
Index

Symbols

- \$AttrDef file, 278, 305-306, 382
- \$ATTRIBUTE_LIST attribute, 282, 321, 365-366
- \$BadClus file, 278, 312
- \$BITMAP attribute, 276, 282, 372
- \$Bitmap file, 278, 312, 383
- \$Boot file, 278, 304, 379-381
- \$DATA attribute, 282, 319, 364
- \$EA attribute, 282
- \$EA_INFORMATION attribute, 282
- \$Extend file, 278
- \$FILE_NAME attribute, 282, 318, 362-364
- \$INDEX_ALLOCATION attribute, 282, 295, 336, 371-372
- \$INDEX_ROOT attribute, 282, 295, 336, 369-370
- \$LogFile file, 278, 391
- \$LOGGED_UTILITY_STREAM attribute, 282, 288
- \$MFT file, 276, 302, 379
- \$MFTMirr file, 278, 303
- \$OBJECT_ID attribute, 335, 367-368
- \$Quota file, 339-340, 388-389
- \$Reparse file, 335
- \$REPARSE_POINT attribute, 282, 368
- \$Secure file, 278, 322
- \$SECURITY_DESCRIPTOR attribute, 282, 322
- \$STANDARD_INFORMATION attribute, 282, 316, 359
- \$SYMBOLIC_LINK attribute, 282
- \$Uppcase file, 278
- \$UsrJrnl file, 392-395
- \$Volume file, 278, 305, 385
- \$VOLUME_INFORMATION attribute, 282

INDEX

\$VOLUME_NAME attribute, 282

\$VOLUME_VERSION attribute, 282

4.2BSD fast file system (FFS), 119

A

a-time, 196

acquiring hard disks, 48-49

dd tool, 60

dead acquisition, 50-51

live acquisition, 50-51

via networks, 59

acquisition tools, error handling, 51

ADS (alternate data streams), 283, 319

allocation algorithms, 179

ExtX

content category, 410

metadata category, 418-419, 429

FAT

content category, 224

file name category, 241

metadata category, 233-234

NTFS

content category, 313

file name category, 336

metadata category, 324-325

UFS

content category, 490

file name category, 498

metadata category, 494

alternate data streams (ADS), 283, 319

analysis

Apple partitions, 107

application category (file system journals), 205

BSD partitions, 125

content category, 178

allocation strategy, 179

consistency checks, 184

damaged data units, 181

data unit allocation order, 184

data unit allocation status, 183

data unit viewing, 181

logical file system addresses, 179

logical file system-level searching, 182

wiping techniques, 185

dead, 6

ExtX

application category, 439-441

content category, 411-412

file name category, 423-436

file system category, 404-408

metadata category, 412-423

FAT file systems

content category, 225-226

file name category, 241-244

file system category, 217-221

metadata category, 235-238

file system category, 177-178

GPT disks, 144

live, 6

metadata category, 186

compressed and sparse files, 191

consistency checks, 198, 204

data structure allocation order, 197, 204

encrypted files, 192

file name listing, 202

file name searching, 203

local file viewing, 193

- logical file searching*, 194
- metadata attribute searching and sorting*, 196-197
- metadata-based file recovery*, 188-190
- metadata lookup*, 193
- overview*, 199-201
- slack space*, 187
- unallocated metadata analysis*, 195
- wiping techniques*, 198, 204
- NTFS
 - application category*, 339-343
 - content category*, 311-315
 - file name category*, 333-339
 - file system category*, 301-310
 - metadata category*, 316-332
- Solaris systems, 139
- UFS
 - content category*, 488-492
 - file name category*, 497-499
 - file system category*, 481-488
 - metadata category*, 492-496
- volume analysis, 75
 - consistency checks*, 76-77
 - extracting partitions*, 77-79
 - recovering partitions*, 79-80
 - techniques*, 75
- Apple partitions, 101**
 - analysis, 107
 - data structures, 103-104
 - Image tool output, 105
- application-based file recovery (data carving), 206**
- application category, 175**
 - Ext3
 - analysis*, 440-441
 - journaling*, 437-438
 - file system journals, 205
 - NTFS
 - change journal feature*, 343
 - disk quotas*, 339
 - journaling*, 340, 343
 - TSK tools, 542
- application-level search techniques**
 - application-based file recovery (data carving), 206
 - file type sorting, 207
- ASCII, 23**
- assembly (volumes), 73**
- asymmetric encryption, 288**
- AT Attachment (ATA) disks, 29-30, 32**
 - commands, 52
 - drives (vs. SCSI), 41
- AT Attachment Packet Interface (ATAPI), 35**
- ATA-3, security, 36**
- ATAPI (AT Attachment Packet Interface), 35**
- \$AttrDef file, 278, 306, 382**
- attribute headers, MFT entries, 355-359**
- \$ATTRIBUTE_LIST attribute, 282, 321, 365-366**
- attributes (NTFS)**
 - \$ATTRIBUTE_LIST attribute, 282, 321, 365-366
 - \$BITMAP attribute, 276, 282, 372
 - \$DATA attribute, 282, 319, 364

INDEX

- \$EA attribute, 282
- \$EA_INFORMATION attribute, 282
- \$FILE_NAME attribute, 282, 318, 362-364
- \$INDEX_ALLOCATION attribute, 282, 295, 336, 371-372
- \$INDEX_ROOT attribute, 282, 295, 336, 369-370
- \$LOGGED_UTILITY_STREAM attribute, 282, 288
- \$OBJECT_ID attribute, 335, 367-368
- \$REPARSE_POINT attribute, 282, 368
- \$SECURITY_DESCRIPTOR attribute, 322
- \$STANDARD_INFORMATION attribute, 282, 316, 359
- \$SYMBOLIC_LINK attribute, 282
- \$VOLUME_INFORMATION attribute, 282
- \$VOLUME_NAME attribute, 282
- \$VOLUME_VERSION attribute, 282
- Autopsy, 15, 544**
- B**
- B-trees, 290**
- \$BadClus file, 278, 312**
- base MFT entries, 284**
- Basic Input/Output System. *See* BIOS**
- best fit strategy, 180**
- binary numbers, 18**
- BIOS (Basic Input/Output System), 28, 49**
 - data, accessing, 49-50
 - vs. direct access, 39-40
- BIOS Parameter Block (BPB), 213**
- \$BITMAP attribute, 276, 282, 372**
- \$Bitmap file, 278, 312, 383**
- block bitmap**
 - ExtX, 401, 456
 - UFS, 482, 525
- block devices, 414**
- block group descriptor table, 401-402**
- blocks. *See* ExtX; UFS**
- boot code, 115**
- \$Boot file, 278, 304, 379-381**
- boot loader, 402**
- boot sector**
 - FAT, 213, 253-258
 - NTFS, 304
- bootable CDs, 109**
- bootable flags (DOS), 89**
- bootable Linux CDs, 160**
- booting disks, 27**
 - boot code locations, 28
 - CPUs and machine code, 27
- BPB (BIOS Parameter Block), 213**
- BSD, 115**
 - boot code, 115
 - deleting files, 495
 - union mounts, 498
- BSD partitions, 111**
 - analysis, 125
 - data structures, 116
 - disk labels, 116-119*
 - FreeBSD example image, 123-125*
 - OpenBSD example image, 120-121*
 - overview, 112
- BXDR tool, 52**

C**c-time**, 196**CD-Rs**, 108**Central Processing Units (CPUs)**, 27**CFTT (Computer Forensic Tool Testing)**,
49, 55**change journal feature (NTFS)**, 343**character devices**, 414**character encoding**, 22-24**CHS addresses**, 33**cluster chains**, 229**clusters**

FAT, 221

addresses, 223*allocation status*, 223

NTFS, 311

allocation status, 383*\$BadClus file*, 312**commands (ATA)**, 52**commit blocks**, 477**component entries**, 164**compressed attributes (MFT entries)**, 285**compressed files (metadata category)**, 191**compressed image files**, 58-59**Computer Forensic Tool Testing (CFTT)**,
49, 55**conducting investigations**, 5**consistency checks**

content category, 184

ExtX, 446

FAT, 250

file name category, 204

metadata category, 198

NTFS, 349

UFS, 505

volume analysis, 76-77

content category, 174

allocation strategies, 179

analysis techniques, 178

consistency checks, 184*data unit allocation order*, 184*data unit allocation status*, 183*data unit viewing*, 181*logical file system-level searching*, 182

damaged data units, 181

ExtX

allocation algorithms, 410*allocation status*, 409*analysis*, 411-412*overview*, 409

FAT, 221

allocation algorithms, 224*analysis*, 225-226*cluster and sector addresses*, 223

logical file system addresses, 179

NTFS

allocation algorithms, 313*analysis*, 315*\$BadClus file overview*, 312*\$Bitmap file overview*, 312*clusters*, 311*file system layout*, 313

TSK tools, 539

UFS

allocation algorithms, 490*analysis*, 491*overview*, 488-490

wiping techniques, 185

INDEX

controllers, 32

BIOS vs. direct access, 40

converting

binary numbers to decimal values, 18

cylinder addresses to sector
addresses, 133

from CHS to LBA, 34

hexadecimal numbers to decimal
values, 20

The Coroner's Toolkit, 207**correlation (guideline), 9****corruption of drives, minimizing, 73****CPUs (Central Processing Units), 27****cryptographic hashes**

calculating, 6

dd tool, 65-66

cryptography (NTFS), 288

cylinder group descriptor (UFS), 482,
522, 524

cylinder group summary data struc-
tures, 521

cylinder groups, 479, 483

allocation of blocks and fragments, 490

descriptors, 482

D**D-time, 420****damaged data units, 181****data**

acquiring, 48-49

dd tool, 60

dead acquisition, 50-51

live acquisition, 50-51

analyzing, 10-11

copying, 47-48

essential, 12-13

hidden, 52

nonessential, 12-13

organization, 17

data sizes, 21

data structures, 24

flag values, 26-27

number format, 18-19

strings and character encoding, 22-24

write protecting, 53-55

\$DATA attribute, 282, 319, 364**data carving, 206****data categories (file systems), 174****data decryption fields (DDF), 288****data recovery fields (DRF), 288****data structures, 24****data units, 174**

allocation order, 184

allocation status, 183

orphan, 184

viewing, 181

dcat tool, 181, 340**DCOs. *See* Device Configuration
Overlays****dd tool, acquiring data, 60**

case study, 60-63

cryptographic hashes, 65-66

extracting partitions, 77-79

error handling, 64-65

HPA, 61-63

input sources, 61

output destinations, 63-64

- DDF (data decryption fields), 288**
- dead acquisition (data), 50-51**
- dead analysis, 6**
- decimal numbers, 18**
 - converting
 - from binary numbers, 18*
 - from hexadecimal numbers, 20*
- DEFRAG utility, 236**
- deleting files**
 - Ext3, 443
 - FAT, 246
 - NTFS, 346
 - UFS, 502
- descriptor blocks, 477**
- Device Configuration Overlays (DCO)**
 - acquisition, 53
 - hardware write blockers, 54
 - overview, 38-39
- DEVICE_CONFIGURATION_IDENTIFY command, 38**
- DFTT (Digital Forensic Tool Testing), 191, 237, 421**
- differential voltage, 42**
- digital crime scenes, preserving, 5**
- digital evidence, 4-5**
- Digital Forensic Tool Testing (DFTT), 191, 237, 421**
- digital investigations, 4**
 - Autopsy, 544
 - conducting, 5
 - defined, 4
 - Event Reconstruction Phase, 8
 - Evidence Searching Phase, 7
 - focus, 3
 - forensic, 4
 - guidelines, 8-9
 - Linux systems, file deletion order, 435
 - partitions, 69
 - RAID systems, 155
 - System Preservation Phase, 5-6
- digital storage, organization, 69-70**
- direct access vs. BIOS, 39-40**
- directories**
 - attribute, 228
 - content category (FAT file systems), 230
 - hash trees, 428
 - root (UNIX), 72
 - UNIX, 427
- directory entries**
 - ExtX, 424-425, 467-469
 - FAT
 - content category, 227*
 - data structure, 261-265*
 - ordering, 243*
 - UFS, 497, 534
- directory index entry data structure, 376-377**
- directory indexes (NTFS), 333**
- disk commands, 35**
- disk entries (LDM), 164**
- disk groups, 157**
- disk labels, 112**
 - BSD partitions, 116-119
 - FreeBSD, 113
 - Sparc, 128
- disk quotas (NTFS), 339**

INDEX

disk spanning, 156

- acquisition and analysis, 159
- Linux LVM, 160-161
- Linux MD, 158
- overview, 157
- Windows LDM, dynamic disks, 162-169

disks. *See also* hard disks

- booting, 27-28
- DOS, boot code, 87
- GPT, 140-142
- MBR
 - DOS partitions, 88-92, 98-100*
 - extended partitions, 93-95*
- multiple, 147
 - RAID, 148-153*
 - spanning, 156-169*
- partitions (BSD), 112
- quotas (NTFS), 339

diskstat tool, 52, 63, 538**dls tool, 184****DOS partitions, 81-82, 85-88**

- boot code, 87
- bootable flags, 89
- disks, boot code, 87
- extended, 93, 95, 97
- FreeBSD, 113
- MBR concepts, 83
- MBR disks, 88-92
 - analysis, 100*
 - Image tool output, 98-99*
- OpenBSD, 115

double block pointers, 416**DRF (data recovery fields), 288****DRIVEID tool, 52****drives. *See* hard disks****dstat tool, 490****dynamic disks, Windows LDM, 162**

- acquisition and analysis, 168-169
- LDM database, 164-167

E**\$EA attribute, 282****\$EA_INFORMATION attribute, 282****EFI (Extensible Firmware Interface), 139**

- disks, 81
- partitions, 127

embedded image formats, 57**EnCase, 14, 155****encrypted attributes (MFT entries), 287****encrypted files (metadata category), 192****EOF (End of File) markers (FAT), 229****error handling**

- acquisition tools, 51
- dd tool, 64-65

essential data, 12-13**essential file system data, 176****Event Reconstruction Phase (digital investigations), 8****events, reconstructing, 8****evidence**

- digital, 4-5
- searching for, 7

Evidence Searching Phase (digital investigations), 7

Ext2. *See* ExtX

Ext3. *See* ExtX

\$Extend file, 278

extended attributes

ExtX, 462-465

UFS2, 493, 532-533

extended partition (DOS), 92-95

overview, 83-87

Extensible Firmware Interface (EFI), 139

disks, 81

partitions, 127

extracting

partitions, volume analysis, 77-79

unallocated data units, 183

ExtX, 398

access control lists, 417

block bitmap, 456

blocks, 409

consistency checks, 446

content category

allocation algorithms, 410

allocation status, 409

analysis, 411-412

overview, 409

directory entries, 467-469

extended attributes, 462-465

features, 398

file allocation example, 441

file deletion example, 443

file name category

allocation algorithms, 429

analysis, 430-434

hash trees, 428

links, 426

overview, 424-425

root directory, 424

file recovery example, 446

file system category

analysis, 404-408

block group descriptor tables, 401-402

overview, 399

superblock, 399

file system journaling, 437-438

fragments, 409

group descriptor tables, 455-456

hash trees, 470-472

inodes, 457-461

journal data structures, 472-478

metadata category

allocation algorithms, 418-419

analysis, 421-423

inodes, 417

overview, 413-414

superblock, 449-451

flag values, 454

major version, 452

symbolic links, 426, 470

time value updating, 419

F

Fast File system (FFS), 479

FAT (File Allocation Table) file system, 211

boot sector, 253-258

consistency checks, 250

INDEX

- content category, 221
 - allocation algorithms*, 224
 - analysis*, 225-226
 - cluster and sector addresses*, 223
- converting date values, 263
- determining type, 249
- directory entries, 261-265
- FATs, 260-261
- file allocation example, 244
- file deletion example, 246
- file name category, 239
 - allocation algorithms*, 241
 - analysis*, 241-244
 - root directory*, 214
- file recovery, 247
- file system category, 213
 - analysis*, 217-221
 - essential boot sector data*, 214
 - non-essential boot sector data*, 216
- file system creation date, 237
- FSINFO data structure, 259
- long file name directory entries, 267-271
- metadata category
 - analysis*, 235-238
 - cluster chains*, 229
 - directories*, 230
 - directory entries*, 227
 - directory entry allocation*, 233
 - example image*, 233
 - time value updating*, 234
- overview, 212
- FAT12 file systems, 260**
- FAT12/16, boot sector, 256**
- FAT16 file systems, 260**
- FAT32 file system**
 - boot sector, 256
 - FATs, 260
 - FSINFO data structure, 218, 259
- FATs, 260**
- fdisk tool, 98**
- FEK (file encryption key), 288**
- ffind tool, 204, 542**
- FFS (Fast File System), 479**
- FIFO, 414**
- file attributes (NTFS), 359**
 - \$ATTRIBUTE_LIST attribute, 365-366
 - \$DATA attribute, 364
 - \$FILE_NAME attribute, 362-364
 - \$OBJECT_ID attribute, 367-368
 - \$STANDARD_INFORMATION attribute, 361
- file encryption key (FEK), 288**
- \$FILE_NAME attribute, 282, 318, 362-364**
- file name category, 175**
 - analysis techniques
 - consistency checks*, 204
 - data structure allocation order*, 204
 - file name listing*, 202
 - file name searching*, 203
- ExtX**
 - allocation algorithms*, 429
 - analysis*, 430-434
 - directory entry*, 424, 467
 - hash trees*, 428
 - links*, 426
 - overview*, 424-425

- FAT
- allocation algorithms, 241*
 - analysis, 241-244*
 - directory entry, 261*
 - long file name, 267*
 - overview, 239*
- NTFS
- allocation algorithms, 336*
 - analysis, 336-339*
 - directory indexes, 333*
 - links to files and directories, 335*
 - object IDs, 335*
 - root directory, 334*
- overview, 199-201
- TSK tools, 541
- UFS
- allocation algorithms, 498*
 - analysis, 499*
 - directory entry, 497, 534*
 - overview, 497*
- wiping techniques, 204
- file name listing, 202**
- file name searching, 203**
- file records, 275, 353**
- file system category, 174, 177**
- analysis techniques, 178
- ExtX
- analysis, 404-408*
 - block group descriptor tables, 401-402*
 - overview, 399*
 - superblock, 399*
- FAT, 213
- analysis, 217-221*
 - essential boot sector data, 214*
 - non-essential boot sector data, 216*
- NTFS, 301
- analysis, 307-309*
 - \$AttrDef file overview, 306*
 - \$Boot file overview, 304*
 - \$MFT file overview, 302*
 - \$MFTMirr file overview, 303*
 - \$Volume file overview, 305*
- TSK tools, 539
- UFS
- analysis, 487*
 - boot code, 485*
 - cylinder group descriptor, 482*
 - superblock, 481*
- file system journals, 205**
- file systems. *See also* ExtX; FAT; NTFS; UFS**
- analysis by category, 173, 177. *See also* analysis
 - data categories, 174
 - dealing with specific kinds, 207
 - essential/non-essential data, 176
 - overview, 173
- file type sorting, 207**
- finding the source of a moved ExtX file, 432**
- Firewire, 151**
- first available allocation strategy, 179**
- fixup values, 352**

INDEX

- fls tool**, 203, 432
- foremost tool**, 206
- The Forensic Toolkit (FTK)**, 14
- fragment bitmaps (UFS)**, 525-527
- fragmentation**, 179, 488
- FreeBSD**
 - overview, 113
 - partitions
 - BSD disk label entry*, 121
 - example image*, 123-125
 - mounting*, 122
- FSINFO data structure (FAT32)**, 218, 259
- fsstat tool**, 178, 539
 - ExtX, 402
 - FAT, 216, 266
 - NTFS, 306
 - UFS2, 486, 520
- FTK (The Forensic Toolkit)**, 14
- G**
 - generic NTFS index entry data structure**, 375
 - geometry (hard disks)**, 29
 - platters, 31
 - Globally Unique Identifier (GUID)**, 164
 - GPT partitions**, 81, 139
 - analysis, 144
 - data structures, 140-142
 - Intel defined*, 143
 - Microsoft defined*, 143
 - group descriptor tables (ExtX)**, 455-456
 - group descriptors**, 399
 - UFS1, 522-523
 - UFS2, 524
- GUID (Globally Unique Identifier)**, 164
- GUID Partition Table disks**, 81
- Guidance Software**, 14
- guidelines**
 - correlation, 9
 - investigations, 8-9
 - isolation, 9
 - logging, 9
 - PICL, 8
 - preservation, 8
- gzip**, 191
- H**
 - hard disks**, 29
 - ATA interface, 32
 - BIOS vs. direct access, 39-40
 - DCO, 38
 - disk commands, 35
 - geometry and internals, 29
 - platters*, 31
 - sectors*, 31
 - hard disk passwords, 36
 - HPA, 36
 - interface standards, 34
 - SCSI drives, 41
 - connector types*, 43
 - size barriers*, 44
 - types of*, 42
 - vs. ATA*, 41
 - sector addresses, 33-34
 - serial ATA, 39
 - hard links**, 334, 426, 498

hardware

- block devices, 414
- RAID, 151-152

hardware write blockers, 53-55**hash trees, 428**

- ExtX, 470-472

hashes, 6, 59-60**hexadecimal numbers, 19**

- converting to decimal values, 20

high voltage differential (HVD), 42**HPA (Host Protected Area)**

- acquisition, 52
- hardware write blockers, 59
- overview, 36

hpa tool, 52**HVD (high voltage differential), 42****I****i386 Solaris slices, 135-138****IA32-based hardware, 111****icat tool, 194, 354****IDE (Integrated Disk Electronics) disks.**

See AT Attachment disks

IDENTIFY_DEVICE command, 37**IDS (Intrusion Detection System),
48, 196****ils tool, 433****image files, 57**

- acquiring via networks, 59
- compressing, 58-59
- embedded, 57
- format, 57

**INCITS (International Committee
on Information Technology
Standards), 32****\$INDEX_ALLOCATION attribute, 282,
295, 336, 371-372****index attributes (NTFS)**

- \$BITMAP attribute, 372
- \$INDEX_ALLOCATION attribute,
371-372
- \$INDEX_ROOT attribute, 369-370

**index node header data structure,
373-374****\$INDEX_ROOT attribute, 282, 295, 336,
369-370****indexes**

- directory indexes (NTFS), 333
- NTFS, 290
 - attributes, 294*
 - B-trees, 291*

inode bitmaps, 413, 493**inodes**

- ExtX, 413-414, 457-461
- UFS, 492
- UFS1, 527-528
- UFS2, 530

**Integrated Disk Electronics (IDE) disks.
See AT Attachment disks****integrity hashes, 59-60****International Committee on
Information Technology Standards
(INCITS), 32****Intrusion Detection System (IDS),
48, 196**

INDEX

investigations. *See* digital investigations

isolation (guideline), 9

istat tool, 540

ExtX, 418

FAT, 232, 266

NTFS, 297, 302

UFS, 494

J

jcat tool, 542

jls tool, 478

journal data structures (ExtX), 473-477

journaling

Ext3, 437-438

NTFS, 340, 343

junctions, 335

K-L

last accessed time, 196

last changed time, 196

last modified time, 196

layered design (data analysis), 10-11

LBA (Logical Block Address), 31

LCN (Logical Cluster Number), 281

LDM (Logical Disk Manager) controls,
153

LDM database, 164-167

LDM partition area, 162

least significant symbol, 18

levels (RAID), 148-150

LFN (Long File Name) directory
entry, 239

FAT file systems, 267-271

links, junctions, 335. *See also* hard links;
symbolic links

Linux LVM, 160-161

Linux MD software RAID, 155

Linux swap partitions, 96

live acquisition, 50-51

live analyses, 6

\$LogFile file, 278, 391

\$LOGGED_UTILITY_STREAM
attribute, 282, 288

logging (guideline), 9

Logical Block Address (LBA), 31

Logical Cluster Number (LCN), 281

Logical Disk Manager (LDM)
controls, 153

logical disk volume address, 74

logical extents, 160

logical file searching (metadata
category), 194

logical file system addresses, 179

logical file system-level searching, 182

logical file viewing (metadata
category), 193

logical group addresses, 409

logical partition volume address, 74

logical volume addresses, 74, 179

Logical Volume Manager (LVM), 158

logical volumes, 157

long file name (LFN) directory
entries, 267

long file name attribute, 228

low voltage differential (LVD), 42

LSN (\$LogFile Sequence Number), 323

LVD (low voltage differential), 42

LVM (Logical Volume Manager), 158

M**m-time**, 196**machine code**, 27**major version**, 452**Master Boot Record (MBR)**, 81, 402**Master File Table (MFT)**, 274

entry addresses, 277

entry contents, 276

file system metadata files, 278

MFT entries, 279, 353-354

attribute content, 280*base MFT entries*, 284*compressed attributes*, 285*encrypted attributes*, 287*non-base entries*, 366*sparse attributes*, 284*standard attribute types*, 282

overview, 275

zone, 313

MBR (Master Boot Record), 402**MBR disks**, 81-83**MD driver**, 158**metadata attribute searching and sorting**
(*metadata category*), 196-197**metadata category**, 175

analysis techniques

consistency checks, 198*data structure allocation order*, 197*local file viewing*, 193*logical file searching*, 194*metadata attribute searching and*
sorting, 196-197*metadata lookup*, 193*unallocated metadata analysis*, 195

compressed and sparse files, 191

encrypted files, 192

ExtX

allocation algorithms, 418-419*analysis*, 421-423*inodes*, 417*overview*, 413-414

FAT

allocation algorithms, 233*analysis*, 235-238*cluster chains*, 229*directories*, 230*directory entries*, 227

metadata-based file recovery, 188-190

NTFS

allocation algorithms, 324-325*analysis*, 326-332*\$ATTRIBUTE_LIST* attribute, 321*\$DATA* attribute, 319*\$FILE_NAME* attribute, 318*\$Secure file*, 322*\$SECURITY_DESCRIPTOR**attribute*, 322*\$STANDARD_INFORMATION**attribute*, 316

overview, 186

slack space, 187

TSK tools, 540

UFS

allocation algorithms, 494*analysis*, 495-496*extended attributes*, 493*inodes*, 492*wiping techniques*, 198

INDEX

- metadata-based file recovery, 188-190**
metadata lookup (metadata category), 193
MFT (Master File Table). See Master File Table
\$MFT file, 276, 302, 379
MFT Zone, 313
\$MFTMirr file, 278, 303
minimizing drive corruption, 73
mmls tool, 98, 105, 122, 134, 144, 538
multiple device (MD) kernel driver, 154
multiple disks, 147
 - disk spanning, 156
 - acquisition and analysis, 159*
 - Linux LVM, 160-161*
 - Linux MD, 158*
 - overview, 157*
 - Windows LDM, 162-169*
- RAID**
 - hardware, 151-152*
 - levels, 148-150*
 - software, 153*
- N**
- National Institute of Standards and Technology (NIST), 49**
NetBSD partitions, 115
Network File System (NFS), 415
networks, acquiring data via, 59
New Technologies File System. See NTFS
next available strategy, 180
- NFS (Network File System), 415**
NIST (National Institute of Standards and Technology), 49, 55
nonessential data, 12-13, 176
NoWrite device, 54
NTFS (New Technologies File System), 211
 - analysis, 296
 - application category
 - change journal feature, 343*
 - disk quotas, 339*
 - journaling, 340, 343*
 - attribute headers, 355-359
 - consistency checks, 349
 - content category
 - allocation algorithms, 313*
 - analysis, 315*
 - \$BadClus file overview, 312*
 - \$Bitmap file overview, 312*
 - clusters, 311*
 - file system layout, 313*
 - file allocation example, 344
 - file deletion example, 346
 - file name category
 - allocation algorithms, 336*
 - analysis, 336-339*
 - directory indexes, 333*
 - links to files and directories, 335*
 - object IDs, 335*
 - root directory, 334*

- file recovery, 348
- file system category, 301
 - analysis, 307-309
 - \$AttrDef file overview, 306
 - \$Boot file overview, 304
 - \$MFT file overview, 302
 - \$MFTMirr file overview, 303
 - \$Volume file overview, 305
- file system metadata files
 - \$AttrDef file, 382
 - \$Bitmap file, 383
 - \$Boot file, 379, 381
 - \$LogFile file, 391
 - \$MFT file, 379
 - \$ObjId file, 386
 - \$Quota file, 388-389
 - \$UsrJrnl file, 392-393, 395
 - \$Volume file, 385
- files, 274
- fixup values, 352
- index attributes and data structures
 - \$BITMAP attribute, 372
 - directory index entry data structure, 376-377
 - generic index entry data structure, 375
 - \$INDEX_ALLOCATION attribute, 371-372
 - index node header data structure, 373-374
 - \$INDEX_ROOT attribute, 369-370
 - indexes, 290-294
- metadata category
 - allocation algorithms, 324-325
 - analysis, 326-332
 - \$ATTRIBUTE_LIST attribute, 321
 - \$DATA attribute, 319
 - \$FILE_NAME attribute, 318
 - \$Secure file, 322
 - \$SECURITY_DESCRIPTOR attribute, 322
 - \$STANDARD_INFORMATION attribute, 316
- MFT (Master File Table)
 - base MFT entries, 284
 - compressed attributes, 285
 - encrypted attributes, 287
 - entry addresses, 277
 - entry contents, 276
 - file system metadata files, 278
 - MFT entries, 279-284, 353-354
 - overview, 275
- overview, 273
- recovering deleted files, 328
- standard file attributes, 359
 - \$ATTRIBUTE_LIST attribute, 365-366
 - \$DATA attribute, 364
 - \$FILE_NAME attribute, 362-364
 - \$OBJECT_ID attribute, 367-368
 - \$STANDARD_INFORMATION attribute, 361
- NTFS Master File Table (MFT), 175**
- NTFSInfo tool, 296**

INDEX

O**\$OBJECT_ID attribute, 335, 367-368****object IDs (NTFS), 335****opcode, 27****OpenBSD, 115**

example image, 120

partitions, 114

superblock, 514

UFS1 group descriptors, 523

organization

data, 17

*data sizes, 21**data structures, 24**flag values, 26-27**number format, 18-19**strings and character encoding, 22-24*

digital storage, 69-70

volumes, partitions, 72

orphan data units, 184**P****partitions**

Apple, 101

*Image tool output, 105**partition map entry, 103-104*

BSD, 111

*analysis, 125**data structures, 116-125**overview, 112*

creating, 70-72

defined, 70-72

DOS, 81-82, 85-88

*analysis, 100**boot code, 87**extended partitions, 93-95**MBR concepts, 83**MBR disks, 88-92, 98-99*

EFI partitions, 127

extended (DOS), 92

overview, 83-87

extracting contents, 77-79

GPT, 139

*analysis, 144**data structures, 140-143*

investigating, 69

organizing volumes, 72

primary extended partitions (DOS), 83

primary file system partitions (DOS), 83

recovering, 79-80

removable media, 107-208

secondary extended partitions (DOS), 84

secondary file system partitions
(DOS), 84

slices (Solaris), 127

*analysis, 139**i386 data structures, 135-138**Sparc data structures, 128-133*

Sparc Solaris disk, 485

VTOC structures, 131

pdisk tool, 106**Penguin Sleuth Kit, 162****physical addresses, 33, 74**

- physical extents, 160
- PICL guidelines (preservation, isolation, correlation, and logging), 8
- platters, 30
- POSIX ACL attribute, 464
- preservation
 - digital crime scenes, 5
 - guideline, 8
- primary extended partitions (DOS), 83
- primary file system partitions (DOS), 83
- Private Header, 164
- ProDiscover toolkit, 15, 155
- protecting data, 53-55
- Q-R**
- \$Quota file, 339-340, 388-389
- RAID (Redundant Arrays of Inexpensive Disks), 147
 - acquisition and analysis, 154
 - hardware, 151-152
 - investigation concerns, 155
 - levels, 148-150
 - software, 153
- Read Only Memory (ROM), 28
- READ_NATIVE_MAX_ADDRESS command, 37
- reconstructing events, 8
- recovering deleted files
 - ExtX, 446
 - FAT file systems, 247
 - NTFS, 348
 - UFS, 504
- recovering partitions, volume analysis, 79-80
- Redundant Arrays of Inexpensive Disks.
See RAID
- reference models, 174
- removable media, 107-108
- \$Reparse file, 335
- \$REPARSE_POINT attribute, 282, 368
- ribbon cables, 32
- ROM (Read Only Memory), 28
- root directories
 - ExtX, 424
 - FAT, 214
 - NTFS, 334
 - UFS, 497
- S**
- SCA (Single Connector Attachment) connectors, 43
- SCSI (Small Computer Systems Interface), 29, 41
 - connector types, 43
 - size barriers, 44
 - types of, 42
 - vs. ATA, 41
- secondary extended partitions (DOS), 84
- secondary file system partitions (DOS), 84

INDEX

sectors

- addresses, 33, 74
 - CHS addresses, 34*
 - converting from cylinder addresses, 34*
 - DCO, 38*
 - disk commands, 35*
 - hard disk passwords, 36*
 - HPA, 36*
 - interface standards, 34*
 - LBA, 31*
 - serial ATA, 39*
- hard disks, 31

secure delete tools, 185**\$Secure file, 278, 322****\$SECURITY_DESCRIPTOR attribute, 282, 322****Security ID (SID), 288****SECURITY_UNLOCK command, 36****Self-Monitoring Analysis and Reporting Technology (SMART), 35****set group ID (SGID), 415****set user ID (SUID), 415****SET_MAX_ADDRESS command, 37****SFN (short file name) directory entry, 239****SGID (set group ID), 415****SID (Security ID), 288****sigfind tool, 219, 238, 308, 406, 543****single block pointers, 416****Single Connector Attachment (SCA) connectors, 43****slack space, 187****Sleuth Kit, The. *See* TSK****slices (Solaris), 127**

- analysis, 139
- i386 data structures, 135-138
- Sparc data structures, 128-133

Small Computer Systems Interface (SCSI) disks, 29**SMART (Self-Monitoring Analysis and Reporting Technology), 35****SMART toolkit, 15****soft links. *See* symbolic links****software**

- RAID, 153
- write blockers, 55

Solaris slices

- analysis, 139
- bootable CDs, 109
- i386 data structures, 135-138
- overview, 127
- slices
 - analysis, 139*
 - i386 data structures, 135-138*
 - Sparc data structures, 128-133*
- Sparc data structures, 128-133
- VTOC structures, 128

source data, reading, 49**spanning (disk), 156**

- acquisition and analysis, 159
- Linux LVM, 160-161
- Linux MD, 158
- overview, 157
- Windows LDM, dynamic disks, 162-169

Sparc data structures, 128-133**sparse attributes (MFT entries), 284**

sparse files (metadata category) 191, 416, 493

speed (SCSI drives) 41

\$STANDARD_INFORMATION

attribute, 282, 316, 359

storage devices

acquiring, 47-48

volumes, 10-11

streams, 356

strings, 22, 24

SUID (set user ID), 415

superblock

ExtX, 399-400, 449-451

flag values, 454

major version, 452

UFS file system category, 481

UFS1, 509, 515

general flags, 513

UFS2, 515, 519

\$SYMBOLIC_LINK attribute, 282

symbolic links, 335, 426, 470, 498

symmetric encryption, 288

System Preservation Phase (digital investigations), 5-6

T

TCT (The Coroner's Toolkit), 538

The Sleuth Kit. *See* TSK

toolkits. *See also* TSK

EnCase, 14

FSK, 14

ProDiscover, 15

SMART, 15

triple block pointers, 416

TSK (The Sleuth Kit), 13-14, 174, 537-543

dcat tool, 181, 540

diskstat tool, 52, 63, 538

dls tool, 184, 539

dstat tool, 490

ffind tool, 204, 542

fls tool, 203, 432

fsstat tool, 178, 539

ExtX, 402

FAT, 216, 266

NTFS, 306

UFS2, 486, 520

icat tool, 194, 354

ils tool, 433

istat tool, 540

ExtX, 418

FAT, 232, 266

NTFS, 297, 302

UFS, 494

jcat tool, 542

jls tool, 478

mmls tool, 98, 105, 122, 134, 144, 538

overview, 537

searching tools, 543

sigfind tool, 219, 238, 308, 406, 543

volume system tools, 538

file name category, 541-542

multiple tools, 543

types (FAT file systems) 249

INDEX

U**UFS (UNIX File System), 397**

block pointers, 415

blocks, 488

content category

allocation algorithms, 490

analysis, 491

overview, 488-490

extended attributes, 463, 466

file allocation example, 500-501

file deletion example, 503

file name category

allocation algorithms, 498

analysis, 499

overview, 497

root directory, 497

file recovery, 504

file system category

analysis, 487

boot code, 485

cylinder group descriptor, 482

superblock, 481

fragments, 488

inodes, 413

journal revoke blocks, 476

logical group addresses, 409

metadata category

allocation algorithms, 494

analysis, 495-496

extended attributes, 493

inodes, 492

overview, 481

UFS1

blocks and fragment bitmaps, 525-527

cylinder group summary data

structures, 521

directory entry, 534-535

general flags, 513

group descriptor data structures, 522-523

inodes, 527-528

superblock, 509-515

UFS2

blocks and fragment bitmaps, 525-527

cylinder group summary data

structures, 521

directory entry, 534-535

extended attributes, 532-533

group descriptor data structures, 524

inodes, 531

superblock, 515-520

unallocated data units, extracting, 183**unallocated metadata analysis (metadata category), 195****Unicode character storage, 23****union mount, 498****Unix File System. *See* UFS****UNIX partition usage, 72****Unix sockets, 414****\$Uppcase file, 278****Update Sequence Number (USN), 344****updating time values**

ExtX, 419

NTFS, 325

USN (Update Sequence Number), 344**\$UsrJrnl file, 392-395**

V

VCN (Virtual Cluster Number), 281, 321

volume analysis, 75

consistency checks, 76-77

extracting partitions, 77-79

recovering partitions, 79-80

techniques, 75

volume entries, 164

\$Volume file, 278, 305, 385

volume groups, 160

\$VOLUME_INFORMATION

attribute, 282

\$VOLUME_NAME attribute, 282

volume slack, 178

\$VOLUME_VERSION attribute, 282

volumes

assembly, 73

defined, 70

logical volumes, 157

organizing partitions, 72

RAID, 153

storage, 10-11, 69

VTOC (Volume Table of Contents), 485.

See also Solaris slices

W-Z

Windows

DEFRAG utility, 236

RAID volumes, 155

Windows 2000 investigations, 330

Windows LDM, dynamic disks, 162

acquisition and analysis, 168-169

LDM database, 164-167

WinZip, 191

wiping techniques

content category, 185

file name category, 204

metadata category, 198

write blockers

hardware, 53-55

software, 55

XOR operator, 150