INDEX

Numerals

6to4 (IPv6 over IPv4) protocol, 143
48-port Ethernet switches, 12
802.11 packet structure
  beacon packets, 304–305
  control packets, 304
  data packets, 304
  management packets, 304

A

AA (Authoritative Answers) field (DNS packets), 173
absolute timestamps, 114
accessibility and connectivity problems
  gateway configuration, 210–213
  troubleshooting, 222–226
  unwanted redirection, 213–216
  upstream problems, 216–219
Acknowledgment Number field (TCP headers), 152
ACK packets
  client latency and, 250
  DHCP initialization process, 169–170
  duplicate, 236–239, 247
  server latency and, 250
  TCP retransmissions, 232–233
  TCP teardown, 158–159
  wire latency and, 249
active fingerprinting, 266
Additional Information Section field (DNS packets), 174
Additional Records Count field (DNS packets), 174
Address Resolution Protocol. *See* ARP
Ad hoc wireless card mode, 298, 299
Advanced preferences (Wireshark), 47
AfriNIC, 82
aggregated network taps, 25
AirPcap
  capturing traffic with, 302
  configuring, 300–301
ALFA network, 300
American Registry for Internet Numbers (ARIN), 81, 82
analysis step (in packet-sniffing process), 4
Answer Count field (DNS packets), 174
Answers Section field (DNS packets), 174
APNIC, 82
Appearance preferences (Wireshark), 46
application baseline, 254–255
Application layer (OSI model), 5
application protocols, 2
ARIN (American Registry for Internet Numbers), 81, 82
ARP (Address Resolution Protocol), 4, 120–121
  cache poisoning, 27–28, 34
    Cain & Abel security tool, 28–31
    traffic manipulation, 267–271
  gratuitous ARP, 124–125
  packet structure, 121–122
  requests, 122–123
  responses, 123, 269
ASCII output, 111
ASN (Autonomous System Number), 207
associations/dependencies, 254
asymmetric routing, 31
attachments, sending via SMTP, 196–198
authentication sequences
  host baseline, 254
  site baseline, 253
Authoritative Answers (AA) field (DNS packets), 173
Authority Section field (DNS packets), 174
Autonomous System Number (ASN), 207
AXFR (full zone transfer), 181

B

basic service set identifier (BSS ID), 307
BE (big-endian) format, 146
beacon packets, 304–305
Berkeley Packet Filter (BPF) syntax, 66–67
big-endian (BE) format, 146
binary system, 326
Blink Led option (AirPcap), 300
Boot File field (DHCP packets), 165
BPF (Berkeley Packet Filter) syntax, 66–67
BPF capture filters, 113–114
broadcast domains, 15–16

broadcast packets, 15–16
broadcast traffic, 15–16
  host baseline, 253
  site baseline, 252
BSS ID (basic service set identifier), 307

C

C2 (command and control) behavior (malware), 290–291
cache poisoning (ARP spoofing), 27–28, 34
  Cain & Abel security tool, 28–31
  traffic manipulation, 267–271
Cain & Abel security tool, 28–31, 319
CAM (Content Addressable Memory) tables, 12, 120
CAPSCREEN command, 284–285
CapTipper tool, 320
capture files, 53
  merging, 55–56
  saving and exporting, 54–55
capture filters, 65–66
  addressing, 67–68
  BPF, 66–67, 113–114
  command line tools and, 113
  commonly used, 70–71
  hostname, 67–68
  port filters, 68
  protocol field filters, 69–70
  protocol filters, 69
Capture Interfaces dialog (Wireshark), 61–65
  Input tab, 61–62
  Options tab, 63
    Display Options section, 64
    Name Resolution section, 64
    Stop capture section, 65
  Output tab, 62–63
capture packets, 56–58
  Capture Interfaces dialog (Wireshark), 61–65
  command line tools and, 106–108
  finding packets, 56–57
  marking packets, 57
  packet time referencing, 60
  printing packets, 58
  time display formats, 59
  time shifting, 60–61
Capture preferences (Wireshark), 47
Capture Type options (AirPcap), 301
-c argument (command line tools), 108
CDNs (content delivery networks), 201
Chanalyzer software, 298
Channel column (Wireshark Packet List pane), 306
channel hopping technique, 297
Channel option (AirPcap), 300
channels
  defined, 296
  signal interference, 297–298
  sniffing, 296–297
Chat messages (Wireshark), 100, 101
Checksum field
  ICMP headers, 144
  TCP headers, 152
  UDP headers, 161
Cisco port mirroring commands, 22
Classless Inter-Domain Routing (CIDR) notation, 127
Client Hardware Address field (DHCP packets), 165
Client Identifier option (DHCP discover packets), 167
Client IP Address field (DHCP packets), 165
client latency, 249–250
CloudShark tool, 317–318
Code field (ICMP headers), 144
collection step (in packet-sniffing process), 3
Coloring Rules window (Wireshark), 48–49
Combs, Gerald, 37
command and control (C2) behavior (malware), 290–291
command line tools, 103–104
  tcpdump
    capturing and saving packets, 106–108
    compared to TShark, 118
    filters, 113–114
    installing, 105
    manipulating output, 109–111
    name resolution, 111–112
  TShark
    capturing and saving packets, 106–108
    compared to tcpdump, 118
    filters, 113–114
    installing, 104
    manipulating output, 109–111
    name resolution, 111–112
    summary statistics, 115–118
    time display formats, 114–115
comma-separated value (CSV) files, 226–230
comparison operators (Wireshark filter expression), 73
computer communication
  network hardware, 10–14
    hubs, 10–11
    routers, 13–14
    switches, 11–12
  network traffic, 15–16
    broadcast, 15–16
    multicast, 16
    unicast, 16

OSI model, 5–10
data encapsulation, 8–10
data flow through, 7
protocols, 4–5
configuration files (Wireshark), 50
Configuration Profiles window (Wireshark), 50–52
connectionless protocols, 160–161. *See also* UDP
connection-oriented protocols, 151. *See also* TCP
connectivity problems. *See* accessibility and connectivity problems
Content Addressable Memory (CAM) tables, 12, 120
content delivery networks (CDNs), 201
control packets, 304
conversations
defined, 78
identifying top talkers with, 80–83
viewing, 79–80
Conversations window (Wireshark)
finding open ports with, 262
TCP communications, 260
conversion step (in packet-sniffing process), 4
Cookie Manager plugin, 273
cost
of packet sniffers, 3
of Wireshark, 38
CryptoLocker malware, 291
CryptoWall malware, 289–290, 294
CSV (comma-separated value) files, 226–230
CyberEYE, 281

D

Damn Vulnerable Web Application (DVWA), 272
`-D` argument (command line tools), 107
data encapsulation (OSI model), 7–10
Data field (IPv4 headers), 127
Data link layer (OSI model), 6
data packets, 304
Data Rate column (Wireshark Packet List pane), 306
data representation (packets), 326–328
data transfer
application baseline, 255
site baseline, 253
through OSI model, 7
Decode As... dialog (Wireshark), 89–90
denial-of-service (DoS) attacks, 28, 31
Destination IP Address field
IPv4 headers, 127
IPv6 headers, 136
destination port (TCP), 152–153
Destination Port field
TCP headers, 152
UDP headers, 161
DHCP (Dynamic Host Configuration Protocol), 4, 163–164
DHCPv6, 171–173
initialization process, 165
acknowledgment packets, 169–170
discover packets, 165–167
offer packets, 167–168
request packets, 168–169
in-lease renewal, 170
message types, 171
options, 170–171
packet structure, 164–165
DHCPv6, 171–173
direct install method, 33, 34
discarding (dropping) packets, 11
discover packets (DHCP initialization process), 165–167
Display filter option (Wireshark), 57
display filters, 71–74, 113
DNS (Domain Name System)
packet structure, 173–174
query, 174–176
question types, 176–177
recursion, 177–180
zone transfers, 181–183
DORA process (DHCP), 165
acknowledgment packets, 169–170
discover packets, 165–167
offer packets, 167–168
request packets, 168–169
DoS (denial-of-service) attacks, 28, 31
dotted-quad (dotted-decimal) notation (IPv4 addresses), 125
double-headed packets (ICMP), 148
dropping (discarding) packets, 11
Duncan, Brad, 322
duplicate acknowledgments (TCP), 235–240
duplicate ACK packets, 236–239, 247
DVWA (Damn Vulnerable Web Application), 272
Dynamic Host Configuration Protocol. *See* DHCP

E

EAPoL (Extensible Authentication Protocol over LAN) packets, 314
echo request packets (ICMP), 145–147
email. *See* SMTP
encapsulation, 8–10, 143
endpoints
defined, 78
identifying top talkers with, 80–83
viewing statistics, 78–79

Enterasys router, 13, 22
enterprise-grade fiber optic taps, 27
ephemeral port group, 153
Error messages (Wireshark), 100, 101
error-recovery features (TCP)
  duplicate acknowledgments, 235–240
  retransmissions, 232–235
ESMTP (Extended SMTP), 190
ESSID (extended service set ID), 303
Ethereal application, 37–38
Ethernet taps, 27
expert information (Wireshark), 99–101
  Chat messages, 100, 101
  Error messages, 100, 101
  Note messages, 100, 101
  Warning messages, 100, 101
exploit kits, 294
exporting
  capture files, 54–55
  endpoint address into colorization rule, 79
Export Specified Packets dialog (Wireshark), 55
expressions, 66. *See also* capture filters
extended service set ID (ESSID), 303
Extended SMTP (ESMTP), 190
Extensible Authentication Protocol over LAN (EAPoL) packets, 314
Extension Channel option (AirPcap), 301

F

fail-open capability (network taps), 27
`-f` argument (command line tools), 113
fast retransmission packets, 236–237
FCS Filter option (AirPcap), 301
FIFO (first in, first out) method, 63
file carving process, 287
file formats (Wireshark), 54
file sets, 63
Filter Expressions preferences (Wireshark), 47
filters
  adding to toolbar, 75–76
  capture filters, 65–71
  display filters, 71–74, 113
  saving, 74–75
  tcpdump, 113–114
  TShark, 113–114
  wireless-specific, 307–308
    filtering specific frequency, 308
    filtering specific wireless packet types, 307–308
    filtering traffic for BSS ID, 307
finding packets, 56–57
Find Packet bar (Wireshark), 56–57
first in, first out (FIFO) method, 63
flags, 329
Flags field
  DHCP packets, 164
  IPv4 headers, 127
  TCP headers, 152
flow control features (TCP), 240
  adjusting window size, 241–242
  sliding window, 243–247
  zero window notification, 242–243
flow graphing, 99
Flow Label field (IPv6 headers), 136
footprinting
  operating system fingerprinting, 263–266
    active fingerprinting, 266
    passive fingerprinting, 263–266
  SYN scan, 258–262
    identifying open and closed ports, 262
    using filters with, 260–262
forced decodes (Wireshark), 88–90
fragmentation (IPv6), 141–143
Fragment Offset field (IPv4 headers), 127
full-duplex devices (switches), 11–12
full zone transfer (AXFR), 181

G

gateway configuration problems, 210–213
  analysis, 210–212
  conclusions, 212–213
  tapping into the wire, 210
Gateway IP Address field (DHCP packets), 165
`GET` requests (HTTP), 184, 187, 208–209, 249–250, 275–276, 280
GNU Public License (GPL), 37, 38
graphing
  flow, 99
  IO graphs, 95–98
  round-trip time, 98–99
gratuitous ARP, 124–125

H

half-duplex mode (hubs), 10
half-open scan (SYN scan), 258–262
  identifying open and closed ports, 262
  using filters with, 260–262
handshakes (TCP), 155–158
Hardware Address Length field (ARP headers), 121
Hardware Length field (DHCP packets), 164
Hardware Type field
  ARP headers, 121
  DHCP packets, 164

`-h` argument (command line tools), 104
Header Checksum field (IPv4 headers), 127
Header Length field (IPv4 headers), 127
help resources, 321–323
  Brad Duncan's Malware Traffic Analysis site, 322
  Chris Sanders's Blog, 322
  Internet Assigned Numbers Authority, 323
  Practical Packet Analysis online course, 322
  SANS SEC503: Intrusion Detection In-Depth course, 322
  The TCP/IP Guide, 323
  Wireshark's Home Page, 322
  W. Richard Stevens's *TCP/IP Illustrated* series, 323
hexadecimal system, 111, 326
Hex value option (Wireshark), 57
higher-order nibble, 326
high latency
  defined, 232
  locating source of, 248–251
Hop Limit field (IPv6 headers), 136
Hops field (DHCP packets), 164
host baseline, 253–254
hostname (capture filters), 67–68
host portion (interface identifier), 126, 134
hosts file, 86–87, 215–216
Host to Host encapsulation, 143
Host to Router encapsulation, 143
hping tool, 321
HTTP (Hypertext Transfer Protocol), 8–9
  browsing with, 183–186
  `GET` requests, 184, 187, 208–209, 249–250, 275–276, 280
  posting data with, 186–187
  `<script>` tags, 278
  session hijacking attacks, 271–275
  `<span>` tags, 279
  streams, 91
hubbing out, 23–24, 33
hub networks, 19–20
hubs, 10–11, 24
Hypertext Transfer Protocol. *See* HTTP

I

IANA (Internet Assigned Numbers Authority), 323
`-i` argument (command line tools), 107
ICMP (Internet Control Message Protocol), 144–150
  ICMPv6, 150
  packet structure, 144
  requests and responses, 145–147
  traceroute utility, 147–150
  types and messages, 144
ICMP protocol dissector, 88
ICMP version 6 (ICMPv6), 150
ICS (Industrial Control System) networks, 330
Identification field (IPv4 headers), 127
IDS (intrusion-detection system), 258
IETF (Internet Engineering Task Force), 120
`ifconfig` command, 107
`<iframe>` tags, 279
IMAP (Internet Message Access Protocol), 195
Include 802.11 FCS in Frames option (AirPcap), 301
incremental zone transfer (IXFR), 181
Industrial Control System (ICS) networks, 330
infrastructure problems, 222
  analysis, 223–226
  conclusions, 226
  tapping into the wire, 223
initialization process (DHCP), 165
  acknowledgment packets, 169–170
  discover packets, 165–167
  offer packets, 167–168
  request packets, 168–169
initial sequence number (ISN), 236
in-lease renewal (DHCP), 170
installing
  tcpdump, 105
  TShark, 104
  Wireshark
    on Linux systems, 41–43
    on OS X systems, 43
    on Windows systems, 39–41
interface identifier (host portion), 126, 134
Interface option (AirPcap), 300
internet accessibility and connectivity problems
  gateway configuration problems, 210–213
  troubleshooting, 222–226
  unwanted redirection, 213–216
  upstream problems, 216–219
Internet Assigned Numbers Authority (IANA), 323
Internet Control Message Protocol. *See* ICMP
Internet Engineering Task Force (IETF), 120
Internet Message Access Protocol (IMAP), 195
Internet of Things (IoT) devices, 210
Internet Protocol addresses. *See* IP addresses
Internet Society (ISOC), 120
intrusion-detection system (IDS), 258

IO graphs, 95–98
IoT (Internet of Things) devices, 210
IP addresses
  determining ownership of, 82
  hostnames, 67–68
  IPv4, 125–127
  IPv6, 133–135
IPv4 (Internet Protocol version 4), 4, 125–132, 328–329
  addresses, 125–127
  packet fragmentation, 130–132
  packet structure, 127–128
  Time to Live value, 128–130
IPv6 (Internet Protocol version 6), 4, 133–143
  addresses, 133–135
  fragmentation, 141–143
  neighbor solicitation, 138–141
  packet structure, 135–138
  transitional protocols, 143
IPv6 over IPv4 (6to4) protocol, 143
ISATAP protocol, 143
ISN (initial sequence number), 236
ISOC (Internet Society), 120
`iwconfig` command (Linux), 303–304
IXFR (incremental zone transfer), 181

K

keep-alive packets, 242, 246, 247
Kismet tool, 297
kit's landing page, 294
Kozierok, Charles, 323

L

LANs (local area networks), 125
latency, 231
  locating source of high
    client latency, 249–250
    latency locating framework, 251
    normal communications, 248
    server latency, 250–251
    wire latency, 248–249
  network baselining, 251–255
    application baseline, 254–255
    host baseline, 253–254
    site baseline, 252–253
  TCP error-recovery features, 232–240
  TCP flow control, 240–247
  troubleshooting, 247
layer 7 (upper-layer) protocols
  DHCP, 163–173
    DHCPv6, 171–173
    initialization process, 165–170
    in-lease renewal, 170
    message types, 171
    options, 170–171
    packet structure, 164–165
  DNS, 173–183
    packet structure, 173–174
    query, 174–176
    question types, 176–177
    recursion, 177–180
    zone transfers, 181–183
  HTTP, 183–187
    browsing with, 183–186
    posting data with, 186–187
  SMTP, 187–198
    sending and receiving email, 188–189
    sending attachments via, 196–198
    tracking email messages, 189–196
LE (little-endian) format, 146
libpcap tool, 321
link-local addresses (IPv6), 134
Linux
  `ifconfig` command, 107
  installing Wireshark, 41–43
    compiling from source, 42–43
    DEB-based systems, 42
    RPM-based systems, 41
  sniffing wirelessly, 303–304
little-endian (LE) format, 146
local area networks (LANs), 125
logical operators, 67, 74
lower-order nibble, 326
low latency, 232

M

MAC (Media Access Control) addresses, 11, 134
MAC Address Scanner dialog box (Cain & Abel tool), 29
mail delivery agent (MDA), 189
mail submission agent (MSA), 189
mail transfer agent (MTA), 188–189
mail user agent (MUA), 188
main window (Wireshark), 45–46
malware
  Brad Duncan's Malware Traffic Analysis site, 322
  Operation Aurora, 275–281
  remote-access trojans, 281–288
Malware Traffic Analysis (MTA) site, 322
managed switches, 12
Managed wireless card mode, 298, 299
management packets, 304
man-in-the-middle (MITM) attacks, 267, 270
marking packets, 57
Master wireless card mode, 298, 299

Maximum concurrent requests option (Wireshark), 85
maximum transmission unit (MTU), 130
MDA (mail delivery agent), 189
Media Access Control (MAC) addresses, 11, 134
merging capture files, 55–56
messages
  ICMP, 144
  Wireshark, 100–101
Message Type options (DHCP discover packets), 167, 171
message types (DHCP), 171
MetaGeek spectrum analyzer, 297–298
missing web content, 200–205
  analysis, 201–204
  conclusions, 204–205
  tapping into the wire, 200
MITM (man-in-the-middle) attacks, 267, 270
Modbus protocol, 330–331
Monitor (RFMON) wireless card mode, 298, 299
More fragments offset value (IP fragmentation), 131–132
MSA (mail submission agent), 189
MTA (mail transfer agent), 188–189
MTA (Malware Traffic Analysis) site, 322
MTU (maximum transmission unit), 130
MTU discovery process, 141–142
MUA (mail user agent), 188
multicast traffic, 16
mystery packets, 330–332

N

name resolution (name lookup)
  enabling, 84–86
  hosts file, 86–87
  manually initiated, 88
  potential drawbacks to, 86
  tcpdump, 111–112
  TShark, 111–112
Name Resolution preferences (Wireshark), 47, 84–88
Name Server (Authority) Record Count field (DNS packets), 174
`-n` argument (command line tools), 112
`-N` argument (command line tools), 112
navigating packets, 325
  data representation, 326–328
  mystery packets, 330–332
  packet diagrams, 328–330
Neighbor Advertisement packets, 140
Neighbor Discovery Protocol (NDP), 139
neighbor solicitation (IPv6), 138–141
NETGEAR hubs, 10
netmask (network mask), 126
network baselining, 251
  application baseline, 254–255
  host baseline, 253–254
  site baseline, 252–253
network diagrams (network maps), 33
network hardware, 10–14
  hubs, 10–11
  routers, 13–14
  switches, 11–12
network interface cards (NICs), 18–19, 298–299
Network layer (OSI model), 6
network layer protocols, 2, 119
  ARP, 120–121
    gratuitous ARP, 124–125
    packet structure, 121–122
    requests, 122–123
    responses, 123
  ICMP, 144–150
    ICMPv6, 150
    packet structure, 144
    requests and responses, 145–147
    traceroute utility, 147–150
    types and messages, 144
  IP, 125–143
    IPv4, 125–132
    IPv6, 133–143
network maps (network diagrams), 33
network mask (netmask), 126
NetworkMiner tool, 319–320
network portion (network prefix), 126, 134
network taps, 24–27, 34
Network Time Protocol (NTP), 60
network traffic, 15–16
  broadcast, 15–16, 252–253
  multicast, 16
  unicast, 16
Next Header field (IPv6 headers), 136
ngrep tool, 321
nibbles, 326
NICs (network interface cards), 18–19, 298–299
Nmap tool, 260, 266
nonaggregated network taps, 25–27
Nortel, 22
Note messages (Wireshark), 100, 101
Npcap tool, 321
NTP (Network Time Protocol), 60

O

offer packets (DHCP initialization process), 167–168
OmniPeek, 2
Only use the profile "hosts" file option (Wireshark), 86

OpCode field
 DHCP packets, 164
 DNS packets, 173
Open Systems Interconnections model. *See* OSI model
operating system fingerprinting
 active fingerprinting, 266
 passive fingerprinting, 263–266
operating system support
 command line tools, 118
 Wireshark, 39
Operation Aurora, 275–281
Operation field (ARP headers), 121
Options field
 DHCP packets, 165
 IPv4 headers, 127
 TCP headers, 152
OSI (Open Systems Interconnections) model, 5
 data encapsulation, 7–10
 data flow through, 7
OS X
 `ifconfig` command, 107
 installing Wireshark on, 43
output (of command line tools), 109–111

P

packet analysis, 1–2
 computer communication, 4–14
  network hardware, 10–14
  network traffic, 15–16
  OSI model, 5–10
  protocols, 4–5
 packet sniffers, 2–4
Packet Bytes pane (Wireshark), 45, 46, 111
packet capture, 44–45
packet color coding, 48–49
Packet Details pane (Wireshark), 45, 46, 238
packet diagrams, 328–330
packet fragmentation (IPv4), 130–132
Packet Length field (UDP headers), 161
packet lengths, 93–94
Packet List pane (Wireshark), 45, 46
 adding wireless-specific columns to, 305–306
 retransmission packets, 239
packet sniffers, 2–4. *See also* sniffer placement
 evaluating, 2–3
 packet-sniffing process, 3–4
  analysis, 4
  collection, 3
  conversion, 4
packet structure
 802.11, 304–305
 ARP, 121–122
 DHCP, 164–165
 DNS, 173–174
 ICMP, 144
 IPv4, 127–128
 IPv6, 135–138
 TCP, 152
 UDP, 161
packet time referencing, 60
packet transcript, 91
Parameter Request List option (DHCP discover packets), 167
passive fingerprinting, 263–266
Payload Length field (IPv6 headers), 136
.pcapng file format, 54
PDUs (protocol data units), 8
Physical layer (OSI model), 6
physical transmission medium (wireless packet analysis), 296–298
 signal interference, 297–298
 sniffing channels, 296–297
ping utility, 145–146
POP3 (Post Office Protocol version 3), 195
port filters, 68
port mirroring (port spanning), 21–22, 33
ports
 SYN scan, 258–262
 TCP, 152–155
posting data with HTTP, 186–187
Post Office Protocol version 3 (POP3), 195
Practical Packet Analysis online course, 322
preferences management (Wireshark), 46–47, 84–86
Presentation layer (OSI model), 5
primitives, 66
printing
 capture packets, 58
 printer problems, 219–222
program support (Wireshark), 39
promiscuous mode, 3, 18–19
Protocol Address Length field (ARP headers), 121
protocol data units (PDUs), 8
protocol dissectors, 88–91, 327
 changing, 88–90
 viewing source code, 90–91
Protocol field (IPv4 headers), 127
protocol field filters, 69–70
protocol filters, 69
Protocol Hierarchy Statistics window (Wireshark), 83–84
 application baseline, 254
 host baseline, 253
 site baseline, 252
protocols, 4–5. *See also names of specific protocols*
 application, 2
 Modbus, 330–331

OSI model, 6–7
Wireshark, 38
Protocols preferences (Wireshark), 47
protocol stack, 4
protocol support (command line tools), 118
Protocol Type field (ARP headers), 121
Python tool, 321

Q

QR (Query/Response) field (DNS packets), 173
qualifiers (BPF syntax), 66
queries (DNS), 174–176
Query/Response (QR) field (DNS packets), 173
Question Count field (DNS packets), 174
Questions Section field (DNS packets), 174
question types (DNS), 176–177

R

RA (Recursion Available) field (DNS packets), 173
ransomware, 288–294
-r argument (command line tools), 108
RAT (remote-access trojans), 281–288
RCode (Response Code) field (DNS packets), 174
RD (Recursion Desired) field (DNS packets), 173
receive window (server), 241–243
reconnaissance. *See* footprinting
recursion (DNS), 177–180
Recursion Available (RA) field (DNS packets), 173
Recursion Desired (RD) field (DNS packets), 173
relative timestamps, 114
remote-access trojans (RAT), 281–288
repeating devices (hubs), 10
Requested IP Address option (DHCP discover packets), 167
request packets
ARP, 122–123, 269
DHCP initialization process, 168–169
ICMP, 145–147
Reserved (Z) field (DNS packets), 174
resets (TCP), 159–160
Resolve MAC addresses option (Wireshark), 84
Resolve network (IP) addresses option (Wireshark), 85
Resolve transport names option (Wireshark), 85
Response Code (RCode) field (DNS packets), 174
response packets
ARP, 123, 269
ICMP, 145–147
retransmission packets, 247
retransmissions (TCP), 232–235
retransmission timeout (RTO), 232–235
retransmission timer, 232
RFMON (Monitor) wireless card mode, 298, 299
ring buffer, 63
RIPE, 82
RJ-45 ports (hubs), 10
Robtex, 82
round-trip time (RTT), 98–99, 145, 232
routed environment, 31–32
routers, 13–14
Router to Router encapsulation, 143
RST packets, 159–160
RTO (retransmission timeout), 232–235
RTT (round-trip time), 98–99, 145, 232

S

SANS SEC503: Intrusion Detection In-Depth course, 322
SARR process (DHCPv6), 172–173
saving
capture files, 54–55
filters, 74–75
packets, 106–108
wireless profile, 309
scanning techniques, 258–262
Scapy tool, 319
<script> tags (HTML), 278
Seconds Elapsed field (DHCP packets), 164
Secure Socket Layer (SSL) protocol, 88
security, 257–258
exploit kit, 294
footprinting
operating system fingerprinting, 263–266
SYN scan, 258–262
malware
Operation Aurora, 275–281
remote-access trojans, 281–288
ransomware, 288–294
traffic manipulation, 266
ARP cache poisoning, 267–271
session hijacking, 271–275
wireless
WEP authentication, 309–312
WPA authentication, 312–314
Sender Hardware Address field (ARP headers), 122
Sender Protocol Address field (ARP headers), 122
Sequence Number field (TCP headers), 152

Server Host Name field
(DHCP packets), 165
Server IP Address field (DHCP packets), 165
server latency, 250–251
session hijacking, 271–275
Session layer (OSI model), 5
Sguil tool, 288–289
signal interference, 297–298
Signal Strength column (Wireshark Packet List pane), 306
Simple Mail Transfer Protocol. *See* SMTP
site baseline, 252–253
sliding-window mechanism (TCP), 240–241, 243–247. *See also* flow control features
slow networks, 231
locating source of high latency
client latency, 249–250
latency locating framework, 251
normal communications, 248
server latency, 250–251
wire latency, 248–249
network baselining, 251
application baseline, 254–255
host baseline, 253–254
site baseline, 252–253
TCP error-recovery features, 232–240
TCP flow control, 240–247
troubleshooting, 247
small office and home office (SOHO) switches, 22
SMTP (Simple Mail Transfer Protocol), 187–198
sending and receiving email, 188–189
sending attachments via, 196–198
tracking email messages, 189–196
sniffer placement, 17. *See also* tapping into the wire
determining best method, 35
hub network, 19–20
promiscuous mode, 18–19
routed environment, 31–32
switched environment, 20–31, 33–34
ARP cache poisoning, 27–31, 34
direct install method, 33, 34
hubbing out, 23–24, 33
network taps, 24–27, 34
port mirroring, 21–22, 33
Sniffer tab (Cain & Abel tool), 28–29
sniffing wirelessly
in Linux, 303–304
sniffing channels, 296–297
in Windows, 300–302
Snort alert, 281–282
software data corruption, 226–230
analysis, 226–230
conclusions, 230
tapping into the wire, 226
SOHO (small office and home office) switches, 22
source code access
packet sniffers, 3
Wireshark, 39
Source IP Address field
IPv4 headers, 127
IPv6 headers, 136
source port (TCP), 152–153
Source Port field
TCP headers, 152
UDP headers, 161
<span> tags (HTML), 279
Spanning Tree Protocol (STP), 84
spear phishing, 275
spectrum analyzer, 297–298
SSL (Secure Socket Layer) protocol, 88
SSL streams
defined, 91
following, 92–93
standard port (system port group), 153
startup/shutdown
application baseline, 254
host baseline, 253
Statistics preferences (Wireshark), 47
stealth scan (SYN scan), 258–262
identifying open and closed ports, 262
using filters with, 260–262
Stevens, W. Richard, 323
STP (Spanning Tree Protocol), 84
stream following, 91–93
String option (Wireshark), 57
subnet mask (network mask), 126
summary statistics (TShark), 115–118
switched environment, sniffing in, 20–31, 33–34
ARP cache poisoning, 27–31, 34
direct install method, 33, 34
hubbing out, 23–24, 33
network taps, 24–27, 34
port mirroring, 21–22, 33
switches, 11–12
SYN scan, 258–262
identifying open and closed ports, 262
using filters with, 260–262
system port group (standard port; well-known port group), 153

T

tapping into the wire, 17. *See also* sniffer placement
determining best method, 35
gateway configuration problems, 210
hub network, 19–20
infrastructure problems, 223
missing web content, 200

  - printer problems, 219
  - promiscuous mode, 18–19
  - routed environment, 31–32
  - software data corruption, 226
  - switched environment, 20–31, 33–34
    - ARP cache poisoning, 27–31, 34
    - direct install method, 33, 34
    - hubbing out, 23–24, 33
    - network taps, 24–27, 34
    - port mirroring, 21–22, 33
  - unresponsive weather service, 206
  - unwanted redirection, 213
  - upstream problems, 216
- Target Hardware Address field (ARP headers), 122
- Target Protocol Address field (ARP headers), 122
- `-t` argument (command line tools), 114
- TC (Truncation) field (DNS packets), 173
- TCP (Transmission Control Protocol), 4, 109, 151–160
  - buffer space, 240–241
  - error-recovery features
    - duplicate acknowledgments, 235–240
    - retransmissions, 232–235
  - flow control features, 240
    - adjusting window size, 241–242
    - sliding window, 243–247
    - zero window notification, 242–243
  - handshakes, 155–158
  - HTTP protocol and, 9
  - packet structure, 152
  - ports, 152–155
  - resets, 159–160
  - streams, 91
  - teardown process, 158–159
- tcpdump, 2
  - capturing and saving packets, 106–108
  - compared to TShark, 118
  - filters, 113–114
  - installing, 105
  - manipulating output, 109–111
  - name resolution, 111–112
- *The TCP/IP Guide* (Kozierok), 323
- *TCP/IP Illustrated* series (Stevens), 323
- Tcpreplay tool, 319
- TCP SYN scan (SYN scan), 258–262
  - identifying open and closed ports, 262
  - using filters with, 260–262
- teardown process (TCP), 158–159
- Teredo protocol, 143
- Terminal-based Wireshark. *See* TShark
- time display formats
  - capture packets, 59
  - TShark, 114–115
- time shifting (capture packets), 60–61
- Time to Live value. *See* TTL value
- TKIP encryption, 314
- TLS (Transport Layer Security) protocol, 195
- toolbar (Wireshark), adding filters to, 75–76
- tools, 317–321. *See also* command line tools
  - Cain & Abel security tool, 319
  - CapTipper, 320
  - CloudShark, 317–318
  - hping, 321
  - libpcap, 321
  - NetworkMiner, 319–320
  - ngrep, 321
  - Npcap, 321
  - Python, 321
  - Scapy, 319
  - Tcpreplay, 319
  - TraceWrangler, 319
  - WireEdit, 318
- top talkers, 80–83
- Total Length field (IPv4 headers), 127
- traceroute utility (ICMP), 147–150
- TraceWrangler tool, 319
- Traffic Class field (IPv6 headers), 135
- traffic manipulation, 266–275. *See also* network traffic
  - ARP cache poisoning, 267–271
  - session hijacking, 271–275
- Transaction ID field (DHCP packets), 164
- transitional protocols (IPv6), 143
- Transmission Control Protocol. *See* TCP
- Transport layer (OSI model), 5–6
- transport layer protocols. *See also* TCP
  - choosing sniffer, 2
  - UDP, 160–161
- Transport Layer Security (TLS) protocol, 195
- troubleshooting
  - inconsistent printers, 219–222
  - internet accessibility problems, 210–219
  - missing web content, 200–205
  - no branch office connectivity, 222–226
  - slow networks, 247
  - software data corruption, 226–230
  - unresponsive weather service, 205–210
- Truncation (TC) field (DNS packets), 173
- TShark (Terminal-based Wireshark)
  - capturing and saving packets, 106–108
  - compared to tcpdump, 118
  - filters, 113–114
  - installing, 104
  - manipulating output, 109–111
  - name resolution, 111–112
  - summary statistics, 115–118
  - time display formats, 114–115
- TTL (Time to Live) value
  - ICMP packets, 148–149
  - IPv4, 128–130

Type field (ICMP headers), 144
Type of Service field (IPv4 headers), 127

U

Ubuntu 14.04 LTS, 105
UDP (User Datagram Protocol), 109, 160–161
    latency and, 251
    packet structure, 161
    streams, 91
unicast packet, 16
Unix systems
    capturing and saving packets, 106–108
    filters, 113–114
    installing, 105
    manipulating output, 109–111
    name resolution, 111–112
unwanted redirection, 213–216
    analysis, 213–216
    conclusions, 216
    tapping into the wire, 213
upper-layer protocols. *See* layer 7 protocols
upstream problems, 216–219
    analysis, 216–219
    conclusions, 219
    tapping into the wire, 216
Urgent Pointer field (TCP headers), 152
USBPcap, 40–41
Use an external network name resolver option (Wireshark), 85
Use captured DNS packet data for address resolution option (Wireshark), 85
User Datagram Protocol. *See* UDP

V

`-V` argument (command line tools), 109–110
`-v` argument (command line tools), 110
Variable field (ICMP headers), 144
Version field
    IPv4 headers, 127
    IPv6 headers, 135
visibility window
    defined, 19
    on switched network, 21

W

WAN (wide area network) link, 222–223
WAPs (wireless access points)
    802.11 packet structure, 304–305
    basic service set identifier, 307
    filtering traffic for BSS ID, 307
    WEP authentication, 309–312
    wireless NIC modes, 298
    WPA authentication, 312–314
`-w` argument (command line tools), 107–108
Warning messages (Wireshark), 100, 101
weather service, unresponsive, 205–210
    analysis, 206–209
    conclusions, 209–210
    tapping into the wire, 206
well-known port group (system port group), 153
WEP (Wired Equivalent Privacy) authentication, 309–312
WEP Configuration option (AirPcap), 301
WHOIS query, 207
WHOIS registry, 81, 82
wide area network (WAN) link, 222–223
Wi-Fi Protected Access. *See* WPA
Windows
    installing Wireshark, 39–41
    sniffing wirelessly, 300–302
    TShark
        capturing and saving packets, 106–108
        compared to tcpdump, 118
        filters, 113–114
        installing, 104
        manipulating output, 109–111
        name resolution, 111–112
        summary statistics, 115–118
        time display formats, 114–115
    WinDump, 105
Window Size field (TCP headers), 152
WinPcap capture driver, 39
Wired Equivalent Privacy (WEP) authentication, 309–312
WireEdit tool, 318
wire latency, 248–249
wireless access points. *See* WAPs
wireless card modes
    Ad hoc mode, 298, 299
    Managed mode, 298, 299
    Master mode, 298, 299
    Monitor mode, 298, 299
Wireless LAN Statistics window (Wireshark), 302
wireless local area networks (WLANs), 296. *See also* wireless packet analysis
wireless packet analysis
    802.11 packet structure, 304–305
    adding wireless-specific columns to Packet List pane, 305–306
    filters, 307–308
    physical considerations
        signal interference, 297–298
        sniffing channels, 296–297
    saving wireless profile, 309
    security, 309–315

sniffing wirelessly
in Linux, 303–304
in Windows, 300–302
wireless card modes, 298–299
wireless sniffing
in Linux, 303–304
sniffing channels, 296–297
in Windows, 300–302
Wireshark, 2, 37
advanced features, 77–101
big-endian format, 146
configuration files, 50
configuration profiles, 50–52
conversations, 78–83, 260, 262
cost, 38
endpoints, 78–83
expert information, 99–101
graphing, 95–99
Home Page, 322
installing, 39–43
on Linux systems, 41–43
on OS X systems, 43
on Windows systems, 39–41
main window, 45–46
name resolution, 84–88
operating system support, 39
Packet Bytes pane, 45, 46, 111
packet capture, 44–45
packet color coding, 48–49
Packet Details pane, 45, 46, 238
packet lengths, 93–94
Packet List pane, 45, 46, 239, 305–306
preferences, 46–47
program support, 39
protocol dissectors, 88–91
protocol hierarchy statistics, 83–84, 252, 253, 254
source code access, 39
stream following, 91–93
supported protocols, 38
user-friendliness, 38
Wi-Spy spectrum analyzer, 298
WLANs (wireless local area networks), 296. *See also* wireless packet analysis
WPA (Wi-Fi Protected Access), 309, 312–314

X

-x argument (command line tools), 110

Y

-Y argument (command line tools), 113
Your IP Address field (DHCP packets), 165

Z

Z (Reserved) field (DNS packets), 174
-z argument (command line tools), 115, 118
zero window packet (TCP), 242–245, 247