Index

Symbols

$AttrDef file, 278, 382
  overview, 305-306
$ATTRIBUTE_LIST attribute, 282, 365-366
  NTFS, 321
$BadClus file, 278
  overview (NTFS), 312
$BITMAP attribute, 276, 372
$Bitmap file, 278, 383
  overview (NTFS), 312
$BITMAT attribute, 282
$Boot file, 278, 379-381
  overview, 304
$DATA attribute, 282, 364
  NTFS, 319
$EA attribute, 282
$EA_INFORMATION attribute, 282
$Extend file, 278
$FILE_NAME attribute, 282, 362-364
  NTFS, 318
$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, 379
  overview, 302
$MFTMirr file, 278
  overview, 303
$OBJECT_ID attribute, 335, 367-368
$Quota file, 388-389
$Quotas file, 340
$Reparse file, 335
$REPARSE_POINT attribute, 282, 368
$Secure file, 278
  NTFS, 322
$SECURITY_DESCRIPTOR attribute
  NTFS, 322
$STANDARD_INFORMATION attribute, 282, 359
  NTFS, 316
$SYMBOLIC_LINK attribute, 282
$Upcase file, 278

$UsrJrnl file, 392-395
$Volume file, 278, 385
  overview, 305
$VOLUME_INFORMATION attribute, 282
$VOLUME_NAME attribute, 282
$VOLUME_VERSION attribute, 282
-r flag, 194
4.2BSD fast file system (FFS), 119
64-bit Intel Itanium processors (IA64), 139

A

a-time, 196, 419
access control lists (ACLs), 417
accessing
  data, 49-50
  hidden data, 52
ACLs (access control lists), 417
acquiring
  data, 48-49
    dd tool, 60
    dead acquisition, 50-51
    live acquisition, 50-51
  files via networks, 59
  storage devices, 47-48
acquisition tools, error handling, 51
addresses
  clusters and sectors, 223
  directory entries, 230
addressing (sectors), 74
ADS (alternate data streams), 283, 319
allocation algorithms
  clusters (FAT), 224
  ExtX
    content category, 410
    metadata category, 418-419, 429
  FAT file system, metadata category, 233-234
  file name category
    FAT file systems, 241
    UFS, 498
  NTFS, 313
    file name category, 336
    metadata category, 324-325
  UFS, 494
    overview, 490
allocation status (inodes), 413
alternate data streams (ADS), 283, 319
analysis. *See also* analyzing
  Apple partitions, 107
  application category (file system journals), 205
  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
  file system category, 177
    analysis techniques, 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
UFS, 495-496
volume analysis, 75
consistency checks, 76-77
extracting partitions, 77-79
recovering partitions, 79-80
techniques, 75
analyzing. *See also* analysis
BSD partitions, 125
data, 10-11
Ext3, application category, 439-441
ExtX
content category, 411-412
file system category, 404-408
metadata category, 421-423, 430-434
FAT file systems
content category, 225-226
file name category, 241-244
file system category, 217-221
metadata category, 235-238
NTFS, 296, 307-309
content category, 315
file name category, 336-339
metadata category, 326-332
Solaris systems, 139
UFS
file name category, 499
file system category, 487
overview, 491
Apple partitions, 101
analysis, 107
data structures
Image tool output, 105
partition map entry, 103-104
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, storing a sentence or word, 23
assembly (volumes), 73
asymmetric encryption, 288
AT Attachment (ATA/IDE) disks, 29-30
AT Attachment Packet Interface (ATAPI), 35
ATA, 151
commands, 52
drives (vs. SCSI), 41
interface, 32
ATA-3, security, 36
ATA/IDE (AT Attachment) disks, 29-30
ATAPI (AT Attachment Packet Interface), 35
$AttrDef file, 278, 382
overview, 306
attribute headers, MFT entries, 355-359
$ATTRIBUTE_LIST attribute, 282, 365-366
NTFS, 321
attributes
$ATTRIBUTE_LIST attribute, 282, 365-366
NTFS, 321
$BITMAP attribute, 276, 372

$BITMAT attribute, 282
$DATA attribute, 282, 364
NTFS, 319
$EA attribute, 282
$EA_INFORMATION attribute, 282
$FILE_NAME attribute, 282, 362-364
NTFS, 318
$INDEX_ALLOCATION attribute, 282, 295, 336, 371-372
$INDEX_ROOT attribute, 282, 295, 336, 369-370
inodes, 417
$LOGGED_UTILITY_STREAM attribute, 282, 288
$OBJECT_ID attribute, 335, 367-368
$REPARSE_POINT attribute, 282, 368
$SECURITY_DESCRIPTOR attribute
NTFS, 322
$STANDARD_INFORMATION attribute, 282, 359
NTFS, 316
$SYMBOLIC_LINK attribute, 282
$VOLUME_INFORMATION attribute, 282
$VOLUME_NAME attribute, 282
$VOLUME_VERSION attribute, 282
Autopsy (TSK), 15
overview, 544

B

B-trees, 290
$BadClus file, 278
overview (NTFS), 312
base MFT entries, 284
Basic Input/Output System. *See* BIOS
best fit strategy, 180
binary numbers, 18
converting to decimal value, 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, 372
$Bitmap file, 278, 383
overview (NTFS), 312
$BITMAT attribute, 282
block bitmap (ExtX), 456
block bitmaps, 401
block devices, 414
blocks
allocating, 490
block pointers, 415
content category, 409
extended attributes, 463, 466
fragments, 488
inodes, 413
journal revoke blocks, 476
logical group addresses, 409
UFS2, 525-527
boot code, 115
$Boot file, 278, 379-381
overview, 304
boot loader, 402
boot sector
essential data, 214
FAT file system, 213, 253-257
volume serial numbers, 258
non-essential data, 216
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

DOS disks, 87
FAT file system, 216
locations, 28
UFS file system category, 485
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

C

c-time, 196, 420
calculating
cryptographic hashes, 6
hashes, 59
case studies
dd tool, 60-63
cryptographic hashes, 65-66
error handling, 64-65
HPA, 61-63
input sources, 61
output destinations, 63-64
CD-Rs, 108
Central Processing Units (CPUs), 27
CFTT (Computer Forensic Tool Testing), 49
change journal feature (NTFS), 343
character devices, 414
character encoding, 22-24
CHS method, 33
cluster chains, 229
clusters, 222
$BadClus file, 312
addresses, 223
allocation status, 223
content category (NTFS), 311
determining allocation status, 383
commands (ATA), 52
commit blocks, 477
component entries, 164
compressed attributes (MFT entries), 285
compressed files (metadata category), 191
compressing images, 58-59
Computer Forensic Tool Testing (CFTT), 49
CONCAT, 166
conducting investigations, 5
connector types (SCSI drives), 43
consistency checks, 184
ExtX, 446
FAT file systems, 250
file name category, 204
metadata category, 198
NTFS, 349
techniques, 75
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
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
copying data, 47-48
The Coroner's Toolkit, 207
correlation (guideline), 9
corruption of drives, minimizing, 73
CPUs (Central Processing Units), 27
creating
HPA, 37
partitions, 70-72
crime scenes (digital), preserving, 5
cryptographic hashes
calculating, 6
dd tool, 65-66
cryptography (NTFS), 288
cylinder group descriptor (UFS file system category), 482
cylinder group summary data structures (UFS1), 521
cylinder groups, 479, 483
allocation of blocks and fragments, 490
descriptors, 482
USF1, 521
USF2, 520

D

D-time, 420
damaged data units, 181
data
accessing, 49
BIOS, 49-50
acquiring, 48-49
dd tool, 60
dead acquisition, 50-51
live acquisition, 50-51
analyzing, 10-11
carving, 206
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
reading/writing, 49
saving, 56-57
source data, reading, 49
structures. *See* data structures
write protecting, 53-55
$DATA attribute, 282, 364
NTFS, 319
data carving, 206
data categories (file systems), 174
data decryption fields (DDF), 288
data recovery fields (DRF), 288
data structures, 24
allocation order
file name category, 204
metadata category, 197

block bitmaps, 456
BSD partitions, 116
disk labels, 116-119
  FreeBSD example image, 123-125
  OpenBSD example image, 120-121
directory entries, 467-469
directory entry (UFS), 497
disk labels, 112
extended attributes, 462-465
FAT boot sector, 254
GPT partitions, 140-142
  Intel defined, 143
  Microsoft defined, 143
group descriptor tables, 455
hash trees, 470-472
i386, 135-139
inodes, 457-461
  allocation status, 461
journal data structures, 473-477
NTFS
  attribute headers, 355-359
  directory index entry data structure, 376-377
  fixup values, 352
  generic index entry data structure, 375
  index attributes, 369-372
  index node header data structure, 373-374
  MFT entries, 353-354
  standard file attributes, 359-368
Sparc, 128-133
symbolic links, 470
UFS1
  cylinder group summary data structures, 521
  directory entities, 534-535
  group descriptor data structures, 522-523
  inodes, 527-528
  superblock, 509, 513-515
UFS2
  blocks and fragment bitmaps, 525-527
  directory entities, 534-535
  extended attributes, 532-533
  group descriptor data structures, 524
  inodes, 531
  superblock, 515-519
data units, 174
  allocation order, 184
  allocation status, 183
  orphan, 184
  viewing, 181
dates, converting to FAT date format, 263
dcat tool, 181
DCOs (Device Configuration Overlays), 38, 53
  detecting, 53
  removing, 53-54
dd command, 514
dd tool
  acquiring data, 60
    case study, 60-63
    cryptographic hashes, 65-66
    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 analyses, 6
decimal numbers, 18
  converting
    from binary numbers, 18
    from hexadecimal numbers, 20
DEFRAG utility, 236
deleting files
  BSD, 495
  Ext3, 443
  NTFS, 346
  Solaris, 495
  UFS, 502
descriptor blocks, 477

detecting
DCOs, 53
HPA, 52
determining types of FAT file systems, 249
Device Configuration Overlays (DCO), 38, 53
detecting, 53
removing, 53-54
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
defined, 4
Event Reconstruction Phase, 8
Evidence Searching Phase, 7
focus, 3
forensic, 4
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 entities
UFS1, 534-535
UFS2, 534-535
directory entries
content category (FAT file systems), 227
ExtX, 467-469
metadata category, 424-425
FAT file systems, 261-265
ordering (FAT file system), 243
time value updating, 234
directory entry data structure (UFS), 497
directory index entry data structure, 376-377
directory indexes (NTFS), 333
disk commands, 35
disk entries, 164
disk groups, 157
disk labels, 112
BSD partitions, 116-119
FreeBSD, 113
Sparc, 128
disk quotas (NTFS), 339
disk spanning, 156
acquisition and analysis, 159
Linux LVM, 160
acquisition and analysis, 161
Linux MD, 158
overview, 157
Windows LDM, dynamic disks, 162-169
disks
booting, 27
boot code locations, 28
CPUs and machine code, 27
DOS, boot code, 87
GPT, 140
data structures, 142
hard disks, 29. *See also* hard disks
ATA interface, 32
BIOS vs. direct access, 39-40
cylinder groups, 483
geometry and internals, 29-31
SCSI drives, 41-44
sector addresses, 33-39
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
dls tool, 184
DOS
bootable flags, 89
disks, boot code, 87
partitions, 81-82, 85-88
DOS Extended file system, 97
DOS partitions, 81-82, 85-88
boot code, 87
extended, 93, 95
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
drives
corruption, minimizing, 73
SCSI, 41
connector types, 43
size barriers, 44
types of, 42
vs. ATA, 41
dstat tool, 490
dynamic disks
Windows LDM, 162
acquisition and analysis, 168-169
LDM database, 164-167
dynamic version, 452

E

$EA attribute, 282
$EA_INFORMATION attribute, 282
effectiveness of software write blockers, 55
EFI (Extensible Firmware Interface), 139
disks, 81
partitions, 127
embedded images, 57
EnCase, 14, 155
encrypted attributes (MFT entries), 287
encrypted files (metadata category), 192
EOF (End of File) markers, 229
error handling
acquisition tools, 51
dd tool, 64-65
superblock, 452
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, 397
Ext3, 397
analysis, 440-441
file allocation example, 441
file deletion example, 443
file system journaling, 437-438
$Extend file, 278
extended attributes
ExtX, 462-465
UFS, 493
UFS2, 532-533
extended partition, 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
block bitmap, 456
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 name category
allocation algorithms, 429
analysis, 430-434
hash trees, 428
links, 426
overview, 424-425
file recovery example, 446
file system category
analysis, 404-408
block group descriptor tables, 401-402
overview, 399
superblock, 399
group descriptor tables, 455-456
hash trees, 470-472
inodes, 457-461
allocation status, 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, 470
time value updating, 419

F

Fast File system (FFS), 479
FAT (File Allocation Table) file system, 211
boot sector, 253-258
volume serial numbers, 258
consistency checks, 250
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
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
LFN 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
FEK (file encryption key), 288
ffind tool, 204, 542
FFS (Fast File System), 479
FIFO, 414
file allocation (UFS), 500-501
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, 362-364
NTFS, 318
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
hash trees, 428
links, 426
overview, 424-425
FAT, 239
allocation algorithms, 241
analysis, 241-244
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
overview, 497
wiping techniques, 204
file name listing, 202
file name searching, 203
file records, 275, 353. *See also* MFT entries
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
analysis by category, 173, 177. *See also* analysis
data categories, 174
dealing with specific kinds, 207
essential/non-essential data, 176
Ext3
analysis, 440-441
file allocation example, 441
file deletion example, 443
journaling, 437-438
extracting unallocated data units, 184
ExtX
consistency checks, 446
content category, 409-412
file name category, 424-434
file recovery example, 446
file system category, 399-408
metadata category, 413-423
FAT, 211
boot sector, 253
consistency checks, 250
content category, 221-226
determining type, 249
file allocation example, 244
file deletion example, 246
file name category, 239-244
file recovery, 247
file system category, 213-221
metadata category, 227-238
overview, 212
NTFS, 211
consistency checks, 349
file allocation example, 344
file deletion example, 346
file recovery, 348
file system layout, 313
metadata files, 379-395
overview, 173
UFS, 397
content category, 488-491
file allocation example, 500-501
file deletion example, 503
file name category, 497-499
file recovery, 504
file system category, 481-482, 485-487
metadata category, 492-496
overview, 480
UFS1
cylinder group summary data structures, 521
directory entities, 534-535
group descriptor data structures, 522-523
inodes, 527-528
superblock, 509, 513-515
UFS2
blocks and fragment bitmaps, 525-527
directory entities, 534-535
extended attributes, 532-533
group descriptor data structures, 524
inodes, 531
superblock, 515, 519
file type sorting, 207
files
acquiring via networks, 59
attribute headers, 355-359
block pointers, 415
recovering (FAT file systems), 247
files, 57. *See also* images
finding the source of a moved file, 432

Firewire, 151
first available strategy, 179
fixup values, 352
flags, 26-27
fls tool, 203, 432
focus of digital investigations, 3
foremost tool, 206
forensics, 4
Forensic Toolkit, The (FSK), 14
format (images), 57
fragment bitmaps (UFS2), 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, 216, 266
  running on the UFS2 image, 520
  showing clusters, 226
FTK (The Forensic Toolkit), 14

G

generic index entry data structure, 375
geometry (hard disks), 29
  platters, 31
Globally Unique Identifier (GUID), 164
GPT (GUID Partition Table) disks, 81
GPT partitions, 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
  cylinder groups, 483
  geometry and internals, 29
    platters, 31
    sectors, 31
  SCSI drives, 41
    connector types, 43
    size barriers, 44
    types of, 42
    vs. ATA, 41
  sector addresses, 33
    CHS addresses, 34
    DCO, 38
    disk commands, 35
    hard disk passwords, 36
    HPA, 36
    interface standards, 34
    serial ATA, 39
hard links, 334, 426
hardware
  block devices, 414
  RAID, 151-152
hardware write blockers, 53-55
hash trees, 428
  ExtX, 470-472

hashes
  calculating, 59
  cryptographic hashes, 6
  integrity hashes, 59-60
hexadecimal numbers, 19
  converting to decimal values, 20
hidden data, 52
high voltage differential (HVD), 42
HPA (Host Protected Area), 36, 52
  detecting
  removing, 52-54
HTML, Autopsy, 544
HVD (high voltage differential), 42

I

i386 data structures, 135-138
IA32-based hardware, 111
icat tool, 194, 354
IDE (Integrated Disk Electronics) disks, 32
IDENTIFY_DEVICE command, 37
IDS (Intrusion Detection System), 48, 196
ils tool, 433
Image tool output, 97-99
  Apple partitions, 105
images, 57. *See also* files
  compressing, 58-59
  embedded, 57
  format, 57
implementing
  preservation, 8
  RAID, 151
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, 402
inodes
  allocation algorithms, 418-419
  ExtX, 413-414, 457-461
    allocation status, 461
    attributes, 417
  sniffer logs, 433
  time value updating, 419
  UFS, 492
  UFS1, 527-528
  UFS2, 530
input sources (dd tool), 61
Integrated Disk Electronics (IDE) disks, 32
integrity hashes, 59-60
internals (hard disks), 29
International Committee on Information Technology Standards (INCITS), 32
Intrusion Detection System (IDS), 48, 196
investigations
  Autopsy, 544
  conducting, 5
  digital, 3
    defined, 4
    Event Reconstruction Phase, 8
    Evidence Searching Phase, 7
    focus, 3
    forensic, 4
    System Preservation Phase, 5-6
  guidelines, 8-9
  Linux systems, file deletion order, 435

partitions, 69
RAID systems, 155
isolation (guideline), 9
istat tool, 266, 297, 302

J

jcat tool, 542
jls tool, 478
journal data structures (ExtX), 473-477
journaling
Ext3, 437-438
NTFS, 340, 343
junctions, 335

K-L

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
ExtX, 426
hard links, 334
junctions, 335
symbolic, 470
symbolic links, 335
Linux, 92
file deletion order, 435
finding the source of a moved file, 432
superblock, 401
Linux LVM, 160-161
Linux MD software RAID, 155
Linux swap partitions, 96
live acquisition, 50-51
live analyses, 6
local file viewing (metadata category), 193
locating
clusters, 222
volume serial numbers, 258
$LogFile file, 278, 391
$LOGGED_UTILITY_STREAM attribute, 282, 288
logging (guideline), 9
Logical Block Address (LBA), 31
Logical Cluster Number (LCN), 281
Logical Disk Manager (LDM) controls, 153
logical extents, 160
logical file searching (metadata category), 194
logical file system addresses, 179
logical file system-level searching, 182
logical group addresses, 409
logical volume addresses, 74, 179
Logical Volume Manager (LVM), 158
logical volumes, 157
long file name (LFN) directory entries, 267
long file name attribute, 228
low voltage differential (LVD), 42
LSN ($LogFile Sequence Number), 323
LVD (low voltage differential), 42
LVM (Logical Volume Manager), 158

M

m-time, 196, 420
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
attribute content, 280
base MFT entries, 284

compressed attributes, 285
encrypted attributes, 287
sparse attributes, 284
standard attribute types, 282
overview, 275
MBR (Master Boot Record), 402
MBR (Master Boot Record) 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
wiping techniques, 198
compressed and sparse files, 191
encrypted files, 192
ExtX
allocation algorithms, 418-419
analysis, 421-423
inodes, 417
overview, 413-414
FAT
analysis, 235-238
cluster chains, 229
directories, 230
directory entries, 227
directory entry allocation, 233
example image, 233
time value updating, 234
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
metadata-based file recovery, 188-190
metadata lookup (metadata category), 193
MFT (Master File Table), 274
entry addresses, 277
entry contents, 276
file system metadata files, 278
MFT entries, 279
attribute content, 280
base MFT entries, 284
compressed attributes, 285
encrypted attributes, 287
sparse attributes, 284
standard attribute types, 282
overview, 275
MFT entries, 353-354
non-base, 366
$MFT file, 276, 379
overview, 302
MFT Zone, 313
$MFTMirr file, 278
overview, 303

minimizing drive corruption, 73
mounting (FreeBSD partition), 122
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

NAMRFP (National Association of Medical Record Filing Procedures), 173
National Institute of Standards and Technology (NIST), 49
NetBSD, 115
Network File System (NFS), 415
networks, acquiring files 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
non-essential file system data, 176
nonessential data, 12-13
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 file systems, 92
slack space, 188
NTFS Master File Table (MFT), 175
NTFSInfo tool, 296

O

$OBJECT_ID attribute, 335, 367-368
object IDs (NTFS), 335
opcode, 27
OpenBSD, 115
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
output destinations (dd tool), 63-64

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, 92
overview, 83-87
extracting volume analysis, 77-79
GPT, 139
analysis, 144
data structures, 140-143

investigating, 69
organizing volumes, 72
primary extended partitions, 83
primary file system partitions, 83
recovering, 79-80
removable media, 107
CD-ROMs, 108
secondary extended partitions, 84
secondary file system partitions, 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, 83
primary file system partitions, 83
Private Header, 164
ProDiscover toolkit, 15, 155
protecting data, 53-55

Q-R

$Quota file, 388-389
$Quotas file, 340
RAID (Redundant Arrays of Inexpensive Disks), 147
hardware, 151-152
investigation concerns, 155
levels, 148-150
software, 153
Read Only Memory (ROM), 28
reading source data, 49
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
CD-ROMs, 108
removing
DCOs, 53-54
HPA, 52
HPAs, 54
$Reparse file, 335
$REPARSE_POINT attribute, 282, 368
ribbon cables, 32
ROM (Read Only Memory), 28
root directories
NTFS, 334
UNIX, 72

S

saving data, 56-57
SCA (Single Connector Attachment) connectors, 43
scalability
NTFS, 273
SCSI (Small Computer Systems Interface), 151
disks, 29

drives, 41
connector types, 43
size barriers, 44
types of, 42
vs. ATA, 41
searching
for deleted directories, 238
for evidence, 7
tools (TSK), 543
secondary extended partitions, 84
secondary file system partitions, 84
sectors
addresses, 33, 74
CHS addresses, 34
converting from cylinder addresses, 133
DCO, 38
disk commands, 35
hard disk passwords, 36
HPA, 36
interface standards, 34
serial ATA, 39
hard disks, 31
secure delete tools, 185
$Secure file, 278
NTFS, 322
$SECURITY_DESCRIPTOR attribute
NTFS, 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, 406
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
sniffer log inodes, 433
soft links, 426
software
RAID, 153
write blockers, 55
Solaris
analysis, 139
bootable CDs, 109
deleting files, 495
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
sources (dd tool), 61
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
speed (SCSI drives) 41
$STANDARD_INFORMATION attribute, 282, 359
NTFS, 316
storage
digital, 69-70
Unicode characters, 23
volumes, 69
storage devices
acquiring, 47-48
volumes, 10-11
streams, 356
strings, 22, 24
SUID (set user ID), 415
superblock, 399-400
ExtX, 449-451
flag values, 454
major version, 452
OpenBSD systems, 514
UFS file system category, 481
UFS1, 509, 515
general flags, 513
UFS2, 515, 519
$SYMBOLIC_LINK attribute, 282
symbolic links, 335
ExtX, 470
symmetric algorithm, 288
System Preservation Phase (digital investigations), 5-6

T

TB (terabytes), 82
TCT (The Coroner's Toolkit), 538
terabytes (TB), 82
The Sleuth Kit. *See* TSK
time values, updating, 234
toolkits
EnCase, 14
FSK, 14
ProDiscover, 15
SMART, 15
TSK, 13. *See also* TSK
tools
acquisition tools, error handling, 51
dd tool, case studies, 60-66
triple block pointers, 416
TSK (The Sleuth Kit), 13-14, 174
dcat tool, 181
disk tools, 538
dls tool, 184
dstat tool, 490
ffind tool, 204, 542
file system tools, 539
metadata category, 540
fls tool, 203, 432
fsstat tool, 178, 216, 266
icat tool, 194, 354
ils tool, 433
istat tool, 266, 297, 302
jcat tool, 542
jls tool, 478
overview, 537
searching tools, 543
volume system tools, 538
file name category, 541-542
multiple tools, 543
types (FAT file systems) 249

U

UFS (UNIX File System), 397
content category
allocation algorithms, 490
analysis, 491
overview, 488-490
ExtX, 398
file allocation example, 500-501
file deletion example, 503
file name category
allocation algorithms, 498
analysis, 499
overview, 497

file recovery, 504
file system category
analysis, 487
boot code, 485
cylinder group descriptor, 482
superblock, 481
metadata category
allocation algorithms, 494
analysis, 495-496
extended attributes, 493
inodes, 492
overview, 481
UFS1
cylinder group summary data structures, 521
directory entities, 534-535
group descriptor data structures, 522-523
inodes, 527-528
superblock, 509, 515
general flags, 513
UFS2
blocks and fragment bitmaps, 525-527
directory entities, 534-535
extended attributes, 532-533
group descriptor data structures, 524
inodes, 531
superblock, 515, 519
unallocated data units, extracting, 183
unallocated metadata analysis
metadata category, 195
Unicode character storage, 23
union mount, 498
UNIX
directories, 427
root directories, 72
volumes, 72-73
Unix File System. *See* UFS
Unix sockets, 414
$Upcase file, 278
Update Sequence Number (USN), 344
updating time values
ExtX, 419
NTFS, 325
USN (Update Sequence Number), 344
$UsrJrnl file, 392-395
UTF-16 Unicode, 385

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, 385
overview, 305
volume groups, 160
$VOLUME_INFORMATION attribute, 282
volume label, 228
$VOLUME_NAME attribute, 282
volume slack, 178
$VOLUME_VERSION attribute, 282
volumes
assembly, 73
defined, 70
logical volumes, 157
organizing partitions, 72
RAID, 153
serial numbers, 258
storage, 10-11, 69
UNIX systems, 72-73
VTOC (Volume Table of Contents), 485
VTOC structures, 128, 131, 135

W-Z

Web sites
  gzip, 191
  Linux NTFS, 164
  Penguin Sleuth Kit, 162
  TCT (the Coroner's Toolkit), 538
  The Coroner's Toolkit, 207
  WinZip, 191
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
writing data, 49

XOR operator, 150