

Index

- Access Data, 228
- Active partition, 96, 97,
 - 101, 102, 109, 117,
 - 118, 119, 120
- Address:
 - HEX editor address panel, 37
 - Logical Block Address (LBA),
 - 130, 132–133
- Adobe, 41, 46, 287
- Advanced Encryption Standard (AES), 65
- Apple/Macintosh:
 - boot process in, 86
 - endian designation by, 117
 - file extensions for, 70–72
 - file signature information for, 76
 - file systems of, 152, 153, 202
 - hard drive removal from, 91
 - operating systems, 44, 76, 86, 152, 153, 202
- ASCII (American Standard Code for Information Interchange):
 - binary and decimal values assigned to, 8–9, 16, 17, 32–34, 57, 66, 285–286, 288
 - extended, 10–11
 - HEX equivalent to, 32–34, 55, 57–58, 66, 77, 154–155, 161, 248–249, 288
 - overview of, 7–9
- Bad clusters, 164, 167, 180
- Base 2 numbering system, 2–3.
 - See also* Binary system
- Binary system:
 - ASCII equivalents to, 8–9, 16, 17, 32–34, 57, 66, 285–286, 288
 - binary (HEX) editor, 34–39, 43, 53–57, 66, 98–101, 117–125, 289
 - binary tree filing system, 196–200
 - bits as building blocks of, 4–7, 165–166, 284
 - b-tree filing system, 200–202
 - character codes using, 7–13, 25–42 (*see also* ASCII; Hexadecimal characters; Unicode)
 - decimal equivalents of, 15–24, 26, 29, 32–34, 252–253, 285–287
 - electricity and magnetism relationship to, 3–4

Binary system (*Continued*)

- exponents/power of 2 in, 5–7, 165–166, 186–187, 251–252, 255–256
- fundamentals of, 2–3
- HEX representation of, 22, 23, 25–42, 43, 53–58, 66, 77, 98–101, 117–125, 227, 288
- origins of data in, 4–5

BIOS (Basic Input Output System), 86, 88–96, 107–108

\$Bitmap, 195, 206

Bits:

- ASCII coding scheme using, 7–9
- as binary system building blocks, 4–7, 165–166, 284
- bit-for-bit imaging of evidence, 225–226
- bytes as eight, 8, 18, 27–30, 31 (*see also* Bytes)
- exponential combinations of, 5–7, 165–166, 186–187, 251–252, 255–256
- HEX system using, 27–30, 31
- as origins of data, 4–5
- Unicode/UCS using, 8, 10–12

Books, cataloging of, 147–149, 150, 151, 153, 177

Boot process:

- BIOS function in, 86, 88–96, 107–108
- boot device sequence, 89, 93–95
- booting up, 86, 87
- boot loader in, 92–93, 96, 101–102, 109
- evidence corruption during, 90–93, 94–96, 289–290
- file mounting in, 85–86, 87, 289

HEX editor in, 98–101, 117–125

Master Boot Record in, 95–110, 117–125

partitions/partition table in, 96–97, 101, 102–107, 109, 117–125, 130, 132–144, 179, 190–191, 192

POST function in, 87–88, 92

setup utility in, 92–96

signature words in, 96–97,

101, 107, 109

summary of, 86–87, 107–111

Volume Boot Record in, 98,

153–157, 179–185

write blocking or protection in,

82, 90–91

Braille Encoding System, 10

Bytes:

- byte offsets, 37, 98–101, 120–121, 124, 130, 154, 162–163, 179–185, 190–193, 248–258
- character codes using, 8, 10, 18, 27–30, 31
- cluster size in, 157, 167–170
- endianness by significance of, 114–117
- HEX system using, 27–30, 31
- partition size in, 121, 138
- per sector, 59, 80, 97, 130, 138, 155–156
- signature, 96–97, 101, 107, 109

Case study, 20–22, 25–26, 30–39, 143–144, 208, 214–216, 228–229, 232–234, 235–237, 264–265, 268–269, 297–302

- Cataloging systems, 147–149, 150, 151, 153, 177. *See also* File systems
- Chain of custody, 218–221, 222–223, 228–229, 268
- Character codes:
 - ASCII as, 7–9, 10–11, 16, 17, 32–34, 55, 57–58, 66, 77, 154–155, 160–161, 248–249, 285–286, 288
 - binary system basis for, 7–13, 25–42
 - decimal value for, 16–24, 26, 29, 32, 34, 55, 120–121, 155–156, 172–173, 192–193, 249, 257
 - HEX as, 22, 23, 25–42, 43, 53–58, 66, 77, 98–101, 117–125, 130, 154–156, 161, 162–163, 170–173, 179–185, 190–193, 227–229, 248–258, 288, 289
 - HEX editor character panel, 38–39
 - textual data processing using, 10
 - Unicode/UCS as, 8, 10–12, 16, 18, 57
- Ciphers, 64–65
- Clocks. *See also* Time
- clock manipulation, 246–247
 - clock model, 247–248
 - clock skew, 245–246, 292
 - system clock verification, 89
- Clusters:
 - allocation of, 132, 195, 206
 - bad, 164, 167, 180
 - cluster size, 104, 106, 132, 140, 157, 167–170
 - file system use of, 106, 132, 146–147, 153, 156–157, 164–170, 171–173, 194–195, 206
 - number of clusters needed, 171
 - sectors per cluster, 156–157
- Complex files, 59–65, 79–83, 229
- Compound files, 59–61, 79–83
- Compressed files, 61–64. *See also* ZIP file format
- Confidentiality of data, 64–65, 270, 276–277, 297
- Coordinated Universal Time (UTC), 242, 247, 259
- Creation date and time, 237–238, 244, 253, 258
- Cyber forensic concepts. *See also* Cyber forensic practices
 - boot process (*see* Boot process)
 - endianness (*see* Endianness)
 - evidential data (*see* Data; Evidence)
 - files (*see* Files; File systems)
 - hard drives (*see* Hard drives; Partition; Volumes)
- Cyber forensic practices. *See also* Cyber forensic concepts
 - case study, 20–22, 25–26, 30–39, 143–144, 208, 214–216, 228–229, 232–234, 235–237, 264–265, 268–269, 297–302
 - data preparation, 229–234, 240, 293
 - evidence acquisition, 221–229, 239–240, 293
 - evidence handling, 216–221, 222, 239, 293
 - evidence retention and curation, 269–273, 294
 - forensic process, 208, 209–211, 283–295

- Cyber forensic
 - practices (*Continued*)
 - investigation, 234–238, 240, 263–280, 293–294
 - Investigative Smart Practices, 207–208, 209, 211–238, 239–240, 264–273, 292–294
 - quality control assessment, 278–279
 - reporting, 265–269, 294, 297–302
 - request for investigation, 211–216, 239, 293
 - time and, 238–239, 241–260, 292
- Cylinders:
 - Cylinder, Head and Sector (CHS) fields, 130, 132–138
 - hard drive tracks and cylinders, 130, 132
- Data. *See also* Evidence
 - ASCII coding scheme of, 7–9, 10–11, 16, 17, 32–34, 55, 57–58, 66, 77, 154–155, 160–161, 248–249, 285–286, 288
 - binary system, 2–13, 15–24, 25–42, 43, 53–58, 66, 77, 98–101, 117–125, 165–166, 186–187, 196–202, 227, 251–253, 255–256, 284–287, 288, 289
 - bits as building blocks of, 4–9, 18, 165–166, 284
 - character codes for, 7–13 (*see also* ASCII; Hexadecimal characters; Unicode)
 - confidentiality of, 64–65, 270, 276–277, 297
 - data preparation in cyber forensics, 229–234, 240, 293
 - decimal system, 15–24, 26, 29, 32–34, 55, 120–121, 155–156, 172–173, 192–193, 249, 252–253, 257, 285–287
 - electricity and magnetism relationship to, 3–4
 - encryption of, 64–65
 - endianness of, 113–125, 155–156, 193, 290–291
 - files of (*see* Files)
 - forensic imaging of, 47, 90–92, 110, 221–223, 225–226, 227–229, 239, 269, 293
 - fundamentals of, 1–13
 - hexadecimal representation of, 22, 23, 25–42, 43, 53–58, 66, 77, 98–101, 117–125, 130, 154–156, 160–161, 162–163, 170–173, 179–185, 190–193, 227–229, 248–258, 288, 289
 - HEX-data panel, 38, 40
 - indexing, 231–232, 234
 - metadata, 45, 59–60, 78, 148–153, 191, 206, 237–238, 242, 244–245
 - native format of, 18, 41, 287
 - origins of, 4–5
 - resident, 194
 - searching, 232–234
 - timestamp, 242, 244–250, 252–259, 292
 - Unicode/UCS standard for, 8, 10–12, 16, 18, 57
 - verifying, 231
 - write blocking or protection of, 88, 90–91, 224–225, 226, 228

- Data preparation:
 - data verification in, 231
 - deleted file recovery in, 229–231, 234
 - indexing in, 231–232, 234
 - mounting in, 229
 - preprocessing in, 229
 - searching in, 232–234
 - steps in, 229–234, 240, 293
- Dates. *See also* Time
 - accessed/last accessed date and time, 245
 - chain of custody including, 218–220
 - creation date and time, 237–238, 244, 253, 258
 - date stamps, 243, 248–250
 - days, 251, 253
 - determination of, 250–254
 - directory entry including, 162–163, 181
 - investigation noting discrepancies in, 237–238
 - last modified date and time, 238, 244, 253, 258
 - months, 251, 253
 - order and interpretation of, 113–114
 - search criteria including, 214, 216
 - years, 252–253
- Decimal system:
 - binary equivalents of, 15–24, 26, 29, 32–34, 252–253, 285–287
 - HEX character equivalents to, 26, 29, 32, 34, 55, 120–121, 155–156, 172–173, 192–193, 249, 257
- Defragmentation of hard drives, 146–147, 173
- Directory entries, 162–163, 167, 170–173, 176–177, 181, 244. *See also* Master File Table
- Domino, 226
- DOS (Disk Operating System), Microsoft:
 - boot process in, 92, 101, 118, 122
 - file extensions used by, 71
 - file signatures for, 75
 - file system of, 152
 - partitions in, 118, 122
 - time and date stamps in, 248–250, 252–259, 292
- Dwords, 114, 126
- Electricity and magnetism, 3–4
- Electronic Communications Privacy Act, 213
- Email, evidence acquisition of, 226
- EnCase, 176, 228–229
- Encrypted files, 64–65
- Endianness:
 - big vs. little, 114–117, 290
 - of data, 113–125, 155–156, 193, 290–291
 - origins of, 117
 - partition tables and, 117–125
- Evidence:
 - access rights to, securing, 276–277
 - acquisition of, 221–229, 239–240, 293
 - best evidence rule, 224
 - bit-for-bit imaging of, 225–226

Evidence (*Continued*)

- boot process corruption of, 90–92, 94–96, 289–290
- chain of custody for, 218–221, 222–223, 228–229, 268
- confidentiality of, 270, 276–277, 297
- data as (*see* Data)
- duplicate, 224
- forensic imaging of, 47, 90–92, 110, 221–223, 225–226, 227–229, 239, 269, 293
- handling of, 216–221, 222, 239, 293
- hashing, 227–229
- ISO standards for, 271–273
- original, 223
- privacy laws related to, 213
- reporting findings from, 265–269, 294, 297–302
- retention and curation of, 269–273, 294
- types/classification of, 223–224
- write blocking or protection of, 88, 90–91, 224–225, 226, 228

Excel, Microsoft, 46, 68, 74

Exchange, 226

exFAT (extended file allocation table) file system, 196

Expert witness testimony, 273–277, 279

Exponents, law of, 5–7, 165–166, 186–187, 251–252, 255–256

Extended partition, 119, 122, 140–142

Extensions, file, 18, 45–53, 61, 68–72, 73–76, 78, 163, 231, 235–237

EXT file systems, 202–203

FAT (File Allocation Table) file systems, 152, 153–187, 196, 244, 259. *See also* File systems

- cluster size determination in, 167–170
- directory entries in, 162–163, 167, 170–173, 176–177, 181, 244

exFAT, 196

FAT 12, 165–166, 180, 182–183

FAT 16, 166, 174–176, 180, 182–183

FAT 32, 166, 180, 184–185

- file allocation table in, 153, 163–167, 180
- HEX in, 154–156, 161, 170–173, 179–185
- limitations of, 174–177
- slack space in, 157–161, 170
- time and date stamps in, 244, 259
- Volume Boot Record in, 153–157, 179–185

FDISK partition editors, 101, 106–107

Files:

- boot process allowing access to (*see* Boot process)
- changing file extensions as deception, 47–53, 231, 235–237
- complex, 59–65, 79–83, 229
- compound, 59–61, 79–83
- compressed, 61–64 (*see also* ZIP file format)
- encrypted, 64–65
- file attributes, 194–195, 205–206, 243, 259

- file extensions, 18, 45–53, 61, 68–72, 73–76, 78, 163, 231, 235–237
- file formats and structures, 44–45, 68–72, 288–289
- file headers, 37, 41, 45, 59–60, 78, 79–83, 194, 206, 287–288, 288–289
- file signature databases, 59, 73–76
- file signature information, 45, 55–57, 58–59, 61–62, 63, 66, 73–78, 236, 288–289
- file slack, 158–161, 170
- file systems, 123–125, 132, 139–140, 147–187, 189–206, 237–238, 242, 243, 244–245, 259, 291–292
- fragmentation of, 132, 146–147, 164, 173
- HEX editor viewing, 53–58, 66, 77, 99–101, 154–155, 239
- metadata in, 45, 59–60, 78, 148–153, 191, 206, 237–238, 242, 244–245
- mounting, 63, 85–86, 87, 229, 289
- native format of, 18, 41, 287
- object linking and embedding in, 60
- recovering deleted, 229–231, 234
- value of file signatures, 58–59
- verification of, 231
- File systems:
 - alternative, 196–203
 - binary tree file systems, 196–200
 - \$Bitmap in, 195, 206
 - boot process allowing access to (*see* Boot process)
 - b-tree file systems, 200–202
 - bytes per sector in, 155–156
 - cluster allocation in, 131–132, 195, 206
 - cluster size determination in, 167–170
 - directory entries in, 162–163, 167, 170–173, 176–177, 181, 244 (*see also* Master File Table)
 - exFAT file systems, 196
 - EXT file systems, 202–203
 - FAT (File Allocation Table) file systems, 152, 153–187, 196, 244, 259
 - file allocation table in, 153, 163–167, 180
 - file attributes in, 194–195, 205–206, 243, 259
 - HEX in, 154–156, 160–161, 170–173, 179–185, 190–193
 - Hierarchical File System, 202
 - library cataloging systems
 - comparison to, 147–149, 150, 151, 153, 177
 - limitations of, 174–177, 196
 - Master File Table in, 191–195, 244 (*see also* Directory entries)
 - metadata in, 148–153, 191, 206, 237–238, 242, 244–245
 - NTFS (New Technology File System), 189–196, 205–206, 244, 259
 - overview of, 147–149, 291–292
 - Partition Boot Record in, 190–191, 192

Files systems (*Continued*)

- partitions, volumes and,
 - 123–125, 139–140, 179 (*see also* Partition Boot Record and Volume Boot Record subentries)
 - sectors per cluster in, 156–157
 - slack space in, 158–161, 170
 - system ID field, 123–124
 - time and date stamps in,
 - 244, 259
 - UNIX File System, 202, 203
 - Volume Boot Record in,
 - 153–155, 179–185
- Forensic imaging, 47, 90–92, 110, 221–223, 225–226, 227–229, 239, 269, 293
- Forensic process, 208, 209–211, 283–295. *See also* Cyber forensic practices
- Forensic report, 265–269, 294, 297–302
- Fourth Amendment, 213
- FTK, 228
- GIF (Graphic Interchange Format)
 - file format, 45, 55, 77
- Google searches, 55, 231–232
- Guidance Software, 176, 228
- Hard drives:
 - boot process (*see* Boot process)
 - clusters on, 104, 106, 131–132, 140, 146–147, 153, 156–157, 164–170, 171–173, 180, 194–195, 206
 - defragmentation of, 146–147, 173
 - evidence corruption on,
 - 90–92, 94–95, 289–290

labels, 233

- partition of, 96–97, 101,
 - 102–107, 109, 117–125, 130, 132–144, 147, 179, 190–191, 231, 232–234, 291
- removal of, 91
- sectors of (*see* Sectors)
- technology of, 130–132
- tracks and cylinders of,
 - 130, 132
- volumes of, 138–142, 147, 291

Hash values, 227–229

Headers, file:

- compound file, 59–60, 79–83
- data in, 41, 287–288
- file format/attributes identifier in, 45, 60, 194, 206, 288–289
- HEX editor header panel, 37
- metadata in, 45, 59–60, 78, 206

Hexadecimal (HEX) characters:

- ASCII equivalent of, 32–34, 55, 57–58, 66, 77, 154–155, 160–161, 248–249, 288

binary to HEX conversion, 30–34, 288

binary values represented by, 22, 23, 25–42, 43, 53–58, 66, 77, 98–101, 117–125, 227, 288

bit, byte and nibble equivalents to, 27–30, 31

boot process using, 98–101, 117–125

decimal equivalents to, 26, 29, 32, 34, 55, 120–121, 155–156, 172–173, 192–193, 249, 257

- file identification using, 53–58, 66, 77, 99–101, 154–155, 289
- file system use of, 154–156, 160–161, 170–173, 179–185, 190–193
- hashes displayed in, 227–229
- HEX editor, 34–39, 43, 53–58, 66, 77, 98–101, 117–125, 154–155, 289
- offsets relative to, 37, 98–101, 120–121, 124, 130, 154, 162–163, 179–185, 190–193, 248–258
- time and date stamps using, 248–258
- Hierarchical File System (HFS), 202
- HTML (hypertext markup language) file format, 45, 77–78
- Indexing data, 231–232, 234
- Intel processors, 116, 117
- Investigation. *See also* Cyber forensic practices
 - closing case files in, 278
 - definition of, 264
 - document initiating, 211–212
 - expert witness role of investigator, 273–277, 279
 - Investigative Smart Practices, 207–208, 209, 211–238, 239–240, 264–273, 292–294
 - legitimacy and scope of, 212–216, 293
 - objectives of/steps in, 234–238, 240, 263–280, 293–294
 - post-investigation quality control assessment, 278–279
 - privacy laws impacting, 213
 - report communicating findings of, 265–269, 294, 297–302
 - request for, 211–216, 239, 293
 - search criteria in, 214, 216, 232, 234
 - wrap-up and conclusion of, 273–279, 294
- ISO standards:
 - 14721:2003, 272–273
 - 15489:2001, 271–272
- Java Virtual Machine, 116
- JPEG (Joint Photographic Experts Group) file format, 45, 52, 55–56, 74, 77
- Keywords, 41, 59, 214, 216, 232, 234, 236–237, 287
- Last modified date and time, 238, 244, 253, 258
- Library cataloging systems, 147–149, 150, 151, 153, 177
- Linux, 44, 78, 122, 152, 153, 202–203
- Logical Block Address (LBA), 130, 132–133
- Logical partition, 122–123
- Macintosh:
 - boot process in, 86
 - endian designation by, 117
 - file extensions for, 70–72
 - file signature information for, 76
 - file systems of, 152, 153, 202
 - hard drive removal from, 91
 - operating systems, 44, 76, 86, 152, 153, 202

- Magic number, 55, 77–78, 202.
 See also Files: file signature information
- Magnetism, 3–4
- Master Boot Record (MBR),
 95–110, 117–125
- Master File Table, 191–195, 244.
 See also Directory entries
- Metadata, 45, 59–60, 78,
 148–153, 191, 206,
 237–238, 242, 244–245
- Microprocessor calculations,
 16–17
- Microsoft:
 - Compound File Binary
 Format, 59
 - DOS, 71, 75, 92, 101, 118, 122,
 152, 248–250, 252–259, 292
 - Excel, 46, 68, 74
 - file extensions used by, 18,
 45–53, 61, 68–72, 73–76,
 78, 163
 - file signatures of MS products,
 56–58, 61–62, 63,
 73–76, 236
 - file system of, 150, 152,
 153–157, 189–196,
 205–206, 244, 259
 - Head values bug in, 138
 - Office 2003, 58, 63
 - Office 2007, 58, 63
 - Office Open XML format, 58,
 61, 68, 74
 - Outlook, 226
 - PowerPoint, 68, 73
 - time and date stamps by, 244,
 245, 248–250, 252–259,
 292
 - Windows Operating System,
 43, 45–53, 68–72, 73–76,
 78, 86, 92, 107, 118–119,
 122, 125, 150, 152, 153,
 163, 189–196, 205–206,
 244, 245, 259
 - Word, 18, 41, 46, 52–53,
 56, 57, 58, 61–62, 63, 68,
 73, 147, 150, 231,
 236–237, 287
- Motorola processors, 116
- Mounting files, 63, 85–86, 87,
 229, 289
- Native format, 18, 41, 287
- Network acquisitions, 222–223,
 226
- Network Time Protocol (NTP),
 243, 250
- Nibbles, 27–30, 31
- Non-disclosure agreements, 212
- Novell, 122
- NTFS (New Technology File
 System), 189–196, 205–206,
 244, 259
- \$Bitmap in, 195, 206
- file attributes in, 194–195,
 205–206, 259
- limitations of, 196
- Master File Table in, 191–195,
 244
- Partition Boot Record in,
 190–191, 192
- OAIS (open archival information
 systems), 271, 272–273
- Object linking and embedding
 (OLE), 60
- Obsolescence, technological, 43,
 153, 177, 271
- OEM (original equipment manu-
 facturer), 190

- Office, Microsoft. *See also specific software by name*
 - Office 2003, 58, 63
 - Office 2007, 58, 63
 - Office Open XML format, 58, 61, 68, 74
- Offsets, 37, 98–101, 120–121, 124, 130, 154, 162–163, 179–185, 190–193, 248–258
- Operating systems:
 - Apple/Macintosh, 44, 76, 86, 152, 153, 202
 - boot process in, 85–86, 88, 89, 91–92, 94, 96–97, 101–104, 106–109, 118–119, 122
 - decimal value references by, 18
 - endian designation in, 116, 117, 120, 290–291
 - file extensions used by, 18, 45–53, 61, 68–72, 73–76, 78, 163
 - file folder structure of, 53
 - file formats executed by, 44–45, 287–288, 288–289
 - file systems of, 123–125, 132, 139–140, 147–187, 189–206, 237–238, 242, 243, 244–245, 259, 291–292
 - HEX longevity vs., 43
 - Linux, 44, 78, 122, 152, 153, 202–203
 - Microsoft DOS, 71, 75, 92, 101, 118, 122, 152, 248–250, 252–259, 292
 - Microsoft Windows, 43, 45–53, 68–72, 73–76, 78, 86, 92, 107, 118–119, 122, 125, 150, 152, 153, 163, 189–196, 205–206, 244, 245, 259
 - Novell, 122
 - OEM (original equipment manufacturer) of, 190
 - partitions and, 102, 103–104, 106, 107, 118–119, 121–125, 138–144, 291
 - registry, 46
 - time and date stamps by, 244–245, 248–259, 292
 - Unix and Unix-like, 44, 78, 152, 153, 202, 203
 - variety of and changes to, 264–265
 - volumes recognized by, 138–142, 291
- Order of data. *See* Endianness
- Outlook, Microsoft, 226
- Partition:
 - active, 96, 97, 101, 102, 109, 117, 118, 119, 120
 - Cylinder, Head and Sector (CHS) fields of, 130, 132–138
 - deletion and recovery of, 143–144, 231, 232–234
 - extended, 119, 122, 140–142
 - FDISK partition editors, 101, 106–107
 - file systems in (*see* File systems)
 - HEX starting value of, deciphering, 120
 - logical, 122–123
 - Logical Block Address in, 130, 132–133
 - Partition Boot Record, 96, 101, 109, 190–191, 192
 - partition table, 96–97, 101, 102–107, 109, 117–125, 130, 134–142, 179, 233
 - primary, 117, 122–123

Partition (*Continued*)

- size of, 121, 138
 - start of, 119–120
 - system ID field, 123–124
 - type of, 121–125
 - volumes vs., 138–142, 147, 291
- POST (Power On Self Test), 87–88, 92
- PowerPC processors, 116
- PowerPoint, Microsoft, 68, 73
- Primary partition, 117, 122–123
- Privacy Protection Act, 213
- Processors, endian designation in, 116, 117, 120. *See also* Operating systems
- Quality control assessment, 278–279
- QuickTime file format, 45
- Registry, operating systems, 46
- Report, forensic:
 - characteristics of, 266–268
 - contents of, 268–269, 297–302
 - purpose of, 265–266, 294
 - sample of, 297–302
- Resident data, 154
- Searches:
 - data preparation searches, 232–234
 - Google searches, 55, 231–232
 - investigation search criteria, 214, 216, 232, 234
 - keyword, 41, 59, 214, 216, 232, 234, 236–237, 287
- Sectors:
 - bytes per, 59, 80, 97, 130, 138, 155–156
 - clusters of, 104, 106, 131–132, 140, 146–147, 153, 156–157, 164–170, 171–173, 180, 194–195, 206
 - compound file, 59, 80–82
 - Cylinder, Head and Sector fields, 130, 132–138
 - file systems use of (*see* File systems)
 - in hard drive structure, 130–138
 - Logical Block Address of, 130, 132–133
 - Master Boot Record as first, 95–110, 117–125
 - number of, 121, 124, 138
 - partition as collection of, 138–139, 291 (*see also* Partition)
 - Partition Boot Record sector, 96, 101, 109, 190–191, 192
 - SecID of, 81–82
 - Sector Allocation Table, 81–82
 - signature words as end of sector markers, 96–97, 101, 107, 109
 - slack as unused, 157–161, 170
 - volume as collection of, 138–139, 291 (*see also* Volumes)
 - Volume Boot sector, 98, 153–157, 179–185
- Setup utility, 92–96
- Signature, file, 45, 55–57, 58–59, 61–62, 63, 66, 73–78, 236, 288–289
- Signature words/bytes, 96–97, 101, 107, 109

- Slack space, 157–161, 170
- Stevens, Malcolm, 247
- Sun's SPARC, 116
- System ID field, 123–124
- Technological obsolescence, 43, 153, 177, 271
- TIF (Tagged Image File) file format, 52, 74–75
- Time. *See also* Dates
 - accessed/last accessed date and time, 245
 - chain of custody including, 218–220
 - clock manipulation impacting, 246–247
 - clock model of, 247–248
 - clock skew impacting, 245–246, 292
 - Coordinated Universal Time (UTC), 242, 247, 259
 - creation date and time, 237–238, 244, 253, 258
 - cyber forensics and, 238–239, 241–260, 292
 - definition of, 241–243
 - determination of, 254–258
 - directory entry including, 162–163, 181
 - hours, 254, 255, 257
 - inaccuracy of, 258–260, 292
 - investigation noting discrepancies in, 237–238
 - keeping track of, 245–247
 - last modified date and time, 238, 244, 253, 258
 - minutes, 254, 255, 257
 - MS-DOS 32-bit timestamp, 248–250, 252–259, 292
 - Network Time Protocol, 243, 250
 - search criteria including, 214, 216
 - seconds, 254, 255–257
 - system clock verification, 89
 - time-bounding techniques, 247–248
 - timelines, 242, 292
 - timestamps, 242, 244–250, 252–259, 292
- Unallocated space, 142, 159, 160, 161–163, 164, 167, 178, 180, 195, 206, 226, 229–231, 232
- Unicode/Universal Character Set (UCS):
 - ASCII as foundation of, 8, 10–12
 - decimal values for, 16, 18
 - HEX equivalent of, 57
- Unix and Unix-like operating systems, 44, 78, 152, 153, 202, 203
- Unix File System (UFS), 202, 203
- UTC (Coordinated Universal Time), 242, 247, 259
- Volumes:
 - file systems in (*see* File systems)
 - partitions vs., 138–142, 147, 291
 - Volume Boot Record (VBR), 98, 153–157, 179–185
- Windows Operating System. *See also* Microsoft
 - boot process in, 86, 92, 107, 118–119

Windows Operating

System (*Continued*)

file extensions used by, 45–53,
68–72, 73–76, 78

file folder structure of, 53

file system of, 150, 152, 153,
189–196, 205–206,
244, 259

HEX longevity vs., 43

metadata information via, 150

partitions in, 107, 118–119,
122, 125

time and date stamps by, 244,
245, 259

Word, Microsoft, 18, 41, 46,
52–53, 56, 57, 58, 61–62,
63, 68, 73, 147, 150, 231,
236–237, 287

Write blocking or protection, 88,
90–91, 224–225, 226, 228

XHTML (extended HTML) file
format, 78

XML (extensible markup lan-
guage) file format, 58, 61,
68, 74, 78

ZIP file format, 58, 61, 63, 229

<http://www.pbookshop.com>

<http://www.pbookshop.com>

<http://www.pbookshop.com>

<http://www.pbookshop.com>