

Index

Note to the reader: Throughout this index **boldfaced** page numbers indicate primary discussions of a topic. *Italicized* page numbers indicate illustrations. See also the appendices.

Symbols and Numbers

\$. file, 66
 \$AttrDef file, 66
 \$BadClus file, 66
 \$Bitmap file, 65–66
 \$Boot file, 66
 \$Extend file, 67
 \$LogFile file, 66
 \$MFT (master file table) file, 65–66
 \$MFTMirr file, 66
 \$Secure file, 66
 \$UpCase file, 67
 \$Volume file, 66
 . (period), in GREP expression, 268
 @ symbol, in web mail address search, 268
 NextPart string, 453
 “0x” for hexadecimal, 250
 “8 dot 3” DOS naming convention, 43
 64-bit time stamp, 338, 338–341, 340
 1394a protocol, 129

A

aborting process, 215
 About EnCase window, installed modules list
 in, 457, 460
 Accelerated Graphics Port (AGP), 8
 acquisition, 473
 drive-to-drive DOS acquisition, 110–116
 compression in, 113
 exam essentials, 147
 FastBloc, 129–135
 helpful hints, 144

 LinEn (EnCase for Linux), 135–140
 spanning drives during, 160–161
 acquisition hash, 128, 158, 162
 acronyms, 2
 Active Code Page keyword search
 option, 262
 ActiveTimeBias TimeZoneInformation key
 value, 342, 343
 Add Device dialog box, 131, 131
 Add Keyword List dialog box, 264, 264
 Add Note Bookmark window, 283, 283
 Add Partition dialog box, 405, 406
 addressing schemes, for hard drive
 platters, 4–5
 Advanced Technology Attachment (ATA), 5
 After Acquisition dialog box, 123
 after-hours response, to incident, 79
 AGP (Accelerated Graphics Port), 8
 AIM Plus history files header, GREP
 expression for searches, 271
 alias, for long file names, 45
 America Online (AOL), .art files, 206
 American Standard Code for Information
 Interchange, 252
 antistatic bagging, 93
 AppDescriptors.ini file, 173
 application binding, 308–310
 applications
 and evidence file restoration, 465
 exporting, 462–465
 locating executable, 464, 464
 on Mac, 234
 .art files, 206
 artifacts, 336
 recovering, exercise, 387–390
 ASCII characters, 252–253
 ATA (Advanced Technology Attachment), 5

508 \$AttrDef file – boot sector

\$AttrDef file, 66
 attribute bit flag values, 44
 audio (sound) card, 8
 authorization for search, 84
 auto-login feature, and password recovery, 457
 autoexec.bat file, 14, 417
 automatic backup, timing of, 171

B

backup file (cbak), 170–173, 473
 opening, 172, 172
 promoting to case file, 172, 172
 timing of automatic, 171
 backups of INI files, 175
 bad cluster, 41
 bad file signature, 315
 \$BadClus file, 66
 bagging evidence, 92–95, 157
 base 2, raising to powers, 244–245
 base-16 encoding (hexadecimal numbering), 249–251
 Base64 Encoded Picture bookmark data type, 281
 Base64 encoding, 449–456, 450
 batch files, 14
 Bemmer, Robert W., 252
 best practices, 189
 BestCrypt, 88
 Bias TimeZoneInformation key value, 342
 Big-Endian Unicode keyword search option, 262
 binary numbers, 243–248
 binding applications, 308–310
 BinHex encoding, 450
 BIOS (Basic Input Output System), 9
 bypassing passwords, 9
 BIOS parameter block (BPB), 34, 35
 \$Bitmap file, 65–66
 bits, 243
 names of groupings, 247
 block size, 125
 and error granularity, 126
 and evidence file corruption, 165
 in Linux, 139
 Blue Screen of Death (BSOD), 471
 Bookmark Data window, 280, 280
 for EMF print file, 385
 bookmarks, 279–293
 for cached items, 377, 378
 color for, 232
 data types, 281–282
 for directory entry information, 48, 48, 50
 for e-mail, 446
 exam essentials, 299
 exercise, 294–297
 extracting and summarizing time zone information, 344
 File Group bookmark, 289, 290
 Folder Information Bookmark, 284–286, 285
 hashing thread results, 290
 Highlighted Data bookmark, 279, 279–283
 Notable File bookmark, 286–289
 Notes bookmark, 168, 283, 284, 290
 organizing, 291–293
 for search results, exercise, 294–297
 search summary bookmark, 291
 in Table view, 291
 Bookmarks case-level tab, 225
 Boolean indicator, 132
 boot disk, forensic, 105–106
 booting with, 107–110
 exam essentials, 146
 \$Boot file, 66
 boot order setting, in RTC/NVRAM, 9
 boot process, 11–16
 in DOS, 14, 15
 with EnCase boot disk, 107–110
 for network cable acquisition, 119
 in Windows NT/2000/XP, 15–16
 boot sector, 31, 33–34. *See also* volume boot sector

BOOT.INI file, 15
 bootstrap, 12, 13
 Bottom pane. *See* View pane
 BPB (BIOS parameter block), 34, 35
 BSD, hard drive acquisition, 116
 BSOD (Blue Screen of Death), 471
 business hours, response to incident
 during, 79
 bytes, 246
 decimal integer value for, 248
 bytes useable in hard drive sector, 5

C

C++ operators, in EnScript, 437
 cables
 flat ribbon, 130
 labeling, 92
 network
 crossover, 117
 for hard drive acquisition, 116–128
 parallel, 120
 cache
 GZIP files in, 445
 for web page files, 377, 444
 exercise, 388
 in Windows 98/Me, 134
 canceling process, 215
 Case Entries view, 186
 case files, 169–170
 Case Initialization EnScript, 473
 case-level views, keywords, 255, 256
 Case Options dialog box, 188
 case sensitivity of searches, 260, 261
 case time settings bookmark, 291
 cases, creating, 187–191
 .cbak file extension, 170–173
 cd command, 138
 CD/DVD drive
 helpful hints, 144
 paperclip to open, 109

 CD file systems, 68–69
 CD Inspector, 69
 CD-ROM (Compact Disc – Read-Only
 Memory) drive, 6–7
 CD-RW (Compact Disc – Read/Write)
 drive, 6–7
 central processing unit (CPU;
 microprocessor), 4
 chain of custody, 93
 Change Icon dialog box, 358
 characters, 252–254
 ASCII, 252–253
 Unicode, 253–254, 254
 Chinese, 254
 chmod command, 138
 Choose Destination dialog box, 106
 Choose Devices window, 466, 467
 icons, 131, 132
 chunks, 114
 CL indicator (Navigation data), 217
 Classic support, in Mac OS X, 234
 Cluster view, 208, 209
 clusters, 30
 data after end of logical file, 63
 FAT entry for, 51, 52
 FAT tracking for file, 50
 files spanning multiple, 53, 53
 search for first available, 56
 CMOS (Complementary Metal-Oxide
 Semiconductor), 8
 CMOS battery, 8, 9
 Code Page keyword search option, 262
 color palette, 232
 columns in Table View tab
 arranging for hash analysis, 323–324, 324
 hiding, 199
 lock, 196, 197
 COMMAND.COM, 14, 105
 compound files, 412–413
 exam essentials, 478
 list of common, 414–415
 compressed files, 473

510 **compression – Create Shortcut Wizard**

- compression
 - algorithms, 159
 - in drive-to-drive DOS acquisition, 113
 - of evidence file, 161
- computer forensics, changes, 475
- computer hardware components, 2–11
 - BIOS (Basic Input Output System), 9
 - case, 2–3
 - CD-ROM (Compact Disc – Read-Only Memory) drive, 6–7
 - CD-RW (Compact Disc – Read/Write) drive, 6–7
 - CMOS battery, 9
 - CMOS (Complementary Metal-Oxide Semiconductor), 8
 - DVD-ROM (Digital Versatile Disc – Read-Only Memory), 7
 - DVD-RW (Digital Versatile Disc–Read/Write), 7
 - exam essentials, 21
 - expansion slots, 7–8
 - fingerprints on, 85
 - floppy drive, 6
 - hard drive, 4–5
 - heat sink and fan, 4
 - IDE (Integrated Drive Electronics) controller, 5
 - IEEE 1394 (FireWire), 7
 - IEEE 1394a ports, 7
 - keyboard port, 10
 - microprocessor, 4
 - modem, 10
 - motherboard, 4
 - mouse port, 10
 - network interface card (NIC), 10
 - parallel port, 11
 - POST testing of, 12
 - power supply, 3–4
 - RAID (Redundant Array of Inexpensive Disks), 6
 - RTC (Real-Time Clock), 8
 - SATA (Serial Advanced Technology Attachment) controller, 6
 - SCSI (Small Computer Systems Interface), 5
 - serial port, 11
 - sound card, 8
 - USB controller, 7
 - USB port, 7
 - video card, 8
- computer systems
 - evaluating for evidence collection, 80–82
 - explanations to jury, 2
 - hidden, 93
 - inspection of interior, 109
 - nonfunctioning, 86–87
 - photographs to record “state,” 88
 - shutdown, 85–92
- conditions, in EnScripts, 441
- Conditions tab, in Filter pane, 219
- config folder, 424
- config.sys file, 14, 417
- configuration files, 173–175
- console mode, for LinEn, 136
- Console view, in View pane, 214, 214
- Content.IE5 folder, 377
- Control Panel, access timedate from, 436
- cookie files, 66
- Cookies folder, 371, 372
 - in Windows 9x, 386
- CookieView, 371, 372
- Copy Folders dialog box, 463
- copy, verifying consistency with original, 113
- copying EnScripts, 439
- corrupted images, crash protection from, 205
- corruption of evidence file, block size and, 165
- CPU (central processing unit; microprocessor), 4
- CRC (Cyclical Redundancy Check), 125, 157
- Create Hash Set dialog box, 321
- Create New Partition Wizard, 18
- Create Shortcut Wizard, 359, 359

creator code (Mac), 309
 crossover cable, 117
 CS (cable select) pinning method, 6
 CurrentControlSet, 424, 425
 Cyclical Redundancy Check (CRC), 125
 cylinder, 5

D

daisy chaining of FireWire devices, 129
 data, after end of logical file, 63
 data area of FAT system, 41–50
 data basics, 243–254. *See also* searches for data
 binary numbers, 243–248
 characters, 252–254
 ASCII, 252–253
 Unicode, 253–254, 254
 exam essentials, 299
 hexadecimal numbers, 249–251
 data blocks, in evidence file, 158, 159
 data fork (Macintosh), 450
 data integrity, exercise, 166–167
 Data Link Layer protocol, 10
 Date and Time Properties dialog box
 (Windows), Time Zone tab, 337,
 337–338
 date format, 230
 dates and times in Windows, 336–347
 64-bit time stamp, 338, 338–341, 340
 time zones, 337–338
 adjusting for offsets, 342–347
 dates, bookmark data types, 282
 day of week, displaying, 230
 DaylightBias TimeZoneInformation key
 value, 342
 DaylightName TimeZoneInformation key
 value, 342
 DaylightStart TimeZoneInformation key
 value, 343
 .dbx file extension, 414
 creator code – directory entries
 DCO (Device Configuration Overlay),
 107–108
 dd command, 156
 dead hard drive, recovering, 115
 debriefing, 78
 Decode Shell Extension tool, 455, 455
 Default Export folder, 188
 deleted files
 SID for tracking, 351, 352
 and status byte, 57
 VFS vs. PDE, 471
 viewing only, 208
 deleted partitions, recovering, 404
 deleting
 EnScripts, 439
 File Signatures database record, 310
 files from Recycle Bin, 353
 keyword folder, 257
 Description column in Table View, 201
 desktop
 creating shortcut, 359
 in Windows 9x, 386
 Desktop Contents bookmark folder, 387
 Desktop folder, 367–368
 Desktop Items dialog box, 368
 Details view, in View pane, 215
 Device Configuration Overlay (DCO),
 107–108
 Device Manager, for confirming FastBloc
 detection, 130, 130
 DEVICE statement, 14
 Devices case-level tab, 225
 digital evidence search-and-seizure
 specialist, 85
 Digital Video Interface (DVI), 8
 Direct ATA access, 111, 112
 DirectCD, 69
 directories. *See* folders
 directory entries (FAT), 43
 bookmark for information, 48, 48, 50
 data structure, 43
 and long file names, 44–45
 raw data in EnCase, 46, 46

512 disk caching – EnCase Enterprise

table, 56–58
viewing, 49

disk caching, in Windows 98/Me, 134

disk drives. *See* drives; hard drive

Disk Manager (Windows 2000/XP), 18

Disk tab
in Filter pane, color-coded legend, 207
in Table pane, 206–208, 207

Display Properties dialog box, General tab, 367

Dixon box, 194, 195, 215–216, 295
for selecting files for search, 272, 273

.doc file extension, 414

documentation
from Guidance Software, 458
of shutdown process, 92

DOS date bookmark data type, 282

DOS Directory Entry bookmark data type, 282

DOS file names, 43

DOS operating system
boot process in, 14, 15
MS-DOS time stamp, 347
shutdown procedures, 90

“dot double dot” signature, for directory, 64, 64

drive-to-drive DOS acquisition, 110–116
compression in, 113

DRIVER.CAB file, 16

drives. *See also* CD/DVD drive; hard drive
acquiring that being previewed, 122–123, 123
hashing, 167–169
unlocking, 113

drug sales example, 269–270

DRVSPACE.BIN file, 105

dust in computers, 87

DVD, GREP_Expressions folder, 271

DVD-ROM (Digital Versatile Disc – Read-Only Memory), 7

DVD-RW (Digital Versatile Disc – Read/Write), 7

DVI (Digital Video Interface), 8

Dword (Double word), 246

E

e-mail, 402, 473
EnCase utility for searching, 442–446
exam essentials, 478

e-mail attachments, 389, 444
Base64 encoding, 449–456, 450
in Hotmail, 378

Edit menu, context sensitivity, 218

Edit “Summary of Findings” window, 288

editing EnScripts, 439

EDS. *See* EnCase Decryption Suite (EDS)

education, 475

EE. *See* EnCase Enterprise (EE)

EISA (Extended Industry Standard Architecture), 7

electronic fingerprint, 126

Email case-level tab, 225
column headings, 446

Email/Internet Search dialog box, 374, 375, 444, 473
exercise, 447–448

EMF (Microsoft Enhanced Metafile) image
format, 382, 383, 384
header search strings, 384

employee, former, as competitor, 379–380

ENBCD (EnCase Network Boot CD), 117–118, 119

ENBD (EnCase Network Boot Disk), 117–118, 119

EnCase
File Extents tab, 52, 53
optional modules, 402
options, 230–232
passwords for, 125
Safe Authentication for EnCase (SAFE), 89
“snapshot” feature, 88

EnCase Decryption Suite (EDS), 402, 456–458

EnCase Enterprise (EE), 140, 141
vs. field intelligence module (FIM), 141

- EnCase for DOS, physical and logical devices, 111
- EnCase for Windows, previewing selected device through network, 122, 122
- EnCase layout, 186–187, 187
 - adjusting panes, 220, 220–221
 - exam essentials, 236–237
 - Filter pane, 186
 - Find feature, 218, 218
 - navigation, exercise, 221–224
 - other views, 219, 220
 - separator bars in, 220, 220
 - Table pane, 186, 196–211
 - Disk tab, 206–208, 207
 - Gallery tab, 204–206, 206
 - Report tab, 204, 204
 - Table View tab, 196–203, 197
 - Timeline tab, 208–211, 209, 210
 - Tree pane, 186, 187–191
 - navigation, 191–195, 192
 - View pane, 186, 211–232
 - Console view, 214, 214
 - Details view, 215
 - Dixon box, 215–216
 - Hex view, 211, 212, 213
 - lock for, 215
 - Picture view, 213, 213
 - Report view, 214
 - Text view, 211, 212
- EnCase Network Boot CD (ENBCD), 117–118, 119
- EnCase Network Boot Disk (ENBD), 117–118, 119
- EnCE examination, practical, preparation, 94
- Encrypting File System (EFS)
 - decrypting files and folders from, 456–458
 - exam essentials, 478
- End of File (EOF), 51
- EnScript code, Code tab for, 211
- EnScript tab, in Filter pane, 219
- EnScript Types global view, 228
- EnScripts, 437–442
 - Case Initialization EnScript, 473
 - custom date format and, 231
 - exam essentials, 478
 - file mounting EnScript, 415, 416
 - filters, conditions and queries, 440–442
 - Link File Analysis EnScript, 474
 - Link File Parser EnScript, 360, 361, 362, 367
 - navigation and paths, 438–439
 - running, 440
 - Sweep Case EnScript
 - file finder for EMF, 385, 474
 - Initialize Case EnScript, 343, 440
 - Partition Finder, 406, 407
 - Recycle Bin INFO Record Finder, 354, 355
 - syntax, 442
 - Tree pane, 438
- EnScripts global view, 228
- Enterprise version of EnCase, 89
- Entries case-level tab, 225
- Entry Modified column in Table View, 201
- EOF (End of File), 51
- epoch, 338
- error granularity, 125–126
- /etc/initab file, 136
- Ethernet, 10
- evidence file, 156–175
 - components and function, 158–161
 - as duplicate of original, 175
 - exam essentials, 177
 - format when multiple evidence files are required, 159–160, 160
 - physical layout, 158
 - restoration, 465–468
 - verification, 161–167
- Evidence File column in Table View, 203
- evidence handling
 - bagging and tagging, 92–95
 - chain of custody and, 93
 - computer shutdown, 85–92
 - evidence found in plain sight, 84

514 exabyte – FAT

- recording and photographing scene, 85
 - at the scene, 78
 - securing scene, 85
 - exabyte, 245, 246
 - exam essentials
 - acquisition, 147
 - bookmarks, 299
 - compound files, 478
 - computer hardware components, 21
 - data basics, 299
 - e-mail, 478
 - EnCase layout, 236–237
 - Encrypting File System (EFS), 478
 - EnScripts, 478
 - evidence file, 177
 - FAT file system, 70
 - file signature analysis, 329
 - file systems, 70
 - forensic boot disk, 146
 - GREP searches, 299
 - hash analysis, 329
 - incident response, 95–96
 - keywords, 299
 - link files, 393
 - navigation, 236
 - partitions, 478
 - printing, 394
 - Recycle Bin, 393
 - Registry (Windows), 478
 - root user folders, 393
 - time stamp, 393
 - Excel, exporting data to, 436
 - exercises
 - bookmarks, 294–297
 - cache for web page files, 388
 - data integrity, 166–167
 - Email/Internet Search dialog box, 447–448
 - FAT file system, viewing entries, 49
 - fdisk command, recovering partitions
 - deleted with, 411–412
 - file signature analysis, 317–318
 - hard drive preview, 135
 - hash analysis, 325–327
 - Hotmail attachments, 389
 - incident response, 94
 - Internet History files recovery, 388
 - navigation, 221–224
 - partition recovery, 411–412
 - partition table, 18
 - Registry (Windows), 447–448
 - searches for data, bookmarks for results, 294–297
 - Windows artifacts recovery, 387–390
 - expansion slots, 7–8
 - explorer.exe, stopping and starting, 432–433
 - Export dialog box, 263
 - Export folder, 230
 - exporting
 - applications, 462–465
 - bookmark data, 436, 437
 - keyword lists, 263
 - report view, options, 292
 - Selection dialog box for, 455
 - \$Extend file, 67
 - extended ASCII (IBM), 252
 - Extended Industry Standard Architecture (EISA), 7
 - extended partition system, 16
 - external viewer, 228
 - sending data to, 188
-
- F**
- fan, 4
 - FastBloc, 104, 108
 - “blue square” icon, 133
 - out-of-the-box applications of, 233
 - FastBloc acquisitions, 129–135
 - FastBloc FE (Field Edition), 129
 - FastBloc LE (Lab Edition), 129
 - for drive-to-drive DOS acquisition, 114
 - FAT (file allocation table), 19, 30–31, 34–41

- FAT file system, 30–50
 - date and time stamps, 337
 - directory entry, 30
 - exam essentials, 70
 - function, 50–64
 - physical layout, 31–50, 32
 - viewing entries, exercise, 49
- FAT partitions, EnCase for DOS and, 112
- FAT12 file system, 31
 - root directory, 41, 42
 - starting cluster for partition, 44
 - volume boot sector format, 35–36
- FAT16 file system, 31
 - reserved area of FAT, 32
 - root directory, 41, 42
 - starting cluster for partition, 44
 - volume boot sector format, 35–36
- FAT32 file system, 31
 - backup boot sector, 34
 - physical layout, 42
 - reserved area of FAT, 33
 - root directory, 41
 - starting cluster for partition, 44
 - volume boot sector format, 36–38
- fault tolerance, with RAID, 6
- Favorites folder, 369–371, 370
- fdisk command, 18, 19, 137, 404
 - recovering partitions deleted with, exercise, 411–412
- FedEx tracking number, GREGP expression
 - for searches, 271
- field intelligence module (FIM), 89, 140, 143–144
 - vs. EnCase enterprise (EE), 141
 - schematic, 143
- field kit contents, 82–83
 - spare internal floppy drive, 6
- File Acquired column in Table View, 202
- file allocation table (FAT), 19, 30–31, 34–41
- File Category column in Table View, 201
- File Created column in Table View, 201
- File Deleted column in Table View, 202
- File Ext column in Table View, 201
- file extensions, 227
 - for application binding, 309
- File Extents column in Table View, 202
- File Group bookmark, 289, 290
- File Identifier column in Table View, 203
- file integrity component, in evidence file, 158
- File Mounter, EnScript options, 416
- file names, 19
- file signature analysis, 204, 473
 - conducting, 313–316
 - exam essentials, 329
 - exercise, 317–318
 - and File Type column, 316
 - and image display, 213
 - from Search dialog box, 274
- file signatures
 - bad, 315
 - creating, 310–313
- file signatures database, 310
- File Signatures global view, 227, 310, 311
- file slack, 3, 63
- File System Information (FSINFO), 32
- file systems, 19–20. *See also* FAT file system
 - CD file systems, 68–69
 - exam essentials, 70
 - mounting as read-only, 136
 - New Technology File System, 65–67
- file type code (Mac), 309
- File Type column in Table View, 201
- file types, binding to applications, 308–310
- File Types global view, 228
- File Viewers global view, 228
- files
 - deleting. *See also* deleted files; Recycle Bin management, 189
 - physical size, 51
 - undeleting, 58–62
 - user restoring from Recycle Bin, 352–353, 353
- FileSignatures.ini file, 174
- FileTypes.ini file, 174
- Filter column in Table View, 200
- Filter pane, 186, 187, 219

516 filters – GZIP files

filters, in EnScripts, 440–441
 FIM. *See* field intelligence module (FIM)
 Find feature, 218, 218
 Finder (Mac), 234
 fingerprints, on computer, 85
 firewall
 configuring for EnCase network
 connection, 120
 for servlet node, 143
 FireWire (IEEE 1394), 7
 daisy chaining of devices, 129
 first response. *See also* incident response
 hints on network connections and data
 destruction, 10
 fixed IP address, for network connection, 121
 flat ribbon cable, 130
 floppy disks
 helpful hints, 144
 icon, 192
 imaging batch, 122
 with VBR, 13
 floppy drive, 6
 FO (file offset), 217, 359
 Folder Information Bookmark, 284–286, 285
 folders
 Cookies folder, 371, 372
 creating in Linux, 137
 “dot double dot” signature for, 64, 64
 Favorites folder, 369–371, 370
 History folder, 372–376, 373
 for keywords, 256–257, 258
 My Documents folder, 368
 Send To folder, 368
 structure for cases, 189, 189
 structure for hash sets, 321
 structure for Windows 2000/XP, 363–365
 Temporary folder, 369, 369
 Temporary Internet Files folder, 376–378
 Tree pane for manipulating, 291–293
 for Windows system files, 363
 forensic boot disk, 105–106
 booting with, 107–110
 exam essentials, 146

forensic examination, order for conducting,
 472–474
 Formatting Options dialog box, 106
 formatting partition, 18
 fragmented files, 56
 recovering deleted, 59–62
 FSINFO (File System Information), 32
 Full Disk view, of physical drive with NTFS
 partition, 207
 Full Path column in Table View, 203
 Funduc shell decoder, 455, 455

G

Gallery tab, in Table pane, 204–206, 206
 Gallery view, 293
 Get Info command (Mac), 234
 Gigabit Ethernet, 10
 gigabyte, 245, 246
 global views, 226, 226–228
 keywords, 255, 256
 gloves, latex, 86
 Google searches, 87
 granularity
 of drive acquisition, 114
 error, 125–126
 of viewing panes, 186
 Greenwich Mean Time (GMT), 336, 338
 GREP searches
 exam essentials, 299
 keywords, 261, 264–268, 271–272
 for Social Security numbers, 266–267
 useful expressions, 271
 Grokster, 253
 group policy, and desktop, 367
 GUI (graphical user interface) in Linux,
 running, 136
 Guidance Software
 documentation, 458
 white paper on restoration issues, 468
 GZIP files, in cache, 444, 445

518 incident response – Korean

incident response. *See also* evidence handling

- exam essentials, 95–96
- exercise, 94
- planning and preparation, 78–84
 - computer systems, 80–82
 - field kit contents, 82–83
 - personnel, 79–80
 - physical location, 79
 - search authority, 84
- Include folder, for EnScript, 438
- index.dat file, 371
- for Internet history database file, 374
- for Temporary Internet Files, 376–377
- INFO2 file, 348, 349
 - processing by EnCase, 353–354, 354
 - viewing, 350, 350
- INFO2 Recycle Bin Recovery EnScript, 474
- INI (initialization) files, 173, 418
 - sharing, 173
- Initialize Case EnScript, 343
- inspection of computer interior, 109
- INSTALL statement, 14
- installing servlet on Windows, 142
- instant messaging, 449, 474
- integers, bookmark data types, 281
- Integrated Drive Electronics (IDE)
 - controller, 5
- intellectual property, theft, 379–380
- International Standards Organization (ISO), 68, 308
- International Telecommunications Union
 - Telecommunications Standardization Sector, 308
- Internet, browsing history, 372, 373
- Internet Explorer, Internet shortcut files
 - for, 369
- Internet History files
 - recovering, exercise, 388
 - in Windows 9x, 386
- Internet shortcut files, for Internet Explorer, 369
- Invalid Block checksum error message, 164, 165

- IO.SYS file, 14
 - EnCase modification of, 105
- IP addresses, 253
 - assigning to Linux platform, 140
- Is Deleted column in Table View, 201
- ISA (Industry Standard Architecture) expansion slot, 7
- ISO 9660 standard, 68

J

- Japanese, 254
- Jaz disk, 144
- Johnson-Grace compression, 206
- Joliet extension of ISO 9660, 68
- JPEG header, searching for, 453
- jump instruction in boot sector, 34
- jury, computer functioning explained, 2

K

- KaZaA, 253
- keyboard port, 10
- keymaster, 142
- keys in Registry, 418. *See also* Registry (Windows)
- Keyword Tester, 268, 269
 - GREP expression for UPS tracking numbers, 272
- Keyword Tester keyword search option, 263
- Keyword.ini file, 173
- keywords
 - creating and managing, 254–264, 257
 - case-level, 256
 - importing and exporting lists, 263, 264
 - exam essentials, 299
 - GREP, 264–268, 271–272
- Keywords case-level tab, 226
- Keywords global view, 227
- keywords.ini file, 255
- kilobyte, 244, 246
- Korean, 254

L

laptop computers

- hard drive from, 116

- PC Cards, 8

- shutdown procedures, 92

- Last Accessed column in Table View, 201

- Last Known Good Configuration, 16, 417

- Last Written column in Table View, 201

- latex gloves, 86

- LBA (Logical Block Addressing), 5

- LE indicator (Navigation data), 217

- left nibble, 246

- Left pane. *See* Tree pane

- legacy programs, Mac support for, 234

license

- certificate for PDE, 471

- for software, 234

LinEn (EnCase for Linux), 119

- acquisition, 135–140, 139

- at startup, 138

- Link File Analysis EnScript, 474

- Link File Parser dialog box, 362

- Link File Parser EnScript, 360, 361, 362, 367

link files, 357–363

- contents, 359

- exam essentials, 393

- file header, 360

- Properties dialog box, Shortcut tab, 357

- in Recent folder, 366–367

- and theft detection, 379–380

Linux

- assigning IP address to platform, 140

- header information for binding file types, 309

- installing servlet, 142

- Native partitions, 18

- shutdown procedures, 91

- Linux EnCase (LinEn), 104

- “live” physical device, in Tree pane, 192

- .lnk file extension, 357

- local area connections, properties, 121

- Local time option, in EnCase, 339

lock

- for column in Table View tab, 196, 197

- for View pane, 215

- log of case information, 472

- \$LogFile file, 66

- Logical Block Addressing (LBA), 5

- logical devices, in EnCase for DOS, 111

- Logical Disk Manager, 469

- Logical evidence file, 122

- logical OR (pipe) expressions, 268

- Logical Size column in Table View, 202

- long file names, 44–45

- storage scheme, 45–46

- Lotus Date bookmark data type, 282

- Lotus Notes, 463

- welcome screen, 465

- Low ASCII bookmark data type, 281

- low-bit ASCII, 449

- lowercase letters in ASCII, 253

- LS indicator (Navigation data), 217

M

- MAC (Media Access Control) address, 10

- MAC (Media Access Control) times, 337

- for link files, 359, 361

- Macintosh, 233–234

- binding files to applications, 309–310

- BinHex encoding, 450

- hard drive acquisition, 116

- HFS format, 69

- OS X partitions, 18

- shutdown procedures, 91

- macro-focusing for photographs, 88

- magnets, 94

- mail clients, determining type, 442

- .MailDB file extension, 414

- mainboard, 4

- man command, 137

- master boot record (MBR), 13, 13, 14, 403, 405

520 master evidence file – Notes bookmark

master evidence file, 94
master file table in NTFS, 19
master/slave IDE devices, 5–6
master-to-master data transfer, 110
MBR (master boot record), 13
.mbx file extension, 414
MCA (IBM Micro Channel Architecture), 7
MD5 hash, 126, 157, 158, 308, 318, 319
 in drive-to-drive DOS acquisition, 113
megabyte, 245, 246
metadata, 19
\$MFT (master file table) file, 65–66
\$MFTMirr file, 66
microprocessor, 4
Microsoft Encrypting File System (EFS),
 decrypting files and folders from,
 456–458
MIME (Multipurpose Internet Mail
 Extensions Standard), 450
mkdir command, 137, 138
modem, 10
molex power connector, 4
motherboard, 4
Mount As Emulated Disk dialog box,
 469, 470
Mount As Network Share dialog box,
 461, 461
mounting
 file systems as read-only, 136
 files, 412–415
 Registry hive file, 423
mouse port, 10
moving
 columns in Table View tab, 200
 EnScripts, 439
 keyword folder, 257
MS-DOS
 configuration settings, 417
 time stamp, 347
MSDOS.SYS, 14
.msi file extension, 414
multiple monitors, 221

Multipurpose Internet Mail Extensions
 (MIME) Standard, 450
My Documents folder, 368
 in Windows 9x, 386

N

Name column in Table View, 200
names
 of bookmarked files for Web Page report
 format, 297
 for case folder, 189–190, 190
 for devices, 132
 for evidence files, changing, 173
 for files in Recycle Bin, 348
 for multiple evidence file, 160
 for Windows system files, 363
National Software Reference Library
 (NSRL) hash sets, 322
Navigation Data (GPS), 216, 217–218, 218
navigation, exam essentials, 236
Nero, for burning CD image, 118
nesting subpartitions, 16
netstat.exe command, 89
network cable
 crossover, 117
 for hard drive acquisition, 116–128
network connections
 and data destruction, 10
 disconnecting, 89
network interface card (NIC), 10, 117
network share, for INI file, 173
New File Signature dialog box, 310, 311
New Keyword dialog box, 257, 259, 260
New Technology File System, 65–67
NextPart string, 453
nibble, 243
NIC (network interface card), 10, 117
 drivers, 120
nonvolatile memory, 3
Notable File bookmark, 286–289
Notes bookmark, 168, 283, 284, 290

NTDETECT.COM, 15
NTFS (New Technology File System), 65–67
 date and time stamps, 337
NTFS partition, 65
 EnCase for DOS and, 112
 recovering, 67
NTFS5, 65
NTLDR file, 15
NTOSKRNL.EXE, 16
ntuser.dat file, 309, 364, 423
numbers, as integers, 253
NVRAM (nonvolatile random access memory), 3

O

objects, selected, 194
opening
 backup file (cbak), 172, 172
 CD/DVD drive, with paperclip, 109
operating system. *See also* Linux;
 Macintosh; Unix; Windows
 artifacts, 336
 and computer shutdown, 89
Options dialog box, 123
 Case Options tab, 230
 Colors tab, 232, 232
 Fonts tab, 232
 Global tab, 171, 205, 231
 Storage Paths tab, 174, 232
OR (pipe) expressions, logical, 268
organizing bookmarks, 291–293
Original Path column in Table View, 203
Outlook, 378
 search for PST data in unallocated
 clusters, 416
output from EnScripts, Console view for,
 214, 214
Output Path, 127
“overwritten file,” 62

P

packet writing, 69
pagefile.sys (swap) file, 362–363. *See also*
 swap (pagefile.sys) file
pager, 449
parallel cable, for computer connections, 120
parallel port, 11
parent directory (FAT), 43
 directory entry (FAT) pointing to, 64
 directory entry pointing to, 64
parity bit, 252
Partition Entry bookmark data type, 282
partition table, 403, 403
 for deleted partitions, 405
 exercise, 18
 field definitions, 17
partitions, 16–19
 exam essentials, 478
 locating and mounting, 403–410
 NTFS, 65
 recovering, 19, 409–410, 410
 exercise, 411–412
 passwords
 automatic recovery, 457
 bypassing BIOS access passwords, 9
 in drive-to-drive DOS acquisition, 113
 for EnCase, 125
 for Lotus Notes, 463
 Windows storage of, 457–458, 458
path, for EnScripts, 439, 439
PC Cards, 8
PCI (Peripheral Component Interconnect), 7
PCI Express, 8
PCMCIA (Personal Computer Memory
 Card International Association), 8
PDE. *See* Physical Disk Emulator (PDE)
peer-to-peer file sharing, 474
perimeter control, 85
period (.), in GREP expression, 268
Peripheral Component Interconnect (PCI), 7
Permission Denied error, 138

522 Permissions column in Table View – Recycle Bin

Permissions column in Table View, 202
 personnel, at the scene, 79–80
 PGPdisk, 88
 photographs
 of scene, 85
 for “state” of computer system, 88
 physical devices, in EnCase for
 DOS, 111
 Physical Disk Emulator (PDE), 402,
 468–472, 473
 Physical Location column in Table
 View, 202
 Physical Sector column in Table
 View, 203
 Physical Size column in Table
 View, 202
 pictographs, Unicode characters
 for, 254
 picture, Base64 encoding, 452
 Picture bookmark data type, 281
 Picture view, in View pane, 213, 213
 pinned area, of program list, 426
 pipe (logical OR) expressions, 268
 platters in hard drive, 4
 plus sign (+), in Tree pane, 193, 193
 POST (Power On Self-Test), 12
 power supply, 3–4
 .ppt file extension, 414
 Preview Device window, 132, 132
 primary IDE controller, 5
 print job, 474
 recovering, 390
 print spooling, 382–385, 383
 printing, exam essentials, 394
 program counter, 12
 programs. *See* applications
 progress bar, for file verification, 161
 PS indicator (Navigation data), 217
 PS2 connection, for mouse, 10
 .pst file extension, 414
 pulling plug for shutdown, 92

Q

Quad word, 246
 queries
 with e-mail filters, 443
 in EnScripts, 441
 Queries tab, in Filter pane, 219
 Quick Reacquisition feature, 126–127
 Qword, 246

R

RAID (Redundant Array of Inexpensive
 Disks), 6, 116
 in Tree pane, 193, 193
 RAM (random access memory), 3
 RAM slack, 63
 RAW mode, for printer definition, 382
 Read Ahead, 127
 read-only memory (ROM), 3
 read-only, mounting file systems as, 136
 reading file, actions occurring for, 50–51
 Real-Time Clock (RTC), 8
 Recent folder, 366, 366–367
 in Windows 9x, 386
 Reconstructed HTML bookmark data type,
 281
 recording the scene, 85
 Recover Folders feature, 410
 recovering
 dead hard drive, 115
 encrypted data, 88
 files, 58–62
 partitions, 19, 409–410, 410
 exercise, 411–412
 Recycle Bin, 347–357
 bypassing, 355
 comparison by Windows version, 349
 deleting files, 353
 exam essentials, 393
 restoring files from, 352–353, 353

- Recycle Bin properties dialog box, 355, 356
- red characters, in EnCase, 63, 63
- Red Hat, manually mounting file system, 136
- References column in Table View, 202
- regedit.exe, 418, 426
 - refreshing contents, 433
- regedt32.exe, 418
- Registry (Windows), 417–437
 - application binding information in, 309
 - desktop objects defined in, 367
 - Dword in, 246
 - EnCase to mount and view, 423–424
 - exam essentials, 478
 - exercise, 447–448
 - history, 417–418
 - HKEY_CLASSES_ROOT, 419
 - HKEY_CURRENT_CONFIG, 419
 - HKEY_CURRENT_USER, 419, 423
 - \Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist, 426
 - HKEY_LOCAL_MACHINE, 419
 - hive keys, 420
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BitBucket, 355–356, 356
 - \Print\Printers\DefaultSpool Directory, 382
 - HKEY_USERS, 419, 420–421
- monitoring reads and writes, 429–430, 430
- navigating, 421
- organization and terminology, 418–423
- research techniques, 425–437
- root keys, 419
- time zone offset in, 342
- usernames and passwords recovered from, 458
- user's hive, 364
- value data types, 422–423
- Registry editor, 418, 418, 422
- Registry (Windows), Dword in, 246
- regmon utility, 429–430, 430, 433
 - writes to UserAssist key, 435, 435
- repair folder, 424
- Report tab, in Table pane, 204, 204
- report view
 - of bookmark folder structure for USB device, 285
 - of bookmark from Link File Parser EnScript, 362
 - for device with corrupted data, 163–164, 164
 - for devices, 162
 - export options, 292
 - Internet history bookmark entries, 376
 - of notable file bookmark, 287
 - after changes, 288
 - of Notes bookmark layout, 284
 - in View pane, 214
- reports
 - bookmarks as foundation, 279
 - Web Page format for, 292–293, 293
- reserved area of FAT, 31
 - for FAT16 system, 32
 - for FAT32 system, 33
- resident data, 66
- resource fork (Macintosh), 450
- response to incident. *See* incident response
- restoration of evidence file, 402, 465–468
- Restore dialog box, 466
- restore point, for Registry, 417
- restoring files, from Recycle Bin, 352–353, 353
- reverification feature, 163, 163
- right nibble, 246
- Right pane. *See* Table pane
- roaming profiles, 365
- Rock Ridge extension, 69
- ROM (read-only memory), 3
- root directory in FAT, 41
- root user folders, 363–364, 364, 365, 473
 - exam essentials, 393
- ROT-13 bookmark data type, 281

524 ROT-13 encoding – .SHD file extension

ROT-13 encoding, 426, 436
 decoding, 428
 Roxio, for burning CD image, 69, 118
 RS-232 connection, 11
 RSA (Rivest, Shamir and Adleman)
 algorithm, 126
 RTC/NVRAM, 8
 boot order setting, 9
 system date and time setting, 9
 RTC (Real-Time Clock), 8
 RTL Reading keyword search option, 262
 Run command, for Registry editor, 418

S

SAFE (Safe Authentication for EnCase),
 89, 142
 safety, in incident response, 79, 85
 SATA (Serial Advanced Technology
 Attachment) controller, 6
 saving configuration files, 175
 Scan Registry EnScript, 474
 scientific calculator, Windows 64-bit time
 stamp in, 341
 screen display. *See* EnCase layout
 screen shots, for timeline, 211
 SCSI (Small Computer Systems Interface), 5
 drivers, 120
 imaging drive, 116
 seal, for evidence file component, 158
 search-and-seizure specialist, 85
 search authority, 84
 and hash sets, 323
 Search dialog box, 273
 and file hashing, 319, 320
 for file signature analysis, 314
 options, 274–275
 “Search Only Slack Area of Files in Hash
 Library,” 323
 Search hits, color for, 232
 Search Hits view, 225, 275, 276
 Table pane, right-click menu options,
 277–278
 search summary bookmark, 291
 search warrants, 84
 terminology in, 11
 searches for data, 254–297
 bookmarks for results, exercise, 294–297
 compound files, 415
 GREP keywords, 264–268, 271–272
 hash analysis and, 322–325
 keyword creation and management,
 254–264, 257
 starting, 272–275
 viewing hits, 275–278
 secondary IDE controller, 5
 sector slack, 63
 sectors, 4
 determining visibility of all, 108, 110
 \$Secure file, 66
 Secure Storage case-level tab, 226
 securing scene, 79, 85
 Security Accounts Manager (SAM) Registry
 file, 351
 Security ID global view, 228
 security ID (SID), for tracking deleted files,
 351, 352
 SecurityIDs.ini file, 174
 selected files, 223
 sorting, 199
 viewing, 216
 selected objects, 194
 Selection dialog box, for exporting data, 455
 Send To folder, 368
 separator bars, in EnCase layout, 220, 220
 Serial Advanced Technology Attachment
 (SATA) controller, 6
 serial port, 11
 for mouse, 10
 servers, shutdown procedures, 92
 servlet node, 142
 “Set Included Folders” trigger, 195, 195,
 196, 216, 259
 Setup routine, entering, 109
 shadow file, for print job, 382, 383
 .SHD file extension, for print job, 382, 383

- SHELL statement, 14
- Short Name column in Table View, 203
- shortcuts. *See* link files
- Show Columns dialog box, 200
- shutting down computers, 85–92
- Signature column in Table View, 201
- slack space, 63
- Small Computer Systems Interface (SCSI), 5
- Snapshot feature, 88, 141
- SO indicator (Navigation data), 217
- Social Security numbers, GREP search for, 266–267
- software. *See* applications
- Solaris partitions, 18
- sorting columns in Table View tab, 197–199, 198, 223
- sound card, 8
- sound codec (Compression/Decompression Module) chip, 8
- source drive, for evidence files, 160
- spanning drives during acquisition, 160–161
- special master situations, 113
- speed of acquisition over network, 128
- .SPL file extension, for print job, 382, 383
- spool file, for print job, 382, 383
- spooling, 382–385, 383
- spyware/Trojan scan, 461
- “stand-offs,” 4
- StandardBias TimeZoneInformation key value, 343
- StandardName TimeZoneInformation key value, 343
- StandardStart TimeZoneInformation key value, 343
- Start menu (Windows), 427
- Control Panel
 - Network Connections, 121
 - Windows Firewall, 120, 121
 - My Recent Documents, 366, 366
- start sector, for reacquisition, 127
- Starting Extent column in Table View, 202
- startup disk, converting to forensic boot floppy, 105
- startx command, 136
- “state” of computer system, photographs to record, 88
- status byte, 57, 63–64
- stop sector, for reacquisition, 127
- storage drive. *See* drives; hard drive
- subnet mask, for network connection, 121
- SubSeven, 319
- Trojan, 429
- SuSE, manually mounting file system, 136
- swap (pagefile.sys) file, 3, 362–363, 380, 381
- in Windows 9x, 386
- Swap partitions, 18
- Sweep Case EnScript
- file finder for EMF, 385, 474
 - Initialize Case EnScript, 343, 440
 - Partition Finder, 406, 407
 - Recycle Bin INFO Record Finder, 354, 355
 - Scan Registry module, 436
- sweeping bookmark, 279
- Symantec, PartitionMagic, 18
- Symbolic Link column in Table View, 203
- SYSINIT, 14
- SysInternals web site, 429–430
- system administrators, assistance from, 79–80
- system date and time setting, in RTC/NVRAM, 9
- system folders, in Windows, 364

T

- Table pane, 186, 187
- Disk tab, 206–208, 207
 - Gallery tab, 204–206, 206
 - navigation, 196–211
 - Report tab, 204, 204
 - Table View tab, 197
 - Timeline tab, 208–211, 209, 210, 223
- Table View tab, in Table pane, 197

526 tagging evidence – US Postal Service Express Mail tracking number

tagging evidence, 92–95, 157
 .tar file extension, 415
 target drive, wiping, 466, 467
 Task Manager
 New Task function, 433
 Processes tab, 432, 432
 telephone, modem for connection, 10
 template, for case folder structure, 189, 189
 temporary files, as compound files, 413
 Temporary folder, 188, 230, 369, 369
 Temporary Internet Files folder, 376–378
 terabyte, 245, 246
 terminology, 175
 in search warrants, 11
 testing, by POST, 12
 text fragment bookmark, 279
 text messaging, 449
 Text Styles bookmark data type, 282
 Text Styles feature in EnCase, 46, 47, 49
 Text Styles global view, 227
 Text Styles tab, in Filter pane, 219
 Text view, in View pane, 211, 212
 TextStyles.ini file, 173
 threats to safety, 79
 Thumbs.db file, 414
 time for system, 473
 user alteration, 434–435
 Time Properties dialog box, 345, 346
 time zones, 337–338
 adjustments for offsets, 342–347
 Timeline tab, in Table pane, 208–211, 209, 210
 timeout period, before caching invalid image, 205, 205
 Token Ring, 10
 Tools menu, > Create Boot Disk, 105, 105–106, 106
 tracks, 4–5
 training, 475
 transporting computer evidence, 94
 Tree pane, 186, 187, 222
 dragging keywords to folder, 263
 folder manipulation, 291–293
 navigation, 191–195, 192, 229

“Trojan Defense,” 88
 TWAIN, 2

U

UDF (Universal Disk Format), 69
 unallocated clusters, 3
 search for PST data in, 416
 in Virtual File System, 471
 undeleting files, 58–62
 Unicode bookmark data type, 281
 Unicode characters, 253–254, 254
 for swap file, 380
 Unicode keyword search option, 262
 uninterrupted power supplies (UPS), 82
 Unique Name column in Table View, 203
 Universal Disk Format (UDF), 69
 Universal Time, 336
 Unix
 hard drive acquisition, 116
 header information for binding file types, 309
 installing servlet, 142
 shutdown procedures, 91
 time stamp, 338–339
 Unix Date bookmark data type, 282
 Unix Text Date bookmark data type, 282
 unlocking storage drive, 113
 unmounting mounted file, 413
 “Unused Disk Area,” physical device with, 133
 \$UpCase file, 67
 uppercase letters in ASCII, 253
 UPS tracking numbers, GREP expression in Keyword Tester, 272
 for searches, 270, 271
 UPS (uninterrupted power supplies), 82
 URL address, GREP expression for searches, 271
 .url file extension, 369
 US Postal Service Express Mail tracking number, GREP expression for searches, 271

USB controller, 7
 USB flash media, helpful hints, 144
 USB port, 7
 for mouse, 10
 USB thumb drive, viewing FAT entries, 49
 User Assist Area in Start Menu, 427
 user profile folders, in Windows, 364
 user profiles, roaming, 365
 UserAssist, 474
 after removal of keys, 432
 date timestamp for value, 435
 NoLog, 437
 Settings, 431, 431
 value attributes decoded, 434
 UserAssist key, 426
 UTF-7 keyword search option, 262
 UTF-8 keyword search option, 262
 UUE Encoded Picture bookmark data
 type, 281
 uuencoding, 450

V

V-Communications, Partition
 Commander, 18
 VBM (volume bit map), 19
 VBR (volume boot record), 13, 13, 404, 404
 for partition recovery, 19
 Verification Hash, 128
 verification hash value, 162
 verification, of evidence file, 161–167
 Verify File Integrity function, 169
 VESA Local Bus (VL-Bus), 7
 VFS. *See* Virtual File System (VFS)
 VGA (video graphics array), 8
 video card, 8
 View pane, 186, 187, 211–232
 Console view, 214, 214
 Details view, 215
 Dixon box, 215–216
 Hex view, 211, 212, 213
 lock for, 215

 Picture view, 213, 213
 Report view, 214
 Text view, 211, 212
 View Search Hits dialog box, 276
 viewer, sending data to external, 188
 Viewers.ini file, 174
 views, global, 226, 226–228
 Virtual File System (VFS), 402, 458–461, 459, 473
 vs. Physical Disk Emulator, 471–472
 stopping, 462
 virus scan, 461
 visibility of sectors, determining, 108, 110
 VL-Bus (VESA Local Bus), 7
 VMWare, 470, 474
 volatile system-state data, capturing, 140
 volatility of RAM, 3
 and data loss in shutdown, 88
 volume bit map (VBM), 19
 volume boot record (VBR), 13, 13, 33–34, 404, 404
 NTFS storage of backup, 65
 for partition recovery, 19
 volume boot sector, 31, 32
 format
 for FAT12/16 file system, 35–36
 for FAT32 file system, 36–38
 \$Volume file, 66
 volumes, 16
 hashing, 167–169

W

web cache, 444, 474
 Web Cache case-level tab, 225
 web mail addresses, GREP searches for, 268
 Web Page format
 bookmarked file names for, 297
 for reports, 292–293, 293
 Wilson, Craig, 371
 windows. *See* EnCase layout

528 Windows – Zulu Time

Windows. *See also* Recycle Bin; Registry (Windows)

artifacts recovery, exercise, 387–390

bookmark data types, 282

dates and times, 336–347

64-bit time stamp, 338, 338–341, 340

time zone adjustments for offsets, 342–347

time zones, 337–338

forensic boot disk for, 105

installing servlet, 142

passwords storage by, 457–458, 458

in View pane, 211–232

Windows 3.1, shutdown procedures, 90

Windows 9x/Me

artifacts, 386

disk caching, 134

shutdown procedures, 90

Windows 95 Info File Record bookmark

data type, 282

Windows 2000 Info File Record bookmark

data type, 282

Windows Date/Time bookmark data

type, 282

Windows firewall, options, 120, 121

Windows Initialize Case dialog box, 344

Windows NT/2000/XP

boot process in, 15–16

directory structure, 363–365

OEM version, default favorites, 370

partitions, 17–18

Recycle Bin, 352

root user folders, 363–364, 364, 365

shutdown procedures, 90

support for AOL .art files, 206

WINNT folder, 363

wiping hard drive, 67, 466, 467

wireless NIC cards, 10

wires, on molex power connector, 4

word, 246

write-blocking device, FastBloc as, 129

writing files, in FAT system, 54–56

X

.xls file extension, 414, 436, 437

xxencoding, 450

Y

“yellow” crossover cable, 117

Z

zip disk, 144

.zip file extension, 414, 415

Base64 attachment, 451

Zoned-Bit Recording (ZBR), 5

Zulu Time, 336





























