Contents

Preface xiii

Acknowledgments xvii

Chapter 1: The Fundamentals of Data 1

Base 2 Numbering System: Binary and Character Encoding 2
Communication in a Two-State Universe 3
Electricity and Magnetism 3
Building Blocks: The Origins of Data 4
Growing the Building Blocks of Data 5
Moving Beyond Base 2 7
American Standard Code for Information Interchange 7
Character Codes: The Basis for Processing Textual Data 10
Extended ASCII and Unicode 10
Summary 12
Notes 13

Chapter 2: Binary to Decimal 15

American Standard Code for Information Interchange 16
Computer as a Calculator 16
Why Is This Important in Forensics? 18
Data Representation 18
Converting Binary to Decimal 19
Conversion Analysis 20
A Forensic Case Example: An Application of the Math 20
Decimal to Binary: Recap for Review 22
Summary 23

Chapter 3: The Power of HEX: Finding Slivers of Data 25

What the HEX? 26
Bits and Bytes and Nibbles 27

Nibbles and Bits 29
Binary to HEX Conversion 30
Binary (HEX) Editor 34
The Needle within the Haystack 39
Summary 41
Notes 42

Chapter 4: Files 43

Opening 44
Files, File Structures, and File Formats 44
File Extensions 45
Changing a File's Extension to Evade Detection 47
Files and the HEX Editor 53
File Signature 55
ASCII Is *Not* Text or HEX 57
Value of File Signatures 58
Complex Files: Compound, Compressed, and Encrypted Files 59
Why Do Compound Files Exist? 60
Compressed Files 61
Forensics and Encrypted Files 64
The Structure of Ciphers 65
Summary 66
Notes 67
Appendix 4A: Common File Extensions 68
Appendix 4B: File Signature Database 73
Appendix 4C: Magic Number Definition 77
Appendix 4D: Compound Document Header 79

Chapter 5: The Boot Process and the Master Boot Record (MBR) 85

Booting Up 87
Primary Functions of the Boot Process 87
Forensic Imaging and Evidence Collection 90
Summarizing the BIOS 92
BIOS Setup Utility: Step by Step 92
The Master Boot Record (MBR) 96
Partition Table 102
Hard Disk Partition 103
Summary 110
Notes 111

Chapter 6: Endianness and the Partition Table 113

The Flavor of Endianness 114
Endianness 116
The Origins of Endian 117
Partition Table within the Master Boot Record 117
Summary 125
Notes 127

Chapter 7: Volume versus Partition 129

Tech Review 130
Cylinder, Head, Sector, and Logical Block Addressing 132
Volumes and Partitions 138
Summary 142
Notes 144

Chapter 8: File Systems—FAT 12/16 145

Tech Review 145
File Systems 147
Metadata 149
File Allocation Table (FAT) File System 153
Slack 157
HEX Review Note 160
Directory Entries 161
File Allocation Table (FAT) 163
How Is Cluster Size Determined? 167
Expanded Cluster Size 169
Directory Entries and the FAT 170
FAT Filing System Limitations 174
Directory Entry Limitations 176
Summary 177
Appendix 8A: Partition Table Fields 179
Appendix 8B: File Allocation Table Values 180
Appendix 8C: Directory Entry Byte Offset Description 181
Appendix 8D: FAT 12/16 Byte Offset Values 182
Appendix 8E: FAT 32 Byte Offset Values 184
Appendix 8F: The Power of 2 186

Chapter 9: File Systems—NTFS and Beyond 189

New Technology File System 189
Partition Boot Record 190

Master File Table 191
NTFS Summary 195
exFAT 196
Alternative Filing System Concepts 196
Summary 203
Notes 204
Appendix 9A: Common NTFS System Defined Attributes 205

Chapter 10: Cyber Forensics: Investigative Smart Practices 207

The Forensic Process 209
Forensic Investigative Smart Practices 211
Step 1: The Initial Contact, the Request 211
Step 2: Evidence Handling 216
Step 3: Acquisition of Evidence 221
Step 4: Data Preparation 229
Time 238
Summary 239
Note 240

Chapter 11: Time and Forensics 241

What Is Time? 241
Network Time Protocol 243
Timestamp Data 244
Keeping Track of Time 245
Clock Models and Time Bounding: The Foundations of Forensic Time 247
MS-DOS 32-Bit Timestamp: Date and Time 248
Date Determination 250
Time Determination 254
Time Inaccuracy 258
Summary 259
Notes 260

Chapter 12: Investigation: Incident Closure 263

Forensic Investigative Smart Practices 264
Step 5: Investigation (Continued) 264
Step 6: Communicate Findings 265
Characteristics of a Good Cyber Forensic Report 266
Report Contents 268
Step 7: Retention and Curation of Evidence 269
Step 8: Investigation Wrap-Up and Conclusion 273

Investigator’s Role as an Expert Witness 273
Summary 279
Notes 280

Chapter 13: A Cyber Forensic Process Summary 283

Binary 284
Binary—Decimal—ASCII 285
Data Versus Code 287
HEX 288
From Raw Data to Files 288
Accessing Files 289
Endianness 290
Partitions 291
File Systems 291
Time 292
The Investigation Process 292
Summary 295

Appendix: Forensic Investigations, ABC Inc. 297

Glossary 303

About the Authors 327

Index 329