
Index

A

agent notes worksheets, 168

aiο file analysis

dynamic analysis

GNU debugger, 358-360, 362, 364

of recovered uncompressed aiο binary,
397-402, 408

overview, 353

recovering the uncompressed aiο
binary, 364-369, 372-377

strace command, 353-357

overview, 345-346

static analysis

file command, 347

hexadecimal viewer, 348-349

ldd command, 350

ls -al command, 346

md5sum command, 346

nm command, 349

objdump commands, 352-353

of recovered uncompressed aiο binary,
377-397

overview, 346

readelf command, 350-352

strings -a command, 347-348

alert data

NSM collection of, 87

overview, 79-80

tools for, 93

anonymous remailers, 605, 607

Anti-Hacker Tool Kit (Jones), 404

anti-static bags, 165

AOL, 289

app paths registry entries, 295

Apple Mail, 289

Argus

overview, 92

Windows intrusion, 102-104, 114, 116,
122-123

auditing policy, 36

INDEX

B

- Bejtlich, Richard, 88
- BinText, 420
- blank CD-R/DVD-R, 165
- blank floppies, 166
- boot disks, 165
- bootable CD-ROM environment
 - Knoppix distribution, 504-511
 - overview, 503

C

- cable ties, 165
- cached NetBIOS name tables, 13
- Carrier, Brian, 209
- CF (Compact Flash) cards
 - content analysis, 588
 - with commercial solutions, 593-594
 - with open source solutions, 589-591, 593
 - duplication of, 575-576
- chain of custody forms, 165, 168
- commercial solutions
 - CF (Compact Flash) cards, 593-594
 - file signatures and electronic discovery, 236, 238
 - metadata collection, 221, 223, 225
 - recovering deleted files, 214, 218
 - removing known files, 230, 232
 - string searching and file fragments, 244, 246
 - USB memory devices, 585, 588
- commercial-based forensic duplications
 - with EnCase, 175, 180-181
 - with FTK, 181, 185
 - overview, 171
 - read-only IDE to Firewire device, 172-175

common forensic analysis techniques

- file signatures and electronic discovery
 - commercial solutions, 236, 238
 - open source solutions, 233-235
 - overview, 233
 - metadata collection
 - commercial solutions, 221-225
 - open source solutions, 218, 220
 - overview, 218
 - overview, 207
 - recovering deleted files
 - commercial solutions, 214, 218
 - open source solutions, 207-214
 - overview, 207
 - removing known files
 - commercial solutions, 230, 232
 - open source solutions, 225-230
 - string searching and file fragments
 - commercial solutions, 244, 246
 - open source solutions, 238, 240-243
 - overview, 238
- Compact Flash cards. See CF (Compact Flash) cards**
- consolidation, 83**
- “The Coroner’s Toolkit” (Farmer and Wietse), 209**

D

- data collection**
 - accessing network traffic, 89-93
 - collecting and storing network traffic, 91
 - overview, 82
 - using alert data, 87, 93
 - using full content data, 84, 92
 - using session data, 85-86, 92
 - using statistical data, 88, 93
- DataRescue, 405**

dates, Excel problem with, 635-636

DCFL DD

- overview, 195-197
- on ultimate response CD, 501

DD (data dump)

- evidence file, creation of, 188-192
- evidence hard drive, creation of, 192-193
- overview, 187

DD Rescue, 193-195

debugfs command, 364, 366

debuggers, 440-441

deleted file recovery

- commercial solutions, 214, 218
- open source solutions, 207-214
- overview, 207

digital camera, 164

documentation

- agent notes worksheets, 168
- chain of custody forms, 168
- evidence access log, 169
- evidence custodian log, 169
- evidence labels, 168
- evidence worksheets, 167
- overview, 167-169
- system worksheets, 167

domain name ownership

- IP addresses, translating FQDNs to, 616-619
- overview, 609
- Postgres, importing TLD Zone files into, 610-615
- searching for DNSs, 620-624
- searching for domains, 619-620

domain name servers, searching for, 620-624

dremel tool, 164

Dykstra, Brian, 504

E

80 pin IDE cables, 165

Eindeutig, 276

e-mail activity reconstruction

- commercial forensic tools, 274-275
- with FTK, 274
- open source solutions
 - AOL, 289
 - Apple Mail, 289
 - Lotus Notes, 288
 - Netscape/Mozilla, 288
 - Outlook, 288
 - Outlook Express, 275, 278-279, 282-283
- overview, 273
- with Paraben's Network Email Examiner, 274

E-Mail DBX file format, 281, 283-284

e-mail tracing

- anonymous remailers, 605, 607
- Hotmail, 597-599
- Netscape, 601-603
- POP-based email, 604-605
- Yahoo!, 600-601

EnCase, 171, 175, 180-181

- deleted file recovery with, 214, 217
- file signatures and electronic discovery, 236, 238
- forensic acquisition using, 517, 519, 522, 529, 531
- forensic analysis using, 564, 567, 570
- metadata collection, 221-224
- removing known files, 230, 232
- string searching and file fragments, 244, 246
- Web browsing activity reconstruction, 248-272

INDEX

- Ethereal, 92
- evidence access log, 169
- evidence custodian log, 169
- evidence envelopes, 165
- evidence file, creation of, 188-192
- evidence hard drive
 - creation of, 192-193
 - overview, 165
- evidence labels, 165, 168
- evidence tape, 165
- evidence worksheets, 167
- executables opening TCP or UDP ports, 10-12
- exploitation, 83
- F**
- Farmer, Dan, 209
- FatBack, 581
- file command, 307, 347, 418
- file signatures and electronic discovery
 - commercial solutions, 236, 238
 - open source solutions, 233-235
 - overview, 233
- file system MD5 checksum values, 61
- file system time and date stamps, 31-35, 59, 61
- Filemon, 441, 485, 487
- flashlight, 164
- Folders DBX file format
 - internal structure, 278-279
 - overview, 277
- forensic analysis techniques. *See* common forensic analysis techniques
- forensic duplication
 - anti-static bags, 165
 - blank CD-R/DVD-R, 165
 - blank floppies, 166
 - boot disks, 165
 - cable ties, 165
 - chain of custody forms, 165
 - digital camera, 164
 - documentation
 - agent notes worksheets, 168*
 - chain of custody forms, 168*
 - evidence access log, 169*
 - evidence custodian log, 169*
 - evidence labels, 168*
 - evidence worksheets, 167*
 - overview, 167-169*
 - system worksheets, 167*
 - dremel tool, 164
 - 80 pin IDE cables, 165
 - evidence envelopes, 165
 - evidence hard drives, 165
 - evidence labels, 165
 - evidence tape, 165
 - flashlight, 164
 - forensic software dongles, 166
 - 40 pin IDE cables, 165
 - jumpers, extra, 164
 - network cable, 166
 - network hub/switch, 166
 - operating system installation media, 166
 - pens, 165
 - power extension cords, 165
 - power strip, 166
 - preparation for, 163-164, 166
 - screwdriver, 164
 - screws, extra, 164
 - SCSI cables, 165
 - SCSI terminators, 165
 - tool kit, 164
 - ultimate response CD, tools on, 501-502

- forensic software dongles, 166
 - forensic tool analysis on Linux-based platform
 - aio file
 - dynamic analysis*, 353-369, 372-377, 397-402, 408
 - overview*, 345-346
 - static analysis*, 346-353, 377-397
 - case background, 302
 - “Hello World” program, examining,
 - 303-305
 - dynamic analysis of*, 335-342
 - static analysis of*, 305-335
 - overview*, 301-302
 - forensic tool analysis on Windows-based platform
 - case background, 409
 - “Hello World” program, examining,
 - 410, 413
 - dynamic analysis of*, 438-443
 - static analysis of*, 418, 420-426, 429, 434, 438
 - overview*, 409
 - sak.exe file
 - dynamic analysis of*, 457-461, 465, 467, 470, 473-479
 - overview*, 444
 - static analysis of*, 444-452, 456-457
 - forensic workstation, 4
 - 40 pin IDE cables, 165
 - FTK (Forensic Tool Kit)
 - e-mail activity reconstruction with, 274
 - overview*, 171, 181, 185
 - Web browsing activity reconstruction,
 - 252, 257
 - full content data
 - NSM collection of, 84
 - overview*, 76-77
 - tools for, 92
 - full system memory dumps, 26-27, 29
 - G-H**
 - Galleta, 268, 270-271
 - GNU debugger, 338-342, 358-364
 - Hall, Eric, 76
 - “Hello World” program, Linux-based
 - analysis of*, 303-305
 - dynamic analysis of*, 335
 - GNU debugger*, 338, 340-342
 - strace command*, 336-337
 - static analysis of*, 305
 - file command*, 307
 - hexadecimal viewer, use of*, 311, 313
 - ldd command*, 317
 - md5sum command*, 306
 - nm command*, 314-316
 - objdump command*, 329, 331-332, 334-335
 - readelf command*, 318-320, 322-324, 326-329
 - strings command*, 307-308, 310-311
- “Hello World” program, Windows-based
 - analysis of*, 410, 413
 - dynamic analysis of*, 438
 - debuggers*, 440-441
 - Registry Monitor*, 443
 - Strace*, 439
 - static analysis of*, 418
 - file command*, 418
 - hexadecimal viewer*, 420-422
 - IDA*, 434, 438

INDEX

link command, 429, 434
md5sum command, 418
nm command, 422
objdump command, 422-423,
 425-426
pe map command, 426
strings command, 418, 420
 hexadecimal viewer, 311, 313, 348-349,
 420-422, 446-447
 history files, 67, 69
 Hotmail, 597-599
 HP iPAQ Pocket PC 2003
 forensic acquisition of, 531, 536, 539
 forensic analysis of, 559-563

I

IDA, 434, 438, 452, 456-457
 IE (Internet Explorer) and Web browsing
 activity reconstruction. *See* Web
 browsing activity reconstruction
 IIS logs, 38-41
*Incident Response and Computer
 Forensics* (Prosis, Mandia, and
 Pepe), 163
*Incident Response: Investigating
 Computer Crime* (Mandia and
 Prosis), 397, 404
 Input, Perl used to read, 625-627
 installed programs, identifying, 292,
 295-296
 Interactive Disassembler, 405
 internal routing table, 14-15, 56
Internet Core Protocols (Hall), 76
 intruder, detection of, 70

IP addresses, translating fully qualified
 domain names to, 616-619

J-K

Jones, Keith J., 260, 276, 404
 jumpers, extra, 164
 Knoppix distribution on CD-ROM,
 504-511
 known file removal
 commercial solutions, 230-232
 open source solutions, 225-230

L

ldd command, 317, 350
link command, 429, 434
 Linux-based analysis of “Hello World”
 program, 303-305
 dynamic analysis of, 335
 GNU debugger, 338, 340-342
 strace command, 336-337
 static analysis of, 305
 file command, 307
 hexadecimal viewer, use of, 311, 313
 ldd command, 317
 md5sum command, 306
 nm command, 314-316
 objdump command, 329, 331-332,
 334-335
 readelf command, 318-320, 322-324,
 326-329
 strings command, 307-308, 310-311
 Linux-based platform, forensic tool
 analysis on
 aio file
 dynamic analysis, 353-369, 372-377,
 397-402, 408

- overview*, 345-346
 - static analysis*, 346-353, 377-397
 - case background, 302
 - “Hello World” program, examining, 303-305
 - dynamic analysis of*, 335-342
 - static analysis of*, 305-335
 - overview, 301-302
 - live IR data, Perl used to process, 634-635
 - loaded kernel modules, 57
 - local forensic duplication, 199
 - login history, 37, 62-63
 - logs, 169
 - Lotus Notes, 288
 - ls -al command, 346
- M**
- Makefile, 493-494
 - Malware: Fighting Malicious Code* (Skoudis), 53
 - Mandia, Kevin, 163, 397, 404
 - md5sum command, 306, 346, 418, 445, 450
 - memory devices
 - Compact Flash cards, 575-576
 - overview, 571
 - USB devices, 571-575
 - metadata collection
 - commercial solutions, 221-225
 - open source solutions, 218-220
 - overview, 218
 - Microsoft Windows Registry
 - reconstruction
 - app paths registry entries, 295
 - installed programs, identifying, 292, 295-296
 - “most recently used” documents, identifying, 296, 299
 - overview, 291
 - uninstallation registry entries, 293
 - “most recently used” documents, identifying, 296, 299
 - mounted file systems, 57
- N**
- National Institute of Standards and Technology (NIST), 225
 - National Software Reference Library (NSRL), 225
 - NBE (network-based evidence)
 - alert data, 79-80
 - data collection
 - accessing network traffic*, 89, 91, 93
 - alert data tools*, 93
 - collecting and storing network traffic*, 91
 - full content data tools*, 92
 - overview*, 82
 - session data tools*, 92
 - statistical data tools*, 93
 - using alert data*, 87
 - using full content data*, 84
 - using session data*, 85-86
 - using statistical data*, 88
 - full content data, 76-77
 - overview, 75-76
 - session data, 78-79
 - standard intrusion, 82
 - statistical data, 80-81

INDEX

- Unix intrusion and, 129, 131-133, 136-140, 143-158
 - Windows intrusion and, 95-99, 102-103, 106-122, 126-127
 - NED (Network Evidence Duplicator)**
 - on ultimate response CD, 502
 - overview, 197-198, 200, 203
 - Netcat**, 451, 457
 - Netscape**, 601-603
 - Netscape/Mozilla**, 288
 - network cable**, 166
 - network connections, current**, 6, 8-9, 49-50
 - network hub/switch**, 166
 - network traffic**
 - accessing, 89, 91, 93
 - collecting and storing, 91
 - nm command**, 314-316, 349, 422
 - nonvolatile data**, 3
 - nonvolatile data analyzation**
 - auditing policy, 36
 - file system time and date stamps, 31, 33, 35
 - IIS logs, 38-41
 - logins history, 37
 - overview, 29
 - registry data, 35-36
 - suspicious files, 42-43
 - system event logs, 37-38
 - system version and patch level, 30-31
 - with Unix live response
 - file system MD5 checksum values*, 61
 - file system time and date stamps*, 59, 61
 - history files*, 67, 69
 - login history*, 62-63
 - overview*, 58
 - suspicious files*, 69
 - syslog logs*, 64-66
 - system version and patch level*, 58
 - user accounts*, 66-67
 - users currently logged on*, 62
 - noncommercial-based forensic duplications**
 - DCFLDD, 195-197
 - DD (data dump)
 - evidence file, creation of*, 188-189, 191-192
 - evidence hard drive, creation of*, 192-193
 - overview*, 187
 - DD Rescue, 193-195
 - NED (Network Evidence Duplicator), 197-200, 203
 - overview, 187
 - NSM (network security monitoring)**, 81
- O**
- objdump command**, 329-335, 352-353, 422-426
 - OllyDbg**, 461, 465, 467, 470, 473, 475
 - open files**, 19, 55-56
 - open source solutions**
 - CF (Compact Flash) cards, 589-591, 593
 - e-mail activity reconstruction
 - AOL*, 289
 - Apple Mail*, 289
 - Lotus Notes*, 288
 - Netscape/Mozilla*, 288
 - Outlook*, 288
 - Outlook Express*, 275, 278-279, 282-283
 - overview*, 275

- file signatures and electronic discovery, 233-235
- metadata collection, 218, 220
- recovering deleted files, 207-208, 210-212, 214
- removing known files, 225, 227, 229-230
- string searching and file fragments, 238, 240-241, 243
- USB memory devices, 578-584
- Web browsing activity reconstruction
 - Galleta*, 268, 270-271
 - overview*, 260
 - Pasco*, 260, 262, 264, 266, 268
- open TCP or UDP ports, 9-10
- operating system installation media, 166
- Outlook, 288
- Outlook Express
 - E-Mail DBX file format, 281-284
 - Folders DBX file format, 277-279
 - overview*, 275
- output, Perl used to format, 632-633
- P**
- packer, identifying, 374, 376
- Palm Debugger
 - forensic acquisition using, 540-544, 549-556
 - PDAs, forensic acquisition of, 556
 - PDAs, forensic analysis of, 556, 558
- Palm IIIc
 - forensic acquisition of, 540-543, 549-555
 - forensic analysis of, 556-558
- Palm m505
 - forensic acquisition of, 517, 520, 524, 530-531
- forensic analysis of, 564, 567, 570
- Paraben's Network Email Examiner, 274
- Paraben's PDA Seizure
 - forensic acquisition using, 532, 536, 540
 - forensic analysis using, 559, 562-563
- Pasco, 260-268
- PDA (Personal Digital Assistant)
 - batteries, changing, 519
 - case background, 515, 517
 - EnCase
 - forensic acquisition using*, 517-519, 522, 529, 531
 - forensic analysis using*, 564, 567, 570
 - HP iPAQ Pocket PC 2003
 - forensic acquisition of*, 531, 536, 539
 - forensic analysis of*, 559-563
 - overview*, 515
- Palm Debugger
 - forensic acquisition using*, 540-544, 549-551-556
 - forensic analysis using*, 556-558
- Palm IIIc
 - forensic acquisition of*, 540-543, 549-555
 - forensic analysis of*, 556-558
- Palm m505
 - forensic acquisition of*, 517, 520, 524, 530-531
 - forensic analysis of*, 564, 567, 570
- Paraben's PDA Seizure
 - forensic acquisition using*, 532, 536, 540
 - forensic analysis using*, 559, 562-563
- pe map command, 426
- PEiD, 448

INDEX

pens, 165

Pepe, Matt, 163

Perl

date problem with Excel, 635-636

input, reading, 625-627

live IR data, processing, 634-635

output, formatting, 632-633

overview, 625

read-only files, 627

regular expressions, 629-631

text, matching, 628

pillage, 83

POP-based e-mail, 604-605

Postgres, importing TLD Zone files into,
610-615

power extension cords, 165

power strip, 166

proc file system, 371, 373

ProcDump, 459-460

process memory dumps, 20-25

processes, running, 53, 55

Prosis, Chris, 163, 397, 404

Q-R

read-only files in Perl, 627

read-only IDE to Firewire device, 172-175

readelf command, 318-329, 350-352

reconnaissance, 83

Red Cliff Consulting, 504

registry data, 35-36

Registry Monitor, 443

regular expressions, 629-631

reinforcement, 83

remote forensic duplication, 198

running processes, 15, 17

running services, 17-18

S

sak.exe file analysis

dynamic analysis of

OllyDbg, 461, 465, 467, 470, 473, 475

overview, 457, 477, 479

ProcDump, 459-460

Strace, 457-458

overview, 444

static analysis of

hexadecimal viewer, 446-447

IDA, 452, 456-457

md5sum command, 445, 450

overview, 444

PEiD, 448

strings command, 445-446, 450-451

UnFSG, 449

virus scan, 444

scheduled jobs, 18

screwdriver, 164

screws, extra, 164

SCSI cables, 165

SCSI terminators, 165

session data

NSM collection of, 85-86

overview, 78-79

tools for, 92

shared libraries, 304

Skoudis, Ed, 53

“The Sleuth Kit” (Carrier), 209-210

SMB (Server Message Block), 112

Snort, 93

Unix intrusion, 131, 133, 135, 138

- Windows intrusion, 98-99, 102, 104, 106, 110
- standard intrusion, 82**
- statistical data**
 - NSM collection of, 88
 - overview, 80-81
 - tools for, 93
- Stevens, Richard, 76**
- strace command, 336-337, 353-357**
- string searching and file fragments**
 - commercial solutions, 244, 246
 - open source solutions, 238, 240-241, 243
 - overview, 238
- strings -a command, 347-348**
- strings command, 307-311, 418, 420, 445-446, 450-451**
- suspicious files, 42-43, 69**
- symbols, 304**
- syslog logs, 64-66**
- system date and time, 6, 49**
- system event logs, 37-38**
- system version and patch level, 30-31, 58**
- system worksheets, 167**
- T**
 - The Tao of Network Security*
 - Monitoring: Beyond Intrusion*
 - Detection* (Bejtlich), 88
 - TCP/UDP ports, 50-53
 - Tcpdstat, 93
 - Tcpdump
 - overview, 91
 - Windows intrusion, 95, 97, 106-107
 - Tcpflow
 - overview, 93
 - Unix intrusion, 142-143
 - Windows intrusion, 116-117, 119
 - Tcptrace
 - overview, 92
 - Unix intrusion, 137, 139
 - text, matching, 628**
 - tool kit used for forensic duplication, 164**
 - anti-static bags, 165
 - blank CD-R/DVD-R, 165
 - blank floppies, 166
 - boot disks, 165
 - cable ties, 165
 - chain of custody forms, 165
 - digital camera, 164
 - dremel tool, 164
 - 80 pin IDE cables, 165
 - evidence envelopes, 165
 - evidence hard drives, 165
 - evidence labels, 165
 - evidence tape, 165
 - flashlight, 164
 - forensic software dongles, 166
 - 40 pin IDE cables, 165
 - jumpers, extra, 164
 - network cable, 166
 - network hub/switch, 166
 - operating system installation media, 166
 - pens, 165
 - power extension cords, 165
 - power strip, 166
 - screwdriver, 164
 - screws, extra, 164
 - SCSI cables, 165
 - SCSI terminators, 165

INDEX

U**ultimate response CD**

- DCFLDD on, 501-502
- forensic duplication tools, 501-502
- NED on, 502
- overview, 483
- Unix live response toolkit, 492-497, 500
- Windows live response toolkit, 483-484, 488-492

unauthorized intrusion, determination of, 43**UnFSG, 449****uninstallation registry entries, 293****Unix live response**

- intruder, detection of, 70
- nonvolatile data analysis
 - file system MD5 checksum values, 61*
 - file system time and date stamps, 59, 61*
 - history files, 67, 69*
 - login history, 62-63*
 - overview, 58*
 - suspicious files, 69*
 - syslog logs, 64-66*
 - system version and patch level, 58*
 - user accounts, 66-67*
 - users currently logged on, 62*
- overview, 47
- toolkit, 492, 494-495, 497, 500
- volatile data analysis
 - internal routing table, 56*
 - loaded kernel modules, 57*
 - mounted file systems, 57*
 - network connections, current, 49-50*
 - open files, 55-56*

- overview, 48*
- running processes, 53, 55*
- system date and time, 49*
- TCP/UDP ports, 51-53*

USB memory devices

- content analysis
 - overview, 577*
 - with commercial solutions, 585, 588*
 - with open source solutions, 578-584*
- duplication of, 571-575
- user accounts, 38, 66-67
- users currently logged on, 13-14, 62

V**Venema, Wietse, 209****virus scan, 444****Visual C++ Toolkit 2003, 410****volatile data, 3****volatile data analysis**

- cached NetBIOS name tables, 13
- executables opening TCP or UDP ports, 10-12
- full system memory dumps, 26-27, 29
- internal routing table, 14-15
- network connections, current, 6, 8-9
- open files, 19
- open TCP or UDP ports, 9-10
- overview, 5-6
- process memory dumps, 20-25
- running processes, 15, 17
- running services, 17-18
- scheduled jobs, 18
- system date and time, 6
- users currently logged on, 13-14
- with Unix live response
 - internal routing table, 56*

loaded kernel modules, 57
mounted file systems, 57
network connections, current, 49-50
open files, 55-56
overview, 48
running processes, 53, 55
system date and time, 49
TCP/UDP ports, 51-53

W

Web browsing activity reconstruction

commercial forensic tools, 248, 251, 254, 257
with EnCase, 248-249, 251-252
with FTK, 252, 257
with IE History, 259
open source solutions
 Galleta, 268, 270-271
 overview, 260
 Pasco, 260-268
overview, 247

Windows based analysis of “Hello World”

program, 410, 413
dynamic analysis of, 438
 debuggers, 440-441
 Registry Monitor, 443
 Strace, 439
static analysis of, 418
 file command, 418
 hexadecimal viewer, 420-422
 IDA, 434, 438
 link command, 429, 434
 md5sum command, 418
 nm command, 422

objdump command, 422-423, 425-426
pe map command, 426
strings command, 418, 420

Windows based platform, forensic tool analysis on

case background, 409
“Hello World” program, examining, 410, 413
 dynamic analysis of, 438-443
 static analysis of, 418, 420-426, 429, 434, 438
overview, 409
sak.exe file
 dynamic analysis of, 457-461, 465, 467, 470, 473-479
 overview, 444
 static analysis of, 444-452, 456-457

Windows live response

nonvolatile data analyzation
 auditing policy, 36
 file system time and date stamps, 31, 33, 35
 IIS logs, 38-41
 logins history, 37
 overview, 29
 registry data, 35-36
 suspicious files, 42-43
 system event logs, 37-38
 system version and patch level, 30-31
 user accounts, 38
overview, 3, 5
unauthorized intrusion, determination of, 43
volatile data analyzation
 cached NetBIOS name tables, 13

INDEX

executables opening TCP or UDP ports,
10-12
full system memory dumps, 26-27, 29
internal routing table, 14-15
network connections, current, 6, 8-9
open files, 19
open TCP or UDP ports, 9-10
overview, 5-6
process memory dumps, 20-25
running processes, 15, 17
running services, 17-18
scheduled jobs, 18
system date and time, 6
toolkit, 83-484, 488-492
users currently logged on, 13-14

Windump, 92

worksteets, 167, 168

X-Z

Yahoo!, 600-601

Yuschuk, Oleh, 440

Zbikowski, Mark, 446