

# Index

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

---

## Numbers

3-D graphics, 8  
64-bit date and time stamp, Windows OSs,  
382–386, 383, 385

---

## A

Accelerated Graphics Port (AGP), 8  
access control lists (ACLs), 21  
ACLs (access control lists), 21  
acquisition hashes, MD5, 180  
ActiveTimeBias, time zones, 388  
adapters, checklist for field kit, 87  
Add Partition dialog, 474  
Advanced Technology Attachment  
(ATA), 5  
advanced topics  
  Base64 encoding, 524–530  
  EDS (EnCase Decryption Suite),  
  530–534  
  email. *See* email  
  EnScript. *See* EnScript  
  exam essentials, 555  
  exercise in partition recovery,  
  478–480  
  exporting applications, 539–542,  
  540–541  
  mounting files, 480–486, 481, 485  
  mounting partitions, 471–478  
  overview of, 470  
  PDE (Physical Disk Emulator),  
  545–549, 546–547  
  registry. *See* registry  
  restoration, 542–545, 543–545  
  review questions, 556–561  
  summary, 552–554  
  VFS (Virtual File System), 535–538,  
  535–539  
AGP (Accelerated Graphics Port), 8

algorithms  
  CRC, 179  
  MD5. *See* MD5 (Message Digest 5)  
aliases  
  file signature analysis and, 357, 357  
  Windows OSs and, 47  
All Users folder, Windows OSs, 418  
allocation units, file system data units, 21  
America Online (AOL), 233  
American Standard Code for Information  
  Interchange. *See* ASCII (American  
  Standard Code for Information  
  Interchange)  
anchors, HTML, 572  
antistatic packing materials, 99  
AOL (America Online), 233  
app descriptors, global views, 257  
application binding  
  file extensions and, 485  
  overview of, 350–352  
applications  
  exporting as means of examining,  
  539–542, 540–541  
  restoration as means of examining,  
  542–545  
archive files, global views, 257  
ART files, 233  
artifacts, 380. *See also* Windows OS artifacts  
ASCII (American Standard Code for  
  Information Interchange)  
  ASCII table, 285  
  low-bit ASCII, 524  
  overview of, 284–286  
ATA (Advanced Technology Attachment), 5  
attachments, email. *See* Base64 encoding  
ATX form factor motherboard, 4  
auditing levels, event logs, 446–449  
authentication, SAFE (Secure  
  Authentication for EnCase), 163  
AUTOEXEC.BAT, in DOS boot process, 15  
automatic backup, 194–195

**B**

- backup boot sector, FAT32, 35
- backup files (.cbak), EnCase, 193–197
  - modifying automatic backup, 194–195
  - opening, 195–196, 196
  - overview of, 193
- backups, case files, 192–193, 193
- bad file signature, 357
- bagging evidence, 98–100
- bar code scanner, checklist for field kit, 88
- Base16, 281
- Base2, 276–277
- Base64 encoding
  - compared with other encoding methods, 524–525
  - overview of, 526–530
  - ZIP file and, 526, 526
- Basic Input Output System (BIOS)
  - dates and times and, 381
  - overview of, 9
- BCD (Boot Configuration Data), 17
- BestCrypt, 93
- big endian, 46
- binary numbers
  - Base2 and, 276–277
  - bits and nibbles, 275
  - bytes and Dwords, 278–279
  - evaluating, 280–281
  - number of outcomes for 1 to 4 bits, 275
- BinHex encoding, 525
- BIOS (Basic Input Output System)
  - dates and times and, 381
  - overview of, 9
- bit flag values, FAT directories, 45–47
- \$Bitmap, in NTFS, 68
- bits
  - as smallest unit of binary numbers, 275
  - table of properties, 279
- block size, network acquisition and, 133
- blocks, file system data units, 21
- Bookmark Data dialog, 314, 471
- Bookmark Files dialog, 321
- bookmarks
  - case-level views, 254
  - data types, 315–317
  - exercise searching and bookmarking, 330–333
  - file group bookmarks, 324–325, 325
  - folder information bookmarks, 318–321, 320
  - folder structure and, 322, 565, 565
  - hash analysis reports, 362, 362
  - Highlighted Data bookmarks, 313–315, 314
  - INFO2 file, 395–396
  - notable file bookmarks, 321–324
  - notes bookmarks, 317–318, 318–319
  - organizing and creating reports, 327–329
  - other bookmarks, 325–327
  - overview of, 313
  - paperless reports, 572–575
  - report view, 324
  - time zones, 389, 389
- Boot Configuration Data (BCD), 17
- boot disks
  - booting with DOS boot disk, 115–116
  - booting with EnCase boot disk, 113
  - creating forensic boot disks, 111–113
  - floppy and CD formats, 110
  - preparing EnCase network boot disk, 125
  - updating Linux boot CD, 155–156, 155–156
- boot indicator type, MBR, 14
- boot order, RTC/NVRAM settings, 10
- boot process, 16
  - booting with DOS boot disk, 15, 115–116
  - booting with EnCase boot disk, 113
  - exam essentials, 23
  - network acquisition, 127
  - steps in, 12–15
  - Windows NT/2000/XP, 15, 17
  - Windows Vista, 17
- boot sectors. *See* reserved area (boot sector)
- BOOT.INI, in Windows NT/2000/XP boot process, 15

BOOTMGR, in Windows Vista boot process, 17  
 bootstrap. *See* boot process  
 bytes  
   consisting of 8 bits, 278–279  
   table of properties, 279

## C

C++, EnScript and, 509  
 Cable Select (CS) method, of master/slave assignment, 6  
 cables  
   checklist for field kit, 87  
   network cables, 124–125  
 cache folder, EnCase, 199–201  
 CAD (computer assisted dispatch), 83  
 case, computer, 3  
 case files  
   backups, 193  
   folder structure for, 192  
   overview of, 191–193  
 case-level views, 253, 253–255, 258, 290  
 Case options dialog, 212, 212–213  
 Case Processor, EnScript  
   Link File Parser, 411  
   Sweep Case renamed as, 513  
   Windows Event Log Parser, 450  
 case sensitivity, in keyword searches, 291–292, 292  
 Case view, 211–216  
 cases  
   adding evidence to, 216  
   creating, 211–215, 213  
   global views, 255–258  
 Cases view, Clear Invalid Image Cache, 233, 233  
 .cbak. *See* backup files (.cbak), EnCase  
 CD file systems, 70–72  
 CD Inspector, 72  
 CD-ROM (Compact Disc-Read-Only Memory), 7  
 CD-RW (Compact Disc-Read/Write), 7  
 CDs  
   burning reports to, 575–577, 576  
   checklist for field kit, 87  
   imaging, 165  
   preparing EnCase network boot CD, 126  
 central processing unit. *See* CPU (central processing unit)  
 chain of custody, 99  
 Change Icon dialog box, 407  
 characters  
   ASCII, 284–286  
   overview of, 284  
   Unicode, 286–287, 287  
 Choose Devices dialog, 543  
 CHS (Cylinder, Head, Sector), hard drive geometry, 4–5  
 Clear Invalid Image Cache, Cases view, 233, 233  
 clusters  
   FAT, 32–33  
   FAT1 and FAT2 and, 41–43, 42  
   file system data units, 21  
 CMOS battery, 9  
 CMOS chip. *See* RTC/NVRAM  
 CMOS (Complementary Metal-Oxide Semiconductor), 9  
 Code view, Table pane, 238  
 colors, options for customizing, 261, 261  
 column headings, email, 518–519  
 columns, in Table pane  
   hash analysis and, 366, 366  
   locking, 222–223, 222–223  
   naming, 226–230  
   showing hidden, 226, 226  
   sorting, 223–225, 224  
 COMMAND.COM  
   creating EnCase forensic boot disks and, 111, 111  
   in DOS boot process, 15  
 Compact Disc-Read-Only Memory (CD-ROM), 7  
 Compact Disc-Read/Write (CD/RW), 7  
 Complementary Metal-Oxide Semiconductor (CMOS), 9  
 compound files, mounting, 481–482  
 compression  
   of evidence files, 181  
   Johnson-Grace compression, 233  
   network acquisition and, 133

## 594 Compute Hash Value – data

Compute Hash Value, Search dialog box, 361, 361–362  
 computer assisted dispatch (CAD), 83  
 computer shutdown procedures, 94–98  
   DOS, 95  
   Linux/Unix, 96–97  
   Macintosh, 97, 97  
   pulling the plug, 98  
   Windows OSs, 94–96  
 computer systems  
   imaging live systems, 93–94  
   imaging systems for capturing evidence, 87  
   incident response based on types of computer systems being investigated, 84–86  
   list of steps in computer forensics, 549–552  
   seizing computer evidence (physical), 90–92  
 conditions, EnScript, 513–514, 514  
 CONFIG.SYS, 15  
 configuration files, EnCase, 197–199  
   overview of, 197  
   primary INI files, 197–198  
   storage paths for, 198–199  
 configuration files, MS-DOS, 487  
 consent to search, 88  
 Console view, View pane, 240–241, 241  
 Container Report, creating, 568–572  
 contamination, preventing contamination of evidence, 90–91  
 Cookies folder, Windows OSs, 425–426, 425–426  
 CookieView, 426  
 cooling computers, 4  
 copies, of evidence, 110  
 Copy Folder dialog, 540  
 CPU (central processing unit)  
   boot process and, 12–13  
   case compared with, 3  
   overview of, 4  
 CRC (Cyclical Redundancy Check)  
   evidence files and, 180–183  
   file integrity and, 179  
   file verification and, 180–183  
   hash collisions and, 185  
   verifying file integrity, 183–188

Create Hash Set dialog, 362  
 Create Shortcut Wizard, 408  
 creator codes, Macintosh computers, 351  
 CS (Cable Select) method, of master/slave assignment, 6  
 CSEL, 6  
 Cyclical Redundancy Check. *See* CRC (Cyclical Redundancy Check)  
 Cylinder, Head, Sector (CHS), hard drive geometry, 4–5

## D

data  
   adding keyword lists, 297  
   ASCII, 284–286  
   binary, 275–281  
   bookmark data types, 315–317  
   characters, 284  
   creating keywords, 289–294  
   exam essentials, 341–342  
   exercise maintaining integrity of, 188–190  
   exercise searching and bookmarking, 330–333  
   file group bookmarks, 324–325, 325  
   folder information bookmarks, 318–321, 320  
   GREP searches. *See* GREP searches  
   hexadecimal, 281–284  
   Highlighted Data bookmarks, 313–315, 314  
   importing/exporting keywords, 295–296  
   indexed searches, 333–339, 333–339  
   keyword searches, 287–289  
   managing keyword folders, 294–295  
   notable file bookmarks, 321–324  
   notes bookmarks, 317–318, 318–319  
   organizing bookmarks and creating reports, 327–329  
   other bookmarks, 325–327  
   overview of, 274–275  
   review questions, 343–348  
   starting searches, 306, 306–309  
   summary, 340–341

- Unicode, 286–287, 287
  - viewing search hits, 309–313
- data area, FAT, 43–48
- Data Link Layer (DLL), 11
- data types
  - bookmark, 315–317
  - registry, 492
- Date and Time Properties dialog, Windows OS, 382
- date and time stamps, Timeline view, 237, 237
- date and time, Windows OSs
  - 64-bit time stamp, 382–386, 383
  - overview of, 380–381
  - time zone offsets, 386–392
  - time zones, 381–382
- dates, options for customizing, 260
- DCO (Device Configuration Overlay)
  - FastBloc SE support, 146
  - network acquisition and, 123
  - viewing invisible data, 114
- dd command, Unix, 178
- decimal values, hex values corresponding to, 281–282
- decryption. *See* encryption
- Default Export folder, 212
- deleting/undeleting files, FAT, 59–64
- Desktop folder, Windows OSs, 418–419, 418–419
- Desktop Icon Settings dialog box, 419
- Details view, View pane, 242
- Device Configuration Overlay (DCO)
  - FastBloc SE support, 146
  - network acquisition and, 123
  - viewing invisible data, 114
- device drivers, 17
- devices, case-level views, 254
- digital cameras, checklist for field kit, 86
- digital evidence, acquiring, 110–176
  - booting with DOS boot disk, 115–116
  - booting with EnCase boot disk, 113
  - creating forensic boot disks, 111–113, 111–113
  - drive-to-drive DOS acquisition, 116–122
  - Enterprise and FIM acquisitions, 161–165
  - exam essentials, 168–169
  - exercise previewing own hard drive, 145–146
  - FastBloc acquisition. *See* FastBloc acquisition
  - HPA and DCO data, 114
  - LinEn acquisition. *See* LinEn acquisition
  - network acquisition
    - network acquisition
  - overview of, 110–111
  - review questions, 170–176
  - summary, 166–167
  - tips/hints for various devices, 165
- digital evidence, capturing volatile, 92–94
- Digital evidence search-and-seizure specialist, on search team, 90
- Digital Versatile Disc-Read-Only Memory (DVD-ROM), 7
- Digital Versatile Disc- Read/Write (DVD-RW), 7
- Digital Video Interface (DVI), 8
- Direct ATA mode, 114, 118
- directories
  - directory entries, 45–48
    - location of root directory, 43–44
    - Windows OSs, 412
  - directory entries
    - dot double dot directory
      - signature, 66
    - function and structure of, 45–48
    - overview of, 32
    - reading files, 53–55, 53–56
    - status bytes, 66–67
    - table of, 57
    - viewing using EnCase, 48–50, 48–52
    - writing files, 56
- Disk Manager, 19
- Disk view, Table pane, 234–235, 234–235
- DISKPART, 19
- disks, hashing, 190–191, 190–191
- Dixon box
  - cumulative count of selected objects in, 219–220, 220
  - overview of, 242–243
- DLL (Data Link Layer), 11

Doc view, View pane, 241, 241  
 documentation manuals, for EnCase  
 module, 533  
 Documents folder, Windows Vista, 419  
 DOS. *See also* MS-DOS  
 boot process, 15  
 booting with DOS boot disk,  
 115–116  
 computer shutdown procedures, 95  
 dates and times and, 381  
 drive-to-drive DOS acquisition,  
 116–122  
 naming conventions, 45  
 time stamp, 391  
 dot double dot directory signature, 66  
 Drive dialog, 544  
 drive-to-drive DOS acquisition,  
 116–122  
 overview of, 116–117  
 steps in, 117–121, 118–119  
 supplemental information about,  
 121–122  
 DRIVER.CAB file, 17  
 DVD-ROM (Digital Versatile  
 Disc-Read-Only Memory), 7  
 DVD-RW (Digital Versatile Disc-  
 Read/Write), 7  
 DVDs, burning reports to, 575–577  
 DVDs, imaging, 165  
 DVI (Digital Video Interface), 8  
 Dwords, 278–279  
 measurement unit consisting of  
 4 bytes, 278  
 table of properties, 279

---

## E

EDS (EnCase Decryption Suite), 530–534,  
 531–533  
 EE (EnCase Enterprise)  
 digital acquisition, 161–164  
 imaging live systems, 93–94  
 schematic of, 162  
 EFI (Extensible Firmware Interface),  
 9–10  
 EFS (Encrypting File System), 530–534  
 EISA (Extended Industry Standard  
 Architecture), 8  
 electronic fingerprints, MD5 hash, 134–135  
 email  
 attachments. *See* Base64 encoding  
 column headings, 518–519  
 email types supported, 514–515  
 exercise examining, 521–523  
 overview of, 514  
 properties, 517  
 query using email filters, 515  
 Records tab and, 515–516  
 searches, 516, 516–517  
 storage files, 199  
 web mail, 519–521, 519–521  
 embezzlement case, 88–89  
 EMF mode, printing, 437–440, 438, 440  
 ENBCD (EnCase Network Boot CD),  
 125, 126  
 ENBD (EnCase Network Boot Disk),  
 125, 125  
 ENBD.EXE, 125  
 EnCase Decryption Suite (EDS), 530–534,  
 531–533  
 EnCase Enterprise. *See* EE  
 (EnCase Enterprise)  
 EnCase Network Boot CD (ENBCD),  
 125, 126  
 EnCase Network Boot Disk (ENBD),  
 125, 125  
 encoding methods  
 Base64 encoding, 524–525  
 overview of, 524  
 ROT-13, 498  
 Encrypting File System (EFS), 530–534  
 encryption  
 EDS (EnCase Decryption Suite),  
 530–534  
 imaging encrypted data, 93  
 encryption keys, global views, 257  
 EN.EXE, 125  
 EnScript  
 Case Processor, 411  
 determining status of files in Recycle Bin,  
 399–400  
 editing, copying, moving, and deleting  
 scripts, 511–512  
 File Mounter, 484–485, 485

- filters, conditions, and queries, 513–514, 514
- global views, 257
- Index Case tool, 333, 333
- Initialize Case, 388, 388, 512
- Link File Parser, 410–412
- navigation and paths, 510–511
- overview of, 509–510
- Partition Finder, 475–476, 475–476
- Report Generator, 329, 329
- running scripts, 512
- Tree pane view, 510–511
- Enterprise version, EnCase. *See* EE (EnCase Enterprise)
- Entries, case-level views, 253
- environment, EnCase, 209–272
  - adjusting panes, 248–249, 249
  - case-level views, 253, 253–255
  - Code view, 238
  - Console view, 240–241, 241
  - creating a case, 211–216
  - Details view, 242
  - Disk view, 234–235, 234–235
  - Dixon box, 242–243
  - Doc view, 241, 241
  - exam essentials, 265–266
  - exercise navigating, 249–253
  - Filter pane views, 246–248, 247
  - Find feature, 245–246, 246
  - Gallery view, 231–233, 232
  - global views, 255, 255–258, 258
  - Hex view, 239, 239
  - Lock option, 242
  - Macintosh example, 262–263
  - navigation data (GPS), 243–245, 244
  - Options menu, 259–261
  - Output view, 242
  - Picture view, 239–240, 240
  - Report view, Table pane, 231
  - Report view, view pane, 240
  - review questions, 267–271
  - summary, 264–265
  - Table pane, navigating, 222
  - Table view, 222–230
  - Text view, 238, 238–239
  - Timeline view, 235–237
  - Transcript view, 242
- Tree pane, navigating, 216–221, 217–221
- View pane, navigating, 238
- window layout, 210–211, 211
- epoch, Linux/Unix, 382–383
- error granularity, network acquisition and, 134, 134
- Ethernet NICs, 11
- event logs, Windows OSs, 445–452
  - auditing levels, 446–449
  - overview of, 445
  - resources for information regarding, 452
  - type of information available in, 445–446, 445–446
  - Windows Event Log Parser, 450, 450–451
  - Windows Vista, 449, 449
- event viewer, Windows XP, 446
- evidence files
  - components and function of, 180–183
  - exactness of duplication of in forensics, 200–201
  - exam essentials, 202
  - exercise maintaining data integrity, 188–190
  - format of, 178–179
  - format, when multiple files required, 182
  - physical layout of, 180
  - review questions, 204–208
  - verification of integrity, 183–188, 185–186
- evidence handling
  - bagging and tagging, 98–100
  - capturing volatile digital evidence, 92–94
  - computer shutdown procedures, 94–98
  - incident response. *See* evidence handling overview of, 89
  - photographing/recording scene, 90
  - securing the scene, 89–90
  - seizing computer evidence (physical), 90–92
- expansion slots
  - NICs, 10–11
  - overview of, 8
- Explorer, stopping/restarting, 504, 504–505

## 598 Export Report dialog – file integrity

Export Report dialog, 328, 566  
 exporting applications, 539–542, 540–541  
 Extended Industry Standard Architecture (EISA), 8  
 Extensible Firmware Interface (EFI), 9–10

**F**

fans, for cooling computer, 4  
 FastBloc 2  
   features, 138–139  
   steps in acquisition, 139–144, 141–144  
 FastBloc acquisition, 137–153  
   FastBloc 2 features, 138–139  
   FastBloc SE features, 146–147  
   models available for, 137–138  
   overview of, 137  
   steps in FastBloc 2 acquisition, 139–144, 141–144  
   steps in FastBloc SE acquisition, 148–153, 148–153  
 FastBloc SE  
   features, 146–147  
   steps in acquisition, 148–153, 148–153  
 FAT  
   data area, 43–48  
   deleting/undeleting files, 59–64  
   directory entry status byte, 66, 66–67  
   FAT area (file allocation table), 40–43  
   FAT entries viewed using EnCase, 48–50, 48–52  
   file storage, 52–59  
   file systems, 21–22  
   formatting partitions, 19–20  
   overview of, 32–33  
   partitions, 19  
   physical layout, 33–34, 34  
   reserved area (boot sector), 34–40  
   review questions, 74–80  
   slack space, 65, 65  
   time stamp, 391  
 FAT1, 40–43, 41  
 FAT12/16  
   determining starting cluster for, 46  
   FAT area (file allocation table), 41–43  
   FAT versions, 33  
   reserved area (boot sector), 34, 34  
   root directory, 43, 44  
   VBR (volume boot record), 36–38  
 FAT2, 40–43, 41  
 FAT32  
   backup boot sector, 35  
   FAT versions, 33  
   FSINFO, 36  
   reserved area (boot sector), 34–35, 35  
   root directory, 43–44, 44  
   VBR (volume boot record), 38–40  
 Favorites folder, Windows OSs, 421–422, 421–422  
 FDISK  
   partition recovery, 478–480  
   partitions created with, 19  
   partitions removed with, 20, 472–473  
 Field Intelligence Model. *See* FIM (Field Intelligence Model)  
 field kit, for incident response, 86–88  
 file allocation table, as FAT component, 33, 40–43  
 file extensions  
   entering file extension when creating new file signature, 354  
   entering multiple file extensions when creating new file signature, 355  
   file signature analysis and, 350  
   in file signature analysis report, 357–358  
   image files lacking file extensions on Mac system, 356  
   Windows OSs, 351  
 file group bookmarks, 324–325, 325  
 file headers  
   entering header string when creating new file signature, 353  
   file signature analysis and, 350  
   in file signature analysis report, 357–358  
 file integrity  
   CRC and MD5 and, 179  
   exercise maintaining data integrity, 188–189  
   Report view, 184, 186  
   verifying evidence file integrity, 183–188

- File Mounter, EnScript, 484–485, 485
- file segment size, network acquisition and, 133
- file signature analysis, 350–360
  - aliases and, 357, 357
  - application binding and, 350–352
  - conducting, 355–358
  - creating new file signature, 352–355
  - exam essentials, 373
  - exercise performing, 359–360
  - overview of, 350
  - review questions, 374–378
  - status types reported by EnCase, 357–358
  - summary, 372–373
- File signature view, 352
- file signatures
  - creating, 352–355
  - database of, 352
  - global views, 256
  - modifying by changing name of, 354
  - non-Windows systems and, 485
- file slack, 65
- file storage, FAT, 52–59
- file systems, 32–80
  - CD file systems, 70–72
  - exam essentials, 23, 72–73
  - FAT file systems. *See* FAT
  - mounting as read-only, 154
  - NTFS file systems, 67–70
  - overview of, 21–22, 32
  - review questions, 74–80
  - summary, 72
- file type codes, Macintosh computers, 351
- file types
  - file signature analysis and, 358
  - global views, 256
- file viewers, global views, 257
- files
  - backup files, 193–197
  - case file organization and management, 214
  - case files, 191–193
  - configuration files, 197–199
  - deleting/undeleting FAT files, 59–64
  - directory information for reading, 53–55, 53–56
  - directory information for writing, 56
  - evidence files. *See* evidence files
  - exam essentials, 202–203
  - list of compound files that can be mounted, 482–484
  - mounting, 480–486, 481, 485
  - naming conventions, 214–215
  - for paperless reports, 571
  - review questions, 204–208
  - summary, 201–202
  - Windows OSs. *See* folders and files, Windows OSs
- files, Recycle Bin
  - determining ownership of, 396–397, 397
  - EnScript for determining status of, 399–400, 400
  - restored or deleted, 398–399, 398–399
- Filter pane, 246–248, 247, 248
- filters
  - email queries, 515
  - EnScript, 513–514, 514
  - hash analysis and, 366–368, 367
  - regmon output, 501–502
- FIM (Field Intelligence Model)
  - digital acquisition, 164–165
  - imaging live systems, 93–94
  - schematic of, 164
- Find feature, 245–246, 246. *See also* searches
- fingerprints, forensic examination of computers and, 90
- firewalls, 164. *See also* Windows Firewall
- FireWire. *See* IEEE 1394
- floppy drives
  - boot process and, 13
  - checklist for field kit, 87
  - digital acquisition and, 165
  - overview of, 6
  - with VBR, 14
- folder information bookmarks, 318–321
- folders
  - Default Export folder and, 212
  - folder structure for case file, 192

- for hash sets, 363–364
- Index folder and, 213
- managing keyword folders, 294–295
- naming conventions, 214–215
- for paperless reports, 571
- Temporary folder and, 212

folders and files, Windows OSs

- Cookies folder, 425–426, 425–426
- Desktop folder, 418–419, 418–419
- Favorites folder, 421–422
- hibernation files, 435–436
- History folder, 426–431, 427, 429–430
- My Documents/Documents folder, 419
- print spooling files, 436–440, 438, 440
- Recent folder, 416–417, 417
- Send To folder, 420
- swap files, 435
- Temp folder, 420–421
- Temporary Internet Files (TIF) folder, 431–434, 433
- Windows 2000, XP, and Vista folders, 412–416
- Windows Vista Low folders, 422–425

forensic examination

- of computers, 90
- creating forensic boot disks, 111–113
- list of steps in, 549–552

format command, 19

format, of evidence files, 178–179

FSINFO, FAT32, 36

Full Report view, 567

---

## G

- Gallery view, Table pane, 231–233, 232, 567
- Gigabit Ethernet, 11
- global views, 255, 255–258, 258
- globally unique identifier (GUID), 396–397
- gloves
  - checklist for field kit, 86
  - preventing contamination of evidence, 91
- GMT (Greenwich mean time)
  - date and time artifacts and, 380–381
  - Linux/Unix epoch based on, 382–383

- Windows 2000/XP, 382
- Windows 64-bit time stamp and, 383–386, 385
- GPS (navigation data), 243–245, 244
- GREP searches
  - creating GREP expressions, 299–300
  - example, 302–304
  - list of useful expressions, 304–305
  - overview of, 297
  - symbols used in, 298–299
  - testing GREP expressions, 300–302
- GUID (globally unique identifier), 396–397
- Guidance Software
  - manuals for EnCase modules, 533
  - user-suggested features, 245
  - white paper on restoration, 545
  - Windows Vista support, 404
- GZIP files, 520

---

## H

- HAL (Hardware Abstraction Layer), 17
- hard drives
  - acquiring Mac drive using FireWire, 123
  - boot process and, 13
  - dead hard drives not always dead, 121–122
  - exercise previewing own hard drive, 145–146
  - in field kit for capturing evidence, 87
  - IDE, 5–6
  - with MBR and VBR, 14
  - overview of, 4–5
  - SATA, 6
  - SCSI, 5
- Hardware Abstraction Layer (HAL), 17
- hardware components
  - exam essentials, 23
  - list of, 2–11
  - review questions, 24–30
- hash analysis
  - bookmarking, 362, 362
  - condition filters, 366–368
  - conducting, 364–368
  - exam essentials, 373

- exercise performing, 369–371
  - hash sets and hash libraries, 361–364
    - MDS, 360–361
    - overview of, 360
    - review questions, 374–378
    - slack space and, 365, 365
    - summary, 372–373
  - Hash Conditions filter, 366–368, 367
  - Hash Items, Hash Sets view, 368, 368
  - hash libraries
    - including hash sets in, 365
    - overview of, 364, 364
  - Hash Properties tab, of Table pane, 366–367, 367
  - hash sets, 361–364
    - creating custom, 361–362
    - folders for, 363–364
    - global views, 256
    - importing from NSRL, 364
    - including in hash libraries, 365
    - naming, 363
  - Hash Sets view, 363, 363, 368, 368
  - hashing
    - disks and volumes, 190–191, 190–191, 202
    - network acquisition and, 134–135
    - report on hashing devices, 187
  - heads, in hard drive geometry, 5
  - heat sinks, 4
  - Helix, 154
  - hex, 281–284
    - converting binary numbers to, 275
    - decimal values corresponding to, 281–282
    - encoding system, 282
    - FFh, 283–284, 284
    - Hex view, 239, 239
  - Hex view, View pane, 239, 239
  - HFS+ (Hierarchical File System Plus), 351
  - hiberfil.sys file
    - overview of, 435–436
    - RAM contents written to, 412
    - recovering information in RAM when computer is unplugged, 3
    - searches for, 436
  - hibernation files. *See* hiberfil.sys file
  - Hierarchical File System Plus (HFS+), 351
  - high-bit ASCII, 285
  - Highlighted Data bookmarks, 313–315
  - History folder, Windows OSs, 426–431, 427, 429–430
  - hives, registry
    - hive list, 491
    - HKLM hive keys, 489–490
    - HKU hive keys, 490
    - mounting, 494, 494
    - overview of, 488
    - restore points and, 495–496
  - HKLM hive keys, 489–490
  - HKU hive keys, 490
  - Host Protected Area. *See* HPA (Host Protected Area)
  - HPA (Host Protected Area)
    - FastBloc SE support, 146
    - network acquisition and, 123
    - viewing invisible data, 114
  - HTML anchors, 572
  - hubs/switches, checklist for field kit, 87
  - hybrid sleep, Windows Vista, 412
  - hyperlinks, paperless reports, 572–575
- 
- I**
- IDE (Integrated Drive Electronics)
    - FastBloc SE support, 146
    - overview of, 5–6
  - IE (Internet Explorer)
    - Favorites folder, 421, 421
    - History folder, 426–431
  - IEEE 1394
    - acquiring Mac drive using FireWire, 123
    - FastBloc SE support, 146
    - overview of, 7
  - IEEE 1394a port, 7
  - IEEE 1394b port, 7
  - iLink, 7. *See also* IEEE 1394
  - image files. *See also* evidence files
    - format of, 178
    - lacking file extensions, 356
  - images (graphic), Picture view and, 239
  - images, of evidence, 110
  - incident response
    - checklist for field kit, 86–88
    - computer systems available, 84–86
    - evidence handling. *See* evidence handling

**602** Index Case tool – LinEn acquisition

- exam essentials, 101–102
- exercise, 100–101
- overview of, 82
- personnel and, 83–84
- physical location, assessing, 83
- planning and preparation, 82–83
- review questions, 103–108
- search authorization, 88–89
- summary, 101

Index Case tool, EnScript, 333, 333

index files, in Windows Vista Recycle Bin, 402–404

Index folder, folder structure and, 213

indexed searches, 333–339

Industry Standard Architecture (ISA), 8

INFO2 file

- bookmarks, 395–396
- database of information regarding Recycle Bin files, 393, 393–396, 395–396
- files restored or deleted from Recycle Bin, 398–399
- Windows Vista and, 402

INI files, 487. *See also* configuration files, EnCase

Initialize Case, EnScript, 388, 388, 512

Insert Hyperlink dialog, 574

Integrated Drive Electronics (IDE)

- FastBloc SE support, 146
- overview of, 5–6

International Organization for Standardization. *See* ISO (International Organization for Standardization)

International Telecommunications Union

- Telecommunications Standardization Sector (ITU-T), 350

IO.SYS, 111

ISA (Industry Standard Architecture), 8

ISO (International Organization for Standardization)

- CD standard (ISO 9660), 70–72, 71
- file standards, 350

ITU-T (International Telecommunications Union Telecommunications Standardization Sector), 350

---

**J**

Jaz drives, digital acquisition and, 165

Johnson-Grace compression, 233

Joliet extension, CD standard (ISO 9660), 70–71, 71

junctions, reparse points and, 413

---

**K**

keyboard port, 10

keyboards, boot process and, 13

keymaster, SAFE (Secure Authentication for EnCase), 163

Keyword Tester, 300–302, 300–304

keywords, 287–297

- adding keyword lists, 297, 297
- case-level views, 255
- case sensitivity, 291–292, 292
- creating, 289–291
- defined, 287
- global and case-specific, 287–289, 288
- global views, 256
- GREP. *See* GREP searches
- importing/exporting, 295–296, 296
- managing keyword folders, 294–295
- New Keyword dialog box, 289–291, 290
- search options, 292–294

KEYWORDS.INI file, 287

---

**L**

LanMan hash, 534

laptop computers, network acquisition and, 123

“last know good configuration”, 486

left nibbles, 278

legacy Windows OS artifacts, 441

LFN (long file names), 47–48

lighting, checklist for field kit, 86

LinEn acquisition, 153–161

- drive selection, 160
- mounting file system as read-only, 154
- overview of, 153

- running, 156–158
- start up options, 159
- steps in, 158–161
- updating Linux boot CD, 155–156, 155–156

Link File Parser, EnScript

- in Modules list of Case Processor EnScript, 411
- options, 411
- overview of, 410–412
- Report view, 412

link files, Windows OSs, 405–412

- Change Icon dialog box, 407
- changing shortcut properties, 406, 406
- Create Shortcut Wizard, 408
- forensic value of, 406–410, 409
- Link File Parser, 410–412
- overview of, 405
- in Recent folder, 417

Linux/Unix

- application binding and, 351
- computer shutdown procedures, 96
- dd command, 178
- EnCase for Linux. *See* LinEn acquisition epoch, 382–383
- file signatures, 485
- updating Linux boot CD with LinEn, 155–156, 155–156
- VFS (Virtual File System) support in, 535
- writing to NTFS, 157

little endian, 46, 385

.lnk files. *See* link files, Windows OSs

Local Settings folder

- History folder, 426
- Temp folder, 420–421
- Temporary Internet Files (TIF) folder, 416, 431

Lock option, View pane, 242

log record bookmarks, 326

logbooks, checklist for field kit, 87

Logical Disk Manager, in PDE module, 546

long file names (LFN), 47–48

Lotus Notes, exporting, 539–542

low-bit ASCII, 285, 524

Low folders, Windows Vista

- Cookies folder, 425–426
- History folder, 426–431

- overview of, 422–425
- Temporary Internet Files (TIF) folder, 423, 431–434

---

## M

MAC (Media Access Control)

- addresses, 11
- file date and time attributes, 381
- time stamps, 408–409

Macintosh

- acquiring Mac drive using FireWire, 123
- application binding and, 351–352
- BinHex encoding, 525
- computer shutdown procedures, 97, 97
- EnCase environment example, 262–263
- file signature analysis, 355–358
- file signatures, 485
- image files lacking file extensions, 356
- VFS (Virtual File System) support in, 535

magnets, protecting computer evidence from exposure to, 99

mainboard. *See* motherboards

Mandatory Integrity Control (MIC), 423

manuals, checklist for field kit, 87

master boot record. *See* MBR (master boot record)

master devices, vs. slave devices, 6

master file table (MFT), 21, 392

*Mastering Windows Network Forensics and Investigation* (Anson), 94

MBR (master boot record)

- boot process and, 13–14, 14
- mounting partitions and, 471–478

MCA (Micro Channel Architecture), 8

MD5 (Message Digest 5)

- acquisition hashes, 180
- evidence files and, 180–183
- file integrity and, 179
- hash analysis and, 360–361
- hash collisions, 185

## 604 memory – NTFS (New Technology File System)

- network acquisition and, 134–135
    - verifying evidence file integrity, 183–188
  - memory
    - RAM (random access memory), 3–4
    - ROM (read-only memory), 3
  - Message Digest 5. *See* MD5 (Message Digest 5)
  - metadata, file systems and, 21
  - \$MFT, in NTFS, 68
  - MFT (master file table), 21, 392
  - MIC (Mandatory Integrity Control), 423
  - Micro Channel Architecture (MCA), 8
  - microprocessor. *See* CPU (central processing unit)
  - Microsoft FrontPage, 575
  - MIME (Multipurpose Internet Mail Extensions Standard), 525
  - modem (modulate/demodulate), 11
  - Modify Time Zone Settings, Tree pane, 389, 389
  - motherboards, 4
  - Mount As Emulated Disk dialog, 546–547, 547
  - mounting
    - file system as read-only, 154
    - files, 480–486
    - partitions, 471–478
    - registry files, 493–496
  - mouse port, 10
  - MS-DOS. *See also* DOS
    - configuration files, 487
    - time stamp, 391
  - Multipurpose Internet Mail Extensions Standard (MIME), 525
  - My Documents/Documents folder, Windows OSs, 419
- 
- N**
- naming conventions
    - cases, 212
    - columns, in Table pane, 226–230
    - DOS, 45
    - files and folders, 214–215
    - LFN (long file names), 47–48
  - National Software Reference Library (NSRL), 364
  - navigation data (GPS), 243–245, 244
  - navigation, EnScript, 510–511
  - netstat.exe, 94
  - network acquisition
    - acquiring device being previewed, 131
    - booting up, 127
    - completion report, 136
    - configuring options for, 130–137, 132
    - overview of, 123
    - preparing EnCase network boot CD, 126
    - preparing EnCase network boot disk, 125
    - reasons for using, 123–124
    - setting up acquisition, 127–130, 130
    - understanding network cables, 124–125
  - network boot disk, 125
  - network cables
    - checklist for field kit, 87
    - overview of, 124–125
  - network connections, capturing, 94
  - network crossover cables, 124–125
  - Network Interface Card (NIC)
    - network acquisition and, 125
    - overview of, 10–11
  - New File Signature dialog box
    - entering file extension, 354
    - entering header string, 353
  - nibbles
    - consisting of 4 bits, 275
    - table of properties, 279
  - NIC (Network Interface Card)
    - network acquisition and, 125
    - overview of, 10–11
  - nonvolatile random access memory (NVRAM), 3
  - notable file bookmarks, 321–324, 322
  - notes bookmarks, 317–318
  - NSRL (National Software Reference Library), 364
  - NT Loader (NTLDR), 15
  - NTDETECT.COM, 17
  - NTFS (New Technology File System)
    - dates and times and, 381
    - file systems, 21–22
    - Linux writing to, 157

- overview of, 67–68
- partitions, 19
- recovering deleted partition, 69–70
- review questions, 76
- system files, 68–69
- NTFS5, Windows Vista, 67
- NTLDR (NT Loader), 15
- NTOSKRNL.EXE, 17
- NVRAM (nonvolatile random access memory), 3

---

## O

- Options menu, EnCase environment, 259–261
- OSs (operating systems)
  - application binding and, 350–352
  - artifacts, 380. *See also* Windows OS artifacts
- Outlook, searching for PST data, 485–486
- Output view, View pane, 242
- Outside In Technology, Stellent Inc., 241–242

---

## P

- packages, global views, 257
- packet writing, UDF (Universal Disk Format), 71
- page files. *See* swap files
- paperless reports, 564–577
  - bookmarks and hyperlinks, 572–575
  - burning reports to CD or DVD, 575–577
  - creating container reports, 568–572
  - exporting Web page reports, 565–568
  - files and folders needed for, 571
  - overview of, 564–565
- parallel ATA (PATA), 5
- parallel ports, 11
- ParseCache folder, 199–200, 199–200
- Partition Finder, EnScript, 475–476, 475–476
- partitions, 18–20
  - Add Partition dialog, 474
  - exam essentials, 23

- examining partition table, 20
- exercise in partition recovery, 478–480
- formatting, 19–20
- locating/mounting, 471–478, 471–478
- Partition Finder, EnScript, 475–476, 475–476
- recovering deleted NTFS partition, 69–70
- table fields, 18–19
- volumes compared with, 18
- passwords, network acquisition and, 133
- PATA (parallel ATA), 5
- paths, EnScript, 510–511
- PC Cards, 8
- PC reference guides, checklist for field kit, 86
- PCI Express, 8
- PCI (Peripheral Component Interconnect), 8
- PCMCIA cards, 8
- PCMCIA (Personal Computer Memory Card International Association), 8
- PDE (Physical Disk Emulator), 545–549, 546–547
- Peripheral Component Interconnect (PCI), 8
- Personal Computer Memory Card International Association (PCMCIA), 8
- personnel, incident response and, 83–84
- PGPdisk, 93
- Photographer, on search team, 90
- photographing/recording
  - computer screens, 93
  - physical scene in incident response, 90
- Physical Disk Emulator (PDE), 545–549, 546–547
- physical layout
  - of evidence files, 180
  - FAT, 33–34, 34
- physical location, assessing in incident response, 83
- Picture view, View pane, 239–240, 240
- pinned area, Windows interface, 496
- planning aspect, incident response, 82–83
- Plug and Play
  - DRIVER.CAB file and, 17
  - USB and, 7
- ports
  - IEEE 1394, 7
  - mouse and keyboard ports, 10
  - parallel and serial, 11–12
  - USB, 7

## 606 POST (Power On Self-Test) – registry

POST (Power On Self-Test), 12–13  
 power cords  
   checklist for field kit, 86  
   pulling the plug, 98  
 Power On Self-Test (POST), 12–13  
 power supplies, 4  
 power-up sequence. *See* boot process  
 primary IDE, 5  
 print spooling files, Windows OSs, 436–440, 438, 440  
 program counters, resetting, 12  
 projects, global views, 257  
 PS2 connection, for mouse, 10  
 PST data (Outlook), searching for, 485–486  
 Public folder, Windows Vista, 418

**Q**

queries  
   EnScript, 513–514  
   using email filters, 515  
 Qwords  
   measurement unit consisting of  
     8 bytes, 278  
   table of properties, 279

**R**

radio frequency (RF), 99–100  
 RAID (Redundant Array of Inexpensive Disks), 6  
 Rainbow Crack, 534  
 Rainbow tables, 534  
 RAM (random access memory)  
   boot process and, 13  
   overview of, 3  
   swap files and, 435  
 RAM slack, 65  
 RAW mode, printing, 437–438, 438  
 read-only memory (ROM), 3  
 Real-Time Clock (RTC), 9, 13  
 Recent folder, Windows OSs, 416–417, 417  
 Recorder, on search team, 90  
 records, case-level views, 254  
 Records tab, email, 515–516  
 Recover Folders feature, 477  
 Recycle Bin Info Record Finder script, 400  
 Recycle Bin Properties dialog, 401  
 Recycle Bin, Windows OSs, 392–405  
   bypassing, 400–402, 401  
   determining ownership of files in, 396–397, 397  
   EnScript for determining status of files in, 399–400, 400  
   files restored or deleted from, 398–399, 398–399  
   INFO2 file, 393, 393–396, 395–396  
   overview of, 392  
   Windows Vista, 402–405, 402–405  
 Redundant Array of Inexpensive Disks (RAID), 6  
 regedit  
   overview of, 488, 488  
   viewing values in UserAssist key, 497–498  
 regedit.exe, 488  
 regedt32.exe, 488  
 registry  
   decoding ROT-13 values, 498–500  
   exercise examining, 521–523  
   exercise working with, 502–503  
   filtering regmon output, 501–502  
   finding forensic evidence in, 506–508  
   history of, 487  
   hive list, 491  
   HKLM hive keys, 489–490  
   HKU hive keys, 490  
   mounting and viewing with EnCase, 493–496, 494  
   organization and terminology, 488  
   overview of, 486–487  
   regedit for viewing values in UserAssist key, 497–498  
   registry editor, 491  
   registry file displayed in Table pane, 493  
   regmon for observing changes in, 500–501  
   research techniques for, 496–497  
   root keys, 489  
   Scan Registry, EnScript, 508–509, 509  
   time zone offsets stored in, 386  
   value data types, 492  
   viewing results of changes to, 503–506  
   Windows XP registry editor, 488

regmon

- default mode, 501
- Filter settings, 501
- filtering regmon output, 501–502
- finding forensic evidence in registry, 506–508
- observing changes in registry, 500–501
- reparse points, Windows Vista, 413
- Report Generator, 329, 329
- Report view
  - file verification, 184, 186
  - Link File Parser EnScript, 412
  - Table pane, 231, 231
  - View pane, 240
  - Web Page option, 328
- reports, creating from bookmarked data, 327–329
- reserved area (boot sector), 34–40
  - FAT16, 34, 34
  - FAT32, 34–35, 35
  - VBR (volume boot record) for FAT12/16, 36–38
  - VBR (volume boot record) for FAT32, 38–40
- resident data, in \$MFT, 68
- restoration, 542–545, 543–545
- Restore Drives dialog, 543
- restore points
  - hive files and, 495–496
  - registry recovery and, 486
- RF (radio frequency), 99–100
- right nibbles, 278
- Rivest, Shamir, and Adleman (RSA), 134–135. *See also* MD5 (Message Digest 5)
- roaming profiles, Windows OSs, 415–416
- Rock Ridge extension, CD standard (ISO 9660), 72
- ROM (read-only memory), 3
- root directory, FAT, 43–44, 44
- root keys, registry, 489
- root user folder
  - Cookies folder, 425
  - History folder, 426
  - My Documents/Documents folder, 419
  - in Windows NT-based OSs, 414–415, 415

ROT-13
 

- decoding, 498–500
- value attributes decoded, 505

routines, bookmarking, 326

RS-232 port, 11

RSA (Rivest, Shamir, and Adleman), 134–135. *See also* MD5 (Message Digest 5)

RTC/NVRAM
 

- overview of, 9
- settings, 10

RTC (Real-Time Clock), 9, 13

---

## S

SAFE (Secure Authentication for EnCase), 163

safety
 

- assessing physical location in incident response, 83
- securing the scene in incident response, 89

SAM (Security Accounts Manager)
 

- determining ownership of files in Recycle Bin, 396–397
- EDS and, 533

SATA (Serial Advanced Technology attachment) controller, 6

Scan Registry, EnScript, 508–509, 509

scripts. *See* EnScript

SCSI (Small Computer Systems Interface)
 

- FastBloc SE support, 146–147
- hot-swappable, 152
- overview of, 5

seals, file integrity, 180

Search-and-seizure specialist, 90

Search dialog box
 

- Compute Hash Value, 361, 361–362
- file signature analysis tool enabled from, 356
- hash analysis enabled from, 361
- search options, 307, 307–309

search engines, 287

Search Filenames condition, 436

search hints, case-level views, 254

Search Hits view, 309–313, 310

## 608 search strings – Table pane

- search strings. *See* keywords
  - search warrants, 88–89
  - searches. *See also* bookmarks; Find feature
    - authorization for in incident response, 88–89
    - email, 516, 516–517
    - exercise searching and bookmarking, 330–333
    - GREP. *See* GREP searches
    - hash analysis and, 368
    - indexed searches, 333–339, 333–339
    - keyword searches, 287–289
    - search options, 307–309
    - starting, 306, 306–307
    - viewing search hits, 309–313
  - secondary IDE, 5
  - sector slack, 65
  - sectors
    - in hard drive geometry, 5
    - supported by FAT versions, 33
  - Secure Authentication for EnCase (SAFE), 163
  - secure storage, case-level views, 254
  - security
    - securing the scene in incident response, 89–90
    - Windows Vista, 423–424
  - Security Accounts Manager (SAM)
    - determining ownership of files in Recycle Bin, 396–397
    - EDS and, 533
  - security ID (SID), 396–397, 397
  - Send To folder, Windows OSs, 420
  - Serial Advanced Technology attachment (SATA) controller, 6
  - serial ports, 11
  - Set Included Folders
    - hash analysis and, 366
    - importing/exporting keywords and, 296
    - trigger, 220–221, 220–221
  - Setup, RTC/NVRAM settings and, 10
  - shadow files, print jobs, 437, 438
  - shortcuts. *See* link files, Windows OSs
  - shutdown procedures, computer systems, 94–98
  - SID (security ID), 396–397, 397
  - slack space
    - FAT, 65, 65
    - hash analysis and, 365, 365
  - slave devices, vs. master devices, 6
  - Small Computer Systems Interface. *See* SCSI (Small Computer Systems Interface)
  - sound cards, 8
  - SPL files. *See* spool files
  - spool files, 437, 438
  - Start menu, Windows OSs, 496–497, 497
  - status bytes
    - directory entries, 66, 66–67
    - FAT directories, 59
  - Stellent Inc., Outside In Technology, 241–242
  - SubSeven hacking tool, 361
  - suspects, incident response and, 84
  - swap files
    - file artifacts, 435
    - recovering information in RAM when computer is unplugged, 3
    - searches for, 436
  - Sweep Case. *See* Case Processor, EnScript
  - sweeping bookmarks, 313
  - symbols, GREP, 298–299
  - SYSINIT, 15
  - system clock, boot process and, 13
  - system date and time, RTC/NVRAM
    - settings, 10
  - system files
    - NTFS (New Technology File System), 68–69
    - Windows OSs, 413
  - System Properties, Windows Vista, 442
  - system state, capturing live system state data, 93
- 
- T**
- Table pane
    - adjusting panes, 248
    - Code view, 238
    - column names, 226–230
    - Disk view, 234–235
    - Gallery view, 231–233
    - hash analysis and, 366–367, 367
    - locking columns, 222–223, 222–223
    - navigating, 222
    - organizing bookmarks and creating reports, 327

- registry file displayed in Table pane, 493
- Report view, 231, 231
- showing hidden columns, 226, 226
- sorting columns, 223–225, 224
- Table view, 222–230
- Timeline view, 235–237, 236–237
- working with keyword folder in, 295
- tagging evidence, 98–100
- Task Manager, 504, 504–505
- Temp folder, Windows OSs
  - artifacts and, 420, 420–421
  - folder structure and, 212
- Temporary Internet Files (TIF) folder, 431–434, 433
- text fragment bookmarks, 313
- text styles, global views, 256
- Text view, View pane, 238, 238–239
- threads, bookmarking, 326
- TIF (Temporary Internet Files) folder, 431–434, 433
- Time and Date Control Panel, 507
- time artifacts. *See* date and time, Windows OSs
- Time Properties dialog, 390
- time stamps
  - 64-bit date and time stamp in Windows OSs, 382–386
  - date and time stamps, Timeline view, 237, 237
  - DOS and FAT, 391
  - link files, 407
  - MAC (Media Access Control), 408–409
  - Windows Vista, 410
- time zones, Windows OSs
  - ActiveTimeBias, 388
  - adjusting for offsets, 386–392
  - bookmarking, 389, 389
  - extracting time zone information with Initialize Case Enscript, 388, 388
  - key values in registry, 387
  - overview of, 381–382
  - Time Properties dialog, 390
- Timeline view
  - color coding of date and time stamps, 237
  - Table pane, 235–237, 236–237
- Token Ring, 11
- toolkits, checklist for field kit, 86
- tracks, in hard drive geometry, 5

- Transcript view, View pane, 242
- Tree pane
  - adjusting panes, 248
  - Hash Sets view, 363
  - Modify Time Zone Settings, 389, 389
  - navigating, 216–221, 217–221
  - organizing bookmarks and creating reports, 327
  - running scripts, 512
  - viewing scripts, 510–511
  - working with keyword folders and, 295
- tripods, photographing computer screens, 93
- Trojan Defense, 93

---

## U

- UAC (User Account Control), 423
- UDF (Universal Disk Format), 71
- UEFI (Unified EFI), 10
- UIPI (User Interface Privilege Isolation), 424
- Unicode, 286–287, 287
- Unified EFI (UEFI), 10
- Uniform Resource Locators (URLs), 421, 421
- uninterruptible power supplies (UPSs), 86
- Universal Disk Format (UDF), 71
- Universal time, 380–381
- Unix. *See* Linux/Unix
- UPSs (uninterruptible power supplies), 86
- URLs (Uniform Resource Locators), 421, 421
- USB controllers, 7
- USB ports, 7
- USB (universal serial bus)
  - FastBloc SE support, 146
  - imaging USB flash media, 165
  - mouse and keyboard ports, 10
  - overview of, 7
- User Account Control (UAC), 423
- User Interface Privilege Isolation (UIPI), 424
- UserAssist key, registry
  - Start menu content in, 497
  - value attributes decoded, 505
  - viewing values in, 497–498
  - working with registry and, 503
- uencoding, 524

**V**

- VBM (volume bit map), 21
- VBR (volume boot record), 14
  - boot process and, 13–14
  - FAT12/16, 36–38
  - FAT32, 38–40
  - mounting partitions and, 471–478, 472
  - removing partitions and, 20
- verification hash value, 185
- Verify File integrity, 185, 191
- VESA Local Bus (VL-Bus), 8
- VFS (Virtual File System)
  - overview of, 535–538, 535–539
  - PDE (Physical Disk Emulator) compared with, 545–549
- VGA (Video Graphics Array), 8
- video, 13
- video cards, 8
- Video Graphics Array (VGA), 8
- View File Structure, 481
- View pane, 238–242
  - adjusting panes, 248
  - Console view, 240–241
  - Details view, 242
  - Dixon box, 242–243
  - Doc view, 241
  - Find feature, 245–246
  - Hex view, 239
  - Lock option, 242
  - navigating, 238
  - navigation data (GPS), 243–245
  - Output view, 242
  - Picture view, 239–240
  - Report view, 240
  - Text view, 238–239
  - Transcript view, 242
- Virtual File System. *See* VFS (Virtual File System)
- VL-Bus (VESA Local Bus), 8
- volatility, ROM vs. RAM memory, 3
- volume bit map (VBM), 21
- volume boot record. *See* VBR (volume boot record)
- volume shadow copies, Windows Vista, 441–445, 442–444

## volumes

- exam essentials, 23
- hashing, 190–191, 190–191
- partitions compared with, 18

**W**

- web mail, 519–521, 519–521
- Web Page option, Report view, 328
- Web page reports, exporting, 565–568, 567
- Webmail Parser, 519, 519–521, 521
- window layout, EnCase environment, 210–211, 211
- Windows 2000
  - boot process, 15, 17
  - folder artifacts, 412–416
  - GMT and, 382
  - system files, 413
- Windows 9x
  - artifacts, 441
  - system files, 413
- Windows Event Log Parser, 450, 450–451
- Windows Firewall, 129, 129
- Windows NT
  - boot process, 15, 17
  - system files, 413
- Windows OS artifacts
  - dates and times. *See* date and time, Windows OSs
  - event logs. *See* event logs, Windows OSs
  - exam essentials, 460–462
  - exercise performing artifact recovery, 452–455
  - exercise performing artifact recovery in Windows Vista, 455–457
  - folders and files. *See* folders and files, Windows OSs
  - legacy OS artifacts, 441
  - link files. *See* link files, Windows OSs
  - Recycle Bin. *See* Recycle Bin, Windows OSs
  - review questions, 463–468
  - summary, 457–460
  - Windows Vista volume shadow copies, 441–445

Windows OSs, 67

- application binding and, 351
- computer shutdown procedures, 94–96
- Disk Manager for partitioning, 19
- EDS module supporting EFS in, 531
- EMF header search strings, 439
- EnCase updating Windows boot disks, 111, 111
- NTFS, 67–70
- Recycle Bin compared in Windows versions, 394
- registry history and, 487–488
- roaming profiles, 415–416
- root user folder, 414–415, 415
- VFS (Virtual File System) support in, 535

Windows Vista

- boot process, 17
- Cookies folder, 425–426
- event logs, 449, 449
- folder and file artifacts, Windows OSs, 412–416
- History folder, 426–431
- last accessed time stamp disabled, 410
- Low folders, 422–425
- NTFS5, 67
- Recycle Bin artifacts, 402–405, 402–405
- reparse points, 413
- system files, 413
- System Properties, 442
- Temporary Internet Files (TIF) folder, 423, 431–434
- volume shadow copies, 441–445, 442–444

Windows XP

- boot process, 15, 17
- default audit policies, 445
- event viewer, 446
- folder and file artifacts, Windows OSs, 412–416
- GMT and, 382
- NTFS5, 67
- registry editor, 488
- system files, 413

words

- measurement unit consisting of
  - 2 bytes, 278
- table of properties, 279

Write-Block, 152

Write-Protect, 152

---

## X

xxencoding, 524

---

## Z

ZBR (Zoned-Bit Recording), 5

Zip drives, digital acquisition and, 165

ZIP files, Base64 encoding, 516, 516

Zulu time, 380–381