

INDEX

Symbols & Numbers

- && (AND) operator, in BPF syntax, 58
- <iframe> tag (HTML), 200
- <script> tag (HTML), 198–199
- tag (HTML), 200
- == (equal-to) comparison operator, 64
- ! (NOT) operator, in BPF syntax, 58
- .pcap file format, 48. *See also* capture file examples
- || (OR) operator, in BPF syntax, 58, 61
- 802.11 standard, 216
 - packet structure, 223–225

A

- ACKed Lost Packet message, 84
- ACK packet, 102, 132, 167, 168
 - duplicate, 171–172, 179
- acknowledgment number, in ACK packet, 169–170
- acknowledgment packet in DHCP, 119
- active fingerprinting, 196–197
- address registries, 70
- Address Resolution Protocol (ARP), 18, 86–90
 - gratuitous ARP, 89–90
 - header, 87–88
 - packet structure, 88
 - packets, 204
 - reply, 86, 87, 89, 148

- request, 86, 87, 88–89, 145, 148
- spoofing, 27, 205
- unsolicited updates to table, 204
- addressing filters, 59
- ad hoc mode, for wireless NIC, 218, 219
- Advanced Wireless Settings dialog, 221–222
- AfriNIC (Africa), 70
- aggregated network tap, 24–25
- AirPcap
 - capturing traffic, 221–222
 - configuring, 219–220
 - Control Panel, 220–221
- AJAX (Asynchronous JavaScript and XML), 139
- alerts from IDS, 206
- ALFA 1000mW USB wireless adapter, 219
- American Registry for Internet Numbers (ARIN), 70
- analysis step, in sniffer process, 4
- Analyze menu
 - Display Filters, 65
 - Expert Info Composite, 83
- AND (&&) operator, in BPF syntax, 58
- and filter expression logical operator, 65
- APNIC (Asia/Pacific), 70
- application baseline, 185
- Application layer (OSI), 5
- archive file, extracting, 39
- ARIN (American Registry for Internet Numbers), 70

- ARP. *See* Address Resolution Protocol (ARP)
 - ARP cache poisoning, 26–30, 32
 - attacker use, 202–205
 - caution on, 30
 - associations/dependencies
 - in application baseline, 186
 - in host baseline, 185
 - asymmetric routing, 30
 - Asynchronous JavaScript and XML (AJAX), 139
 - attackers
 - exploitation, 197–213
 - ping use to determine host
 - accessibility, 108
 - and random text in ICMP echo request, 110
 - reconnaissance by potential, 190–197
 - Windows command shell
 - use, 201
 - Aurora exploit, 197–202
 - authentication
 - in host baseline, 185
 - in site baseline, 184
 - Twitter vs. Facebook, 140
 - WEP
 - failed, 230
 - successful, 229–230
 - WPA
 - failed, 232–233
 - successful, 231–232
 - Automatic Scrolling in Live Capture
 - option, 56
 - AXFR (full zone transfer), 127
- B**
- baseline for network, 41, 183–187
 - application baseline, 186
 - host baseline, 185
 - site baseline, 184
 - basic service set identifier (BSS ID), 226
 - beacon packet, 224–225
 - broadcast from WAP, 231
 - benchmarking, Protocol Hierarchy Statistics for, 71–72
 - Berkeley Packet Filter (BPF) syntax, 58–61
 - Bootstrap Protocol (BOOTP), 113, 116
 - bottleneck, analyzer as, 30
 - BPF (Berkeley Packet Filter) syntax, 58–61
 - branch office, troubleshooting connections, 155–159
 - broadcast address, 116
 - broadcast domain, 14–15, 18
 - broadcast packet, 14–15
 - broadcast traffic, in site
 - baseline, 184
 - BSS ID (basic service set identifier), 226
 - buffer space in TCP, 173
 - byte offset, for protocol field filters, 60
- C**
- CACE Technologies, 219
 - Cain & Abel, 27–29, 236
 - CAM (Content Addressable Memory) table, 12, 86
 - CAPSCREEN command, 208–209
 - capture file examples
 - 80211beacon.pcap*, 224
 - 80211-WEPauthfail.pcap*, 230
 - 80211-WEPauth.pcap*, 229
 - 80211-WPAauthfail.pcap*, 232
 - 80211-WPAauth.pcap*, 231
 - activeosfingerprinting.pcap*, 197
 - arp_gratuitous.pcap*, 90
 - arppoison.pcap*, 202
 - arp_resolution.pcap*, 88
 - aurora.pcap*, 197
 - dhcp_inlease_renewal.pcap*, 120
 - dhcp_nolease_renewal.pcap*, 115
 - dns_axfr.pcap*, 127
 - dns_query_response.pcap*, 122
 - dns_recursivequery_client.pcap*, 124
 - dns_recursivequery_server.pcap*, 125
 - download-fast.pcap*, 79, 81
 - download-slow.pcap*, 78, 80, 83
 - facebook_login.pcap*, 138
 - facebook_message.pcap*, 139

- http_espn.pcap*, 140
- http_google.pcap*, 77, 82, 129
- http_post.pcap*, 131
- icmp_echo.pcap*, 108
- inconsistent_printer.pcap*, 153
- ip_frag_source.pcap*, 95, 96
- ip_ttl_dest.pcap*, 95
- ip_ttl_source.pcap*, 94
- latency1.pcap*, 180
- latency2.pcap*, 180
- latency3.pcap*, 181
- latency4.pcap*, 182
- lotsofweb.pcap*, 70, 71
- nowebaccess1.pcap*, 145
- nowebaccess2.pcap*, 147
- nowebaccess3.pcap*, 150
- passiveosfingerprinting.pcap*, 195
- ratinfected.pcap*, 207
- stranded_branchdns.pcap*, 157
- stranded_clientside.pcap*, 156
- synscan.pcap*, 191
- tcp_dupack.pcap*, 170
- tcp_handshake.pcap*, 102
- tcp_ports.pcap*, 99
- tcp_refuseconnection.pcap*, 105
- tcp_retransmissions.pcap*, 167
- tcp_teardown.pcap*, 104
- tcp_zerowindowdead.pcap*, 177
- tcp_zerowindowrecovery.pcap*, 175–177
- tickedoffdeveloper.pcap*, 159
- twitter_login.pcap*, 134
- twitter_tweet.pcap*, 136
- udp_dnsrequest.pcap*, 106
- wrongdissector.pcap*, 74
- capture files, 47–49
 - automatically storing packets in, 54–55
 - conversations in, colorizing, 208
 - merging, 49
 - saving and exporting, 48
- capture filters, 56
 - BPF syntax, 58–61
 - sample expressions, 61–62
- Capture menu, Interfaces, 53
- Capture Options dialog, 53–54
 - Display options, 56
 - enabling name resolution, 73
 - for filtering, 57
 - Name Resolution section, 56
- Capture section, for Wireshark preferences, 44
- capture type, for AirPcap, 220
- Chanalyzer software, 217–218
- channel hopping, 216
- channels, 216
 - changing when monitoring, 223
 - overlapping, 217
- Chappell, Laura, 240
- Chat category of expert information, 82, 83
- CIDR (Classless Inter-Domain Routing), 92
- Cisco, set span command, 22
- Cisco router, 13
- Classless Inter-Domain Routing (CIDR), 92
- clearing filters, 193
- Client Identifier DHCP option field, 117
- clients
 - in branch office, access to WAN, 155–159
 - latency, 181
 - misconfigured, 147
- closed ports, identifying, 193–194
- CloudShark, 237
- Colasoft Packet Builder, 237
- collection step, in sniffer process, 3
- collisions, on hub network, 20
- color
 - coding for packets, 45–46
 - in Follow TCP Stream window, 77
- Coloring Rules window (Wireshark), 45–46
- colorization rule, exporting end-points to, 68
- colorizing conversations, 208
- Combs, Gerald, 35
- comma-separated values (CSV) files
 - saving capture file as, 48
 - transmission to central database, 159–163
- comparison operators, 64
- compiling Wireshark from source, 39–40

- computers
 - communication process, 4–14
 - data encapsulation, 8–10
 - OSI model, 5–8
 - protocols, 4
 - screen capture by attacker, 212
 - connectionless protocol, 105–106
 - Content Addressable Memory (CAM) table, 12, 86
 - control packets (802.11), 223
 - conversations, 68
 - in capture file, colorizing, 208
 - viewing, 69
 - Conversations window
 - ESPN.com traffic in, 140–141
 - with TCP communications, 191–192
 - troubleshooting with, 70–71
 - conversion step, in sniffer process, 3
 - costs, of packet sniffers, 3
 - CSV (comma-separated values) files
 - saving capture file as, 48
 - transmission to central database, 159–163
 - CyberEYE remote-access Trojan (RAT), 207
- D**
- data encapsulation, 8–10
 - data flow, halting with zero window notification, 175
 - Data link layer (OSI), 6, 9
 - data packets (802.11), 224
 - data set, graph for overview, 79
 - data-transfer rate
 - in application baseline, 186
 - in site baseline, 184
 - data transmission, testing for corruption, 159–163
 - DEB-based Linux distributions, installing Wireshark on, 39
 - Decode As dialog, 74
 - default gateway, 147
 - attempt to find MAC address for, 145–146
 - denial-of-service (DoS) attacks, 27
 - Department of Defense (DoD)
 - model, 5
 - destination port, for TCP, 98–100
 - DHCP. *See* Dynamic Host Configuration Protocol (DHCP)
 - direct install method, for sniffer placement, 31, 32
 - direct messaging, in Twitter, 137
 - discover packet for DHCP, 116–117
 - Display Filter dialog, 65–66
 - display filters, 56–65
 - sample expressions, 65
 - saving, 65–66
 - dissection
 - expert information from, 82–84
 - viewing source code, 76
 - DNS. *See* Domain Name System (DNS)
 - DoD (Department of Defense)
 - model, 5
 - domain controller, and branch office, 155–159
 - Domain Dossier, 239
 - Domain Name System (DNS), 120–129
 - communication problems, 157
 - filter for traffic, 142–143
 - name-to-IP address mapping, 149
 - packet structure, 121–122
 - queries, 122–123, 142
 - conditions preventing, 149
 - question types, 124
 - recursion, 124–127
 - resource record types, 124
 - zone transfers, 127–129
 - DORA process, 115
 - DoS (denial-of-service) attacks, 27
 - dotted-quad notation, 91
 - double-headed packet, 111
 - downloading
 - NMAP tool, 191
 - pages from web server, 129–131
 - pOf tool, 196
 - WinPcap capture driver, 37
 - dropping packets, 10
 - dst qualifier, filter based on, 59

- duplicate ACK packet, 83, 171–172, 179
 - Dynamic Host Configuration Protocol (DHCP), 113–120
 - acknowledgment packet, 119
 - discover packet, 116–117
 - in-lease renewal, 119–120
 - offer packet, 117–118
 - options and message types, 120
 - packet structure, 114–115
 - renewal process, 115–118
 - request packet, 118–119
- E**
- echo, vs. ping, 109
 - Edit menu
 - Preferences, 44, 170
 - Name Resolution, 100
 - Set Time Reference, 53
 - email message, with link to malicious site, 197
 - encryption, 228
 - endpoints, 67–68
 - exporting, to colorization rule, 68
 - monitoring, 204
 - viewing, 68–69
 - Endpoints window, 68–69
 - troubleshooting with, 70–71
 - Enterasys, set port mirroring create command, 22
 - ephemeral port group, 99
 - equal-to comparison operator (==), 64
 - Error category of expert information, 82, 84
 - ESPN.com traffic, 140–144
 - Ethereal, 35
 - Ethernet, 9
 - broadcast address, 88
 - hub, 10
 - networks
 - ARP process for computers on, 26–27
 - default MTU, 95
 - maximum frame size, 78
 - switch, rack-mountable, 11
 - expert information, from dissection, 82–84
 - exporting
 - capture files, 48
 - endpoint to colorization rule, 68
 - expression, in BPF syntax, 58
 - extracting
 - archive, 39
 - JPG data from Wireshark, 211–212
- F**
- Facebook
 - capturing traffic, 137–139
 - login process, 138
 - private messaging with, 139
 - vs. Twitter, 140
 - fast retransmission, 84, 170, 172
 - FCS filter, for AirPcap, 220
 - file carving, 212
 - Filter Expression dialog, 63
 - Filter Expression Syntax Structure, 64–65
 - filters, 56–66
 - addressing, 59
 - BPF syntax, 58–61
 - clearing, 193
 - display, 62–65
 - Filter Expression dialog, 63
 - Filter Expression Syntax Structure, 64–65
 - sample expressions, 65
 - for DNS traffic, 142–143
 - hostname and addressing, 59
 - port and protocol, 60
 - protocol field, 60–61
 - for STOR command, 160
 - with SYN scans, 192–193
 - wireless-specific, 226–228
 - FIN flag, 103
 - finding packets, 50
 - Find Packet dialog, 50
 - fingerprinting operating systems, 194–197
 - flow graphing, 82
 - for data transmission testing, 159–160

- Follow TCP Stream feature, 76–77, 161–162
- footer, in packet, 8
- footprinting, 190
- forced decode, 74–76
- Fragment Offset field, for packets, 96, 97
- frames, maximum size on Ethernet network, 78
- frequency, filter for specific, 227–228
- Frequency/Channel data, for wireless, 225
- full-duplex devices, 11
 - switches as, 20
- full zone transfer (AXFR), 127
- Fyodor, 191

G

- gateway. *See* default gateway
- GET request packet (HTTP), 130, 135, 181
 - for Facebook, 138
- GIF file, to trigger exploit code, 200
- GNU Public License (GPL), 35
- graphing, 79–82
 - flow, 82
 - IO graphs, 79–80
 - round-trip time, 81
- gratuitous ARP, 89–90

H

- half-duplex mode, 10
- half-open scan, 190
- handshake for TCP, 101–103
 - initial sequence number, 169
 - and latency, 179
 - in Twitter authentication process, 134
- hardware, Wireshark requirements, 37. *See also* network hardware
- header in packet, 8
 - for ARP, 87–88
 - for ICMP, 107
 - for IPv4 header, 92–93

- for TCP, 98
- for UDP, 106–107
- help. *See* program support
- hexadecimal, searching for packets
 - with specified value, 50
- hex editor, 212
- Hide Capture Info Dialog option, 56
- high latency, 166, 179–183
- high-traffic servers, host baseline
 - for, 185
- host address, in IP address, 91
- host baseline, 185
- hostname, filters, 59
- host qualifier, for filter, 59
- hosts file, 149–150
- hping, 239
- HTTP. *See* Hypertext Transfer Protocol (HTTP)
- HTTPS, 134
- hubbing out, 22–23, 32
- hub network, collisions on, 20
- hubs, 10–11
 - finding “true,” 23
 - sniffing on network with, 19–20
- Hypertext Transfer Protocol (HTTP), 8–9, 129–132
 - browsing with, 129–131
 - posting data with, 131–132
 - viewing requests, 143–144

I

- IANA (Internet Assigned Numbers Authority), 240
- ICMP. *See* Internet Control Message Protocol (ICMP)
- Ident protocol, 193
- idle/busy traffic, in host baseline, 185
- IDS (intrusion detection system), 206
- IEEE (Institute of Electrical and Electronics Engineers), 216
- <iframe> tag (HTML), 200
- in-lease renewal for DHCP, 119–120
- incremental zone transfer (IXFR), 127

- installing Wireshark, 37–41
 - on Linux, 39–40
 - on Mac OS X, 40–41
 - on Microsoft Windows, 37–39
- Institute of Electrical and Electronics Engineers (IEEE), 216
- interference, between wireless channels, 217
- International Organization for Standardization (ISO), 5
- Internet access, troubleshooting configuration problems, 144–147
 - unwanted redirection, 147–150
- Internet Assigned Numbers Authority (IANA), 240
- Internet Control Message Protocol (ICMP), 107–112
 - echo requests and responses, 108–110
 - header, 107
 - ping, 95
 - types and messages, 107
- Internet Explorer, vulnerability in, 197
- Internet Protocol (IP), 9, 91–97
 - addresses, 26, 91–92
 - assignments, 70
 - dynamic assignment, 113–120
 - filtering packets with specific address, 64
 - finding. *See* Domain Name System (DNS)
 - fragmentation, 95–97
 - Time to Live (TTL), 93–95
 - v4 header, 92–93
- intrusion detection system (IDS), 206
- IO graphs, 79–80, 209–210
- IP. *See* Internet Protocol (IP)
- IP-to-MAC address mapping, updating cache with, 89–90
- IPv6 address, filter based on, 59
- ISO (International Organization for Standardization), 5
- iwconfig command, 222–223
- IXFR (incremental zone transfer), 127

J

- JFIF string, 209
- JPG file
 - extracting data from Wireshark, 211–212
 - to initiate attack communication, 209–211

K

- Keep Alive message, 84
- keep-alive packets, 175, 177–178, 179
- keys, for SSL, 135
- Kismet, 216
- Kozierok, Charles, *The TCP/IP Guide*, 240

L

- LAN (local area networks), 91
- latency, 166
 - locating framework, 182–183
 - locating source of high, 179–183
 - client latency, 181
 - normal communications, 180
 - server latency, 182
 - wire latency, 180–181
- layer 2 addresses, 26
- layer 8 issue, 7
- leases, from DHCP, 119–120
- LED lights on AirPcap, blinking, 220
- libpcap/WinPcap driver, 19, 239
- Linux
 - default number of retransmission attempts, 167
 - hosts file examination, 150
 - installing Wireshark on, 39–40
 - sniffing wirelessly, 222–223
 - traceroute utility, 112
- local area networks (LAN), 91
- location, for packet sniffer, 17–18, 31–32
- logical addresses, 9, 86
- logical operators
 - in BPF syntax, 58
 - for combining filter expressions, 64–65

- login process
 - for Facebook, 138
 - for Twitter, 134–135
- low latency, 166

M

- MAC address, 26, 86
 - ARP and, 18
 - attempt to find for default gateway, 145–146
 - filter based on, 59
 - name resolution, 73
- MAC Address Scanner dialog (Cain & Abel), 28
- Mac OS X, installing Wireshark on, 40–41
- mailing lists, for program support, 3
- make command, 40
- malware
 - redirecting users to websites
 - with malicious code, 150
 - risk of infection, 150
- man-in-the-middle attacks, 140, 202
- managed mode, for wireless NIC, 218, 219
- managed switches, 11
- management packets (802.11), 223
- mapping path, 110–112
- marking packets, 51
- master mode, for wireless NIC, 218, 219
- maximum transmission unit (MTU), and packet fragmentation, 95
- MD5 hashes, 162–163
- merging capture files, 49
- Message Type DHCP option field, 116
- message types, for DHCP, 120
- messaging methods, Twitter vs. Facebook, 140
- MetaGeek, 217
- Microsoft Windows
 - command shell, attacker use, 201
 - default number of retransmission attempts, 167
 - hosts file examination, 150

- installing Wireshark on, 37–39
- sniffing wirelessly, 219–222
- mission-critical servers, host baseline for, 185
- monitor mode for wireless NIC, 218, 219
 - enabling in Linux, 222–223
- monitor port, for nonaggregated taps, 25
- More Fragments field, for packets, 96, 97
- MTU (maximum transmission unit), and packet fragmentation, 95
- multicast traffic, 15

N

- name resolution, 72–74
- Name Resolution section, for Wireshark preferences, 44
- namespace, for DNS server management, 127
- Netdude, 236
- netmask (network mask), 91–92
- network address, in IP address, 91
- network baselining, 183–187
- network diagrams, 31
- network endpoints, 67–68. *See also* endpoints
- network hardware, 10–14
 - hubs, 10–11
 - routers, 12–14
 - switches, 11–12
 - taps, 24–26
- network interface card
 - promiscuous mode support, 18–19
 - wireless card modes, 218–219
- Network layer (OSI), 6
- network maps, 31
- network mask (netmask), 91–92
- NetworkMiner, 238
- network name resolution, 73
- networks
 - packet level as source of problems, 1
 - traffic classifications, 14–15

- traffic flow, 14
- understanding normal traffic, 85
- network tap, 24–26, 32
- ngrep, 238
- NMAP tool, 191, 197
- No Error Messages message, 84
- nonaggregated network tap, 24, 25–26
- Nortel, port-mirroring mode
 - mirror-port command, 22
- NOT (!) operator, in BPF syntax, 58
- Note category of expert
 - information, 82, 83
- not filter expression logical operator, 65
- Novak, Judy, 240

O

- Offer packet in DHCP, 117–118
- OmniPeek, 2
- one-way latency, 166
- open ports, identifying, 193–194
- operating systems. *See also* Linux;
Mac OS X; Microsoft
Windows
 - fingerprinting, 194–197
 - sniffer support, 3
 - Wireshark support, 37
- Operation Aurora, 197–202
- OR (||) operator, in BPF syntax, 58, 61
- or filter expression logical operator, 65
- OSI model, 5–8
- out of lease, 119
- Out-of-Order message, 84
- oxid.it, 27

P

- packet analysis, 2
 - tools, 235–239
 - web resources, 239–240
- Packet Bytes pane (Wireshark), 43
- packet capture, 41–42. *See also* capture file examples

- Packet Details pane (Wireshark), 43, 153
 - Application Data in Info column, 135
 - retransmission packet information, 168
- Packet List pane (Wireshark), 43, 74, 153
 - adding columns to, 203, 225–226
 - for filter, 160
 - retransmissions in, 168
- packets
 - color coding, 45–46
 - dropping, 10
 - finding, 50
 - fragmentation, 95–97
 - length, 78–79
 - mapping path, 110–112
 - marking, 51
 - printing, 51–52
 - SYN flag, 148–149
 - term defined, 8
 - wireless types, filtering specific, 227
- packet sniffers
 - evaluating, 2–3
 - guidelines, 32
 - how they work, 3–4
 - positioning for data capture, 17–18, 31–32
- packet sniffing, 2. *See also* packet analysis
- Packetstan blog, 240
- packet time referencing, 52, 53
- Parameter Request List DHCP option field, 117
- passive fingerprinting, 194–196
 - .pcap file format, 48. *See also* capture file examples
- pcapr, 237–238
- PDF file, printing packets to, 51
- PDU (protocol data unit), 8
- performance, 165–187. *See also* latency
 - network baselining, 183–187
 - Selective ACK and, 172

- Perl, 239
- physical addresses, 86
- Physical layer (OSI), 5, 6, 9
- ping utility, 108
- plaintext, saving capture file as, 48
- pOf tool, 196
- Poor, Mike, 240
- port mirroring, 21–22, 32
 - for checking for data corruption, 159
 - for troubleshooting printer, 153
- port-mirroring mode mirror-port command (Nortel), 22
- ports
 - attacker research on, 190
 - attackers' efforts to determine open, 190
 - blocking traffic, 158
 - filter based on, 60
 - filter to show all traffic using specific, 192
 - filtering packet capture by, 57
 - filters to exclude, 60
 - for HTTP, 130
 - identifying open and closed, 193–194
 - list of common, 101
 - for TCP, 99–101
- port spanning, 21. *See also* port mirroring
- posting data with HTTP, 131–132
- POST method, 132
 - for Facebook, 139
 - for tweet, 136
- POST packet (HTTP), 131
- PostScript, saving capture file as, 48
- Preferences dialog (Wireshark), 44
 - Name Resolution section, 100
 - Protocols section, 170
- Presentation layer (OSI), 5
- Previous Segment Lost message, 84
- primitives, in BPF syntax, 58
- Print dialog, 51
- printing packets, 51–52
- Printing section, for Wireshark preferences, 44
- privacy, of Twitter direct messages, 137
- private messaging, with Facebook, 139
- problems. *See* troubleshooting
- program support
 - evaluating, 3
 - for Wireshark, 37
- promiscuous mode, 3
 - network interface card support for, 18–19
- protocol analysis, 2. *See also* packet analysis
- protocol data unit (PDU), 8
- protocol field filters, 60–61
- Protocol Hierarchy Statistics, 71–72, 141–142, 184
- protocols, 4
 - in application baseline, 186
 - color coding in Wireshark, 45–46
 - dissection, 74–76
 - filter based on, 60
 - in host baseline, 185
 - lower-layer, 85–112
 - Address Resolution Protocol (ARP), 86–90
 - Internet Control Message Protocol (ICMP), 107–112
 - Internet Protocol (IP), 91–97
 - Transmission Control Protocol (TCP), 98–105
 - User Datagram Protocol (UDP), 105–107
 - and OSI model, 6
 - packet sniffer evaluation and, 2
 - in site baseline, 184
 - support by Wireshark, 37
 - upper-layer, 113–132
 - Domain Name System (DNS), 120–129
 - Dynamic Host Configuration Protocol (DHCP), 113–120
 - Hypertext Transfer Protocol (HTTP), 129–132

- Protocols section, for Wireshark
 - preferences, 44
- protocol stack, 4
- public forums, for program support, 3
- Python, 239

Q

- qualifiers, in BPF syntax, 58
- queries in DNS, 122–123, 142
 - conditions preventing, 149

R

- rack-mountable Ethernet switch, 11
- RAT (remote-access Trojan), 206–213
- reassembly, for packets in FTP-DATA stream, 160–161
- receive window, 173
 - adjusting size, 174, 176
 - halting data flow, 175
- Received Signal Strength Indication (RSSI), 225
- reconnaissance by potential attacker, 190–197
- redirection, troubleshooting
 - unwanted, 147–150
- remote-access Trojan (RAT), 206–213
- remote server, lack of response, 152
- repeating device, hub as, 10
- Replay Counter field, 232
- report-generation module, free vs. commercial sniffers, 3
- Request for Comments (RFC)
 - 791, on Internet Protocol v4, 91
 - 792, on ICMP, 107
 - 793, on TCP, 98
 - 826, on ARP, 86
 - DNS-related, 120
- request packet, 8
 - in DHCP, 118–119
- Requested IP Address DHCP option field, 117
- resource records in DNS servers, 120

- retransmission packets, 154, 166–169, 178–179
- retransmission timeout (RTO), 154, 166, 168
- retransmission timer, 166
- RFC. *See* Request for Comments (RFC)
- Ring Buffer With option, 55
- RIPE (Europe), 70
- Riverbed, 219
- RJ-45 ports, 10
- round-trip time (RTT), 166
 - graphing, 81
- routed environment, sniffing on, 30–31
- routers, 12–14
 - for connecting LANs, 91
- RPM-based Linux distributions, installing Wireshark on, 39
- RSSI (Received Signal Strength Indication), 225
- RST flag, 148–149
- RTO (retransmission timeout), 154, 166, 168
- RTT (round-trip time), 166
 - graphing, 81

S

- Sanders, Chris, blog, 240
- SANS Security Intrusion Detection In-Depth course, 239–240
- saving
 - capture files, 48
 - display filters, 65–66
 - file set, 55
- Scapy, 236
- screen capture, of victim computer, 212
- <script> tag (HTML), 198–199
- secondary DNS server, 127
- Secure Socket Layer (SSL), 74
 - over HTTP, 134–135
- security for wireless, 189–213, 228–233
 - for baseline, 187
 - exploitation, 197–213

- security for wireless (*continued*)
 - reconnaissance, 190–197
 - remote-access Trojan, 206–213
 - screen capture by attacker, 212
 - Twitter and, 136–137
 - WEP authentication
 - failed, 230
 - successful, 229–230
 - WPA authentication
 - failed, 232–233
 - successful, 231–232
 - Selective Acknowledgment
 - feature, 172
 - sequence numbers, in TCP
 - packet, 169
 - server latency, 182
 - Session layer (OSI), 5
 - set port mirroring create command (Enterasys), 22
 - set span command (Cisco), 22
 - site baseline, 184
 - sliding window mechanism (TCP), 173, 175–178
 - slow network. *See* performance
 - Sniffer tab (Cain & Abel), 28
 - sniffing the wire, 17
 - Snort project, 202
 - social networking, packets for, 134–140
 - source code for dissector,
 - viewing, 76
 - source port, for TCP, 99, 100
 - tag (HTML), 200
 - spear phishing, 197
 - spectrum analyzer, 217
 - src qualifier, filter based on, 59
 - SSL (Secure Socket Layer), 74
 - over HTTP, 134–135
 - standard port group, 99
 - startup/shutdown
 - in application baseline, 186
 - in host baseline, 185
 - Statistics menu
 - Conversations, 69, 140–141
 - Flow Graph, 82, 159
 - HTTP, 143
 - IO Graphs, 79
 - Packet Lengths, 78
 - Protocol Hierarchy, 71, 141–142
 - Summary, 143
 - TCP Stream Graph, Round Trip Time Graph, 81
 - Statistics section, for Wireshark
 - preferences, 44
 - stealth scan, 190
 - Stevens, Richard, *TCP/IP Illustrated*, 240
 - Stop Capture settings, 55
 - STOR command (FTP), 160
 - subnet mask, 91–92
 - Summary window, 143–144
 - switches, 11–12
 - sniffing on network with, 20–30
 - ARP cache poisoning, 26–30
 - hubbing out, 22–23
 - port mirroring, 21–22
 - using tap, 24–26
 - SYN/ACK packet, 102
 - SYN packet, 102, 148–149, 151–152
 - lack of response, 158
 - response, 180
 - SYN scans, 190–194
 - filters with, 192–193
- ## T
- tar command, 39
 - TCP. *See* Transmission Control Protocol (TCP)
 - tcpdump, 2, 235–236
 - TCP/IP, address resolution
 - process, 86
 - TCP/IP Guide* (Kozierok), 240
 - TCP/IP Illustrated* (Stevens), 240
 - Tcpdump, 238
 - terminating TCP connection, 148–149
 - three-way handshake for TCP, 101–103
 - initial sequence number, 169
 - and latency, 179
 - in Twitter authentication
 - process, 134
 - throughput
 - graphing, 79
 - of ports being mirrored, 22

- Time Display Formats, 52
 - Time to Live (TTL), 93–95
 - Traceroute, 110–112
 - traffic signatures, 202
 - Transmission Control Protocol (TCP), 8–9, 98–105
 - buffer space, 173
 - capturing only packets with RST flag set, 61
 - DNS and, 127, 157–158
 - duplicate acknowledgments, 169–172
 - error-recovery features, 166–172
 - retransmission, 166–169
 - expert info messages configured for, 83–84
 - flow control, 173–178
 - following streams, 76–77
 - header, 98
 - HTTP and, 129–130
 - learning from error- and flow-control packets, 178–179
 - resets, 104
 - retransmission packets, 83, 154
 - sliding window mechanism, 173, 175–178
 - SYN scan, 190–194
 - teardown, 103–104
 - terminating connection, 148–149
 - three-way handshake, 101–103
 - initial sequence number, 169
 - and latency, 179
 - in Twitter authentication process, 134
 - Transmission Rate (TX Rate), for wireless, 225
 - Transport layer (OSI), 6, 8–9
 - transport name resolution, 73
 - trigger for exploit code, GIF file for, 200
 - troubleshooting
 - branch office connections, 155–159
 - developer tensions, 159–163
 - with Endpoints and Conversations windows, 70–71
 - latency, 178–179
 - no Internet access
 - from configuration problems, 144–147
 - from unwanted redirection, 147–150
 - from upstream problems, 150–153
 - printer inconsistency, 153–155
 - slow networks, 166
 - wireless signal interference, 217
 - TTL (Time to Live), 93–95
 - Twitter
 - capturing traffic, 134–137
 - direct messaging, 137
 - vs. Facebook, 140
 - login process, 134–135
 - sending data, 136–137
 - TX Rate (Transmission Rate), for wireless, 225
- ## U
- Ubuntu, installing Wireshark on, 39
 - UDP. *See* User Datagram Protocol (UDP)
 - unicast packet, 15
 - unmarking packets, 51
 - Update List of Packets in Real Time option, 56
 - uploading data to web server, 131–132
 - upstream problems, troubleshooting lack of Internet access from, 150–153
 - User Datagram Protocol (UDP), 105–107, 157
 - DHCP and, 116
 - DNS and, 123
 - header, 106–107
 - and latency, 182
 - user-friendliness
 - of packet sniffers, 3
 - of Wireshark interface, 37
 - User Interface section, for Wireshark preferences, 44
 - user privileges, for promiscuous mode, 19
 - USER request command (FTP), filter for traffic, 160–161

V

viewing

- conversations, 69
- endpoints, 68–69

View menu

- Time Display Format, 52, 53, 154–155
- Seconds Since Previous Displayed Packet, 179

visibility window, 20, 21

W

WAN (wide area network), branch office access, 156

WAP (Wireless Access Protocol)

- beacon packet, 231
- broadcast packet from, 224

Warning category of expert information, 82, 84

web resources

- on DHCP options, 120
- DNS-related RFCs, 120
- on DNS resource record types, 124
- on intrusion detection and attack signatures, 202
- on packet analysis, 239–240
- on packet analysis tools, 236–239
- on wireless capture filters, 228

web server

- downloading pages from, 129–131
- uploading data to, 131–132

websites, capturing traffic, 140–144

WEP. *See* Wired Equivalent

Privacy (WEP)

WHOIS utility, 70

wide area network (WAN), branch office access, 156

Wi-Fi Protected Access (WPA), 228

- authentication
- failed, 232–233
- successful, 231–232

Window is Full message, 84

Windows. *See* Microsoft Windows

Windows command shell, attacker use, 201

Windows Size field, 175–176

Window Update message, 83

Windump, 235–236

WinHex, 212

WinPcap capture driver, 37

Wired Equivalent Privacy (WEP), 228

authentication

- failed, 230
- successful, 229–230

configuration with AirPcap, 220

wire latency, 180–181

Wireless Access Protocol (WAP)

- beacon packet, 231
- broadcast packet from, 224

wireless packet analysis, 215–233

802.11 packet structure, 223–225

adding columns to Packet List pane, 225–226

filters specific to, 226–228

NIC modes, 218–219

physical considerations, 216–217

signal interference, 217

sniffing channel at a time, 216

security, 228–233

failed WEP

authentication, 230

failed WPA authentication, 232–233

successful WEP authentication, 229–230

successful WPA authentication, 231–232

sniffing

in Linux, 222–223

in Windows, 219–222

Wireshark University, 240

Wireshark

and AirPcap, 221

benefits, 36–37

fundamentals, 41–46

first packet capture, 41–42

main window, 42–43

preferences, 43–44

hardware requirements, 37

history, 35–36

- home page, 239
- installing, 37–41
 - on Linux, 39–40
 - on Mac OS X, 40–41
 - on Microsoft Windows, 37–39
- libpcap/WinPcap driver, 19, 239
- relative sequence numbers, 170
- Wi-Spy, 217
- WPA (Wi-Fi Protected Access), 228
 - authentication
 - failed, 232–233
 - successful, 231–232

X

- XML, saving capture file as, 48
- xor filter expression logical operator, 65

Z

- Zero Window message, 84
- zero window notification, 175, 176, 179
- Zero Window Probe message, 83, 84
- zone transfers
 - for DNS, 127
 - risk from allowing access to data, 128
- failed, 158