 8
File Systems: File Allocation Table (FAT) 9
Defining Computer Forensics 11
First Responders 13
Mirror or Bit Stream Image.................... 15
Computer Is Not Turned On 16
Much More Than Copying Files 18
Write Blockers 18
Computer Forensics Tool Testing (CFTT).................... 22
Forensic Examination Is Done on the Mirror Image 24
Mirror Images Are Verified with Hash Algorithms 25
Mathematical Certitude—Higher than DNA 26
MD5 Collision.................... 28
SHA Hashes.................... 29
SHA-1 Collision.................... 30
One-Way Hash.................... 31
Hash Algorithms Used for Identifying Known Files 31
National Software Reference Library.................... 33
PhotoDNA 34
Computer Forensic Software Tools.................... 35
Computer Forensic Reports 38
Recovering “Deleted” Files in Unallocated Clusters.................... 39

Why Files Are Not Actually Deleted.. 41
Reversing the Delete Process... 41
"Deleted" Files That Are Completely Overwritten Are Not
Recoverable 45
Defragmenting a Hard Drive 47
Regular Computer Usage Will Overwrite Some Deleted Files............. 48
File Slack.. 49
File Slack and Unallocated Clusters Are Not the Same 50
File Slack Is in Allocated Clusters 51
Ram Slack 52
Physical Level and Logical Level... 52
Deleted Files Remain at the Physical Level... 53
Clusters Are Logical Storage Units Where Active Files Are Stored...... 56
Active File Evidence.. 58
Recycle Bin.. 60
INFO2 File... 61
Recovering File Names 62

3. Computer Forensic Techniques and Sources of Digital Evidence *65*

Keyword Searches 65
GREP.. 67
File Signature Analysis.. 68
File Carving... 69
Windows Registry... 71
Restore Points 73
Page File and Swap File.. 74
Thumbs.db File... 75
Link Files 79
E-mail 81
E-mail Technology 81
E-mail Evidence on Computer Hard Drives...................................... 84
E-mail Headers 89
Web Mail 92
Log Files.. 93
Internet Searches 97
Previews and Gallery Views 101
Anti-Forensics 102

Criticism of the Booby Trap Argument 105
Data Hiding Techniques........ 105
Hiding Files by Changing the File Extension 106
Defendants Argue That Searches Should Be Restricted to Certain File Types 107
Steganography 109
Host Protected Area and Device Configuration Overlay........ 110
Temporary Internet Files (Cache)........ 111
Temporary Internet File Evidence........ 113
Computer Forensics and Child Pornography Found in Temporary Internet Files........ 117
Dominion and Control........ 119
Constructive Possession........ 121
Knowledge of Web Browser Caching........ 123
Only Sophisticated User with Specialized Software Can Access Cache?........ 124
Temporary Internet Files and Unallocated Clusters........ 125
Evidence of Internet Searches Can Help Establish Knowing Possession or Receipt 126
Child Pornography in TIFs Prompts Amendments to Federal and State Laws 127
Index.dat Files 129
Content.IE5 Folder........ 130
What Computer Forensics Cannot Do 131
Secondary Sources 133
Computer Forensics........ 133
Books........ 133
Articles 134
Temporary Internet Files/Cache........ 136

4. Child Pornography Investigations ***137***

National Center for Missing and Exploited Children *(NCMEC)*........ 140
Child Pornography Investigations Using Peer-to-Peer Software........ 142
IP Addresses and Peer-to-Peer Networks........ 143
Newsgroups 146
Internet Relay Chat........ 148
Direct Connection and Fserve 149

Defenses.......... 150
Adult Websites.......... 151
Computer Viruses or Trojans 152
Computer Forensics and the Virus or Trojan Horse Defense.......... 153
Pop-Up Defense 154
Hacker.......... 155
Someone Else Had Access to Defendant's Computer 156
Ostrich Defense.......... 157
Search Terms May Undermine Defenses.......... 158

5. Fourth Amendment and Computers *161*

Fourth Amendment 161
Reasonable Expectation of Privacy.......... 161
Reasonable Expectation of Privacy in Closed Containers.......... 163
Computers as Containers.......... 163
Shared Computers.......... 165
Networked Computers 167
Reasonable Expectation of Privacy in Workplace Computers.......... 168
Internet Communications.......... 170
Fourth Amendment Reasonableness.......... 172
Computers Complicate Reasonableness Analysis.......... 173
Search Warrants 173
Probable Cause 175
Illinois v. Gates.......... 176
Great Deference 177
Probable Cause to Support Seizing and Searching Computers.......... 178
IP Address 178
MAC Address 179
Internet Protocol Version 6 (IPv6).......... 183
Probable Cause and Investigations of Peer-to-Peer Networks.......... 185
Nexus.......... 186
Screen Names and Usernames 188
Wireless Defense.......... 190
Non-Internet Scenarios.......... 192
Private Search Doctrine—Computer Searches by Private Parties 196
Scope of the Private Search.......... 198

Good Faith Exception 198
Good Faith Exception and Computer Searches 200
Membership to Child Pornography Website as Basis for Probable Cause 202
United States v. Gourde 204
Staleness........ 206
Staleness and Computer Searches........ 207
Computer Forensic Recovery of Deleted Files Supports Probable Cause 213
Temporary Internet Files Support Probable Cause 215
Staleness Found by a Few Courts 216
Particularity Requirement 217
Guard Against General Searches 217
Particularity and Computer Searches........ 219
Must a Search Warrant Specifically State That Computers Can Be Seized and Searched? 221
Massive Storage Capacity........ 224
Intermingled Documents 226
Relaxing the Particularity Requirement in Computer Searches 227
Limited to a Particular Crime........ 230
Child Pornography Investigations Raise Particularity Concerns........ 232
Incorporation by Reference........ 235
Special Approach to Computer Searches........ 236
United States v. Carey 238
Carey Extended Tamura Rule........ 240
Carey Has Been Limited 241
Carey Limited to Its Particular Facts........ 241
United States Supreme Court Has Rejected Requiring Search Warrants Be Executed in a Certain Way........ 242
Plain View Doctrine and Computer Searches 247
Plain View Doctrine in Comprehensive Computer Searches........ 249
Everything Comes into Plain View 251
Intermingled Data........ 253
Plain View Doctrine Is Based on Physical Rules........ 253

Subjective Intent and Inadvertence....257
Inadvertence and Searches in the Physical World....258
Abolish the Plain View Exception for Computer Searches?....259
Major Plain View Ruling: United States v. Comprehensive Drug Testing, Inc....260
Strong Dissents....262
Reaction to United States v. Comprehensive Drug Testing, Inc....263
CDT Decision Welcomed by Defendants but Criticized by Other Courts....265
Ninth Circuit Issues Revised En Banc Opinion: CDT III....266
Ramifications of Computer Searches on Plain View Doctrine in Physical Searches....266
Hash Searches and the Fourth Amendment....267
Off-Site Searches: Seizure and Search....271
IPv6 Addresses, MAC Addresses & Off-Site Searches....276
Length of Time to Search a Computer....276
Time Delays May Require Justification....277
Statutory Warrant Requirements....278
Rule 41 of the Federal Rules of Criminal Procedure Amended to Explicitly Recognize Unique Nature of Computer Searches....281
Secondary Sources....282

6. Federal Privacy Statutes ***285***

Introduction....285
Why Federal Privacy Statutes Are Needed....288
Third Party Problem....289
Low Subpoena Burden....291
Private Search Doctrine....291
Content and Non-Content....292
Electronic Communications Privacy Act of 1986 (ECPA)....294
Real-Time and Stored Content and Non-Content....295
ECPA Privacy Shortcomings....296
Lack of Suppression Remedy....297

Wiretap Act, 18 U.S.C. §§ 2510–2522 298
- Real Time Interception 300
- Super Warrant 302
- Interception Contemporaneous with Transmission 304
- Interception of Computer Communications 304
- How Is E-mail Wiretapped? 306
- Exceptions 308
- Consent Exception 309
- Provider Exception 310
- Why the Provider Exception May Not Work in Hacking Investigations 311
- Computer Trespasser Exception 312
- The Need for the Computer Trespasser Exception 313

Stored Communications Act, 18 U.S.C. §§ 2701–2711 314
- Electronic Communication Service ("ECS") and Remote Computing Service ("RCS") 315
- Voluntary Disclosure and Required Disclosure 319
- "Specific and Articulable Facts" Order 322
- Notification 324
- Non-Content Records 325
- Subscriber Information 326
- IP Addresses 326
- Screen Names and E-mail Addresses 333
- Lack of Suppression Remedy 336
- Monitoring by ISPs 337
- Unresolved Issue: Privacy Protection for Opened E-mail 338
- SCA Held Unconstitutional: United States v. Warshak 343

Pen Register Statute, 18 U.S.C. §§ 3121–3127 344
- DRAS—Dialing, Routing, Addressing, or Signaling Information 346
- Overcollection 347

Secondary Sources 351
- Book 351
- Articles 351
- Legislative History 353

***Conclusion* 355**

Appendix: Web Resources 357

Computer Forensics ... 357
Government ... 360
Law Enforcement ... 361
Organizations ... 363
Encryption ... 364
Steganography ... 364

Index 365

MAC address, 179, 181, 183–184, 276
MD5, 25–26, 29, 31–32, 34, 145, 185, 267, 337
MD5 collision, 28–29
message header, 147
mirror image, 15–16, 18, 20, 24– 25, 27, 32, 36, 48, 71, 102, 159, 254, 284

National Center for Missing and Exploited Children (NCMEC), 140, 189, 363
National Software Reference Library (NSRL), 33, 361
networks, 167
newsgroups, 32, 146, 330, 335
nexus, 186, 189, 334
non-content, 292–296, 314, 316, 319, 321, 325–326, 344, 346–349
NTFS, 10

off-site searches, 247, 253, 271, 278, 281–282
one-way hash, 31
oral communications, 296–297, 300, 302, 304
ostrich defense, 151, 157
overcollection, 347
overwritten files, 45, 48

packet sniffer, 304
page files, 36, 74
particularity, 200, 202, 217, 219, 221, 224, 227, 230, 232, 235, 238, 243, 247, 249, 260, 273, 287
peer-to-peer networks, 142–143, 149, 185
peer-to-peer software, 29, 32, 142, 171, 181, 271
Pen Register Statute, 294–296, 344, 346–347
PhotoDNA, 34
physical level, 52–54
plain view doctrine, 240, 247–253, 257–260, 262, 264, 266, 270, 282–283
plain view exception, 248, 267
platters, 6
pop-up defense, 150, 154
Post Office Protocol (POP), 342
preview, 20, 101
private search doctrine, 196, 198, 283, 291, 296
probable cause, 163, 175–178, 182–186, 190, 192, 198, 201–202, 204, 206–207, 213, 215, 217, 244, 248–254, 256, 267, 278–279, 301, 328, 330–331, 334, 353
provider exception, 309–311

ram slack, 52
real time interception, 295, 300, 344
reasonable expectation of privacy, 161, 163, 166–168, 171, 173–174, 196, 198, 237, 288, 290, 293, 299, 301, 350
reasonableness, 172–173, 175, 223, 279, 323
recycle bin, 60–61
remote computing service (RCS), 315–317, 319–321, 339
restore points, 73
Rule 41, 247, 264, 281, 282