

Index

- != filter operator*, 174–75
- 4 NOPs in a Row warning*, 256
- 6to4 traffic*, 367
- ACKed Segment that Wasn't Captured warnings*, 253
- addresses*. *See IP (Internet Protocol) or MAC (Media Access Control)*
- AirPcap adapter*, 106–7, 367, 380
- Allen, Lanell*, 265
- Allow subdissector to reassemble TCP streams setting*, 74–79, 94, 211, 266, 276, 278, 342, 352
- analysis steps (typical)*, 10
- annotations*
 - button on Status Bar, 37
 - comment column, 289
 - definition of, 367
 - exporting comments, 291
 - packet and file options, 284
 - packet comments, 287–88
 - pcapng* format required, 288
 - pkt_comment* field, 284
- application analysis*
 - capture filters, 131–35
 - techniques, 239–46
- ARP (Address Resolution Protocol)*
 - description of protocol, 367
 - display filter, 139
 - example, 40
 - exclusion display filter, 167, 174
 - poisoning, 256
 - Source and Destination columns, 29
- ASCII (American Standard Code for Information Interchange)*, 36, 221, 367
- ask.wireshark.org web site*, 19–21
- auto-complete mechanism*, 143
- autostop condition*, 313–15
- background traffic*
 - definition of, 368
 - example analysis of, 47–55
 - file transfers on startup, 173
- bandwidth usage*, 242
- Bejtlich, Richard*, 1
- Blok, Sake*, 227
- Bluetooth*, 23
- Bookmark button*, 151, 153, 192
- Boolean field filtering*, 175
- Bootstrap Protocol (BOOTP)*, 139, 159, 368
- BPF (Berkeley Packet Filtering) syntax*, 8, 122–24, 131, 140, 316, 368
- broadcasts*
 - background traffic, 50
 - capture filter, 125
 - definition of, 368
 - DHCP ACK example, 47
 - Dropbox example, 42
 - switches forward, 17
- Broman, Anders*, 283
- Bug Tracker*, 58
- build a network picture from packets*, 39
- Calculate conversation timestamps setting*, 75–76, 79, 82, 91, 186–87, 335, 369
- Capinfos*, 300
- capture*
 - locations, 13–17, 103–9
 - options, 127, 129, 134
 - options quick reference, 102
 - process overview, 7
 - to file sets, 113
 - with ring buffer, 118
- Capture Engine*
 - description, 368
 - functionality, 8
 - reduce load on, 120
- capture filters*, 122–36
 - applying, 102

- based on ICMP Type/Code numbers, 133
- default set, 126
- description, 368
- purpose of, 110, 120
- recommendation to avoid, 120
- with command-line capture, 316
- capture interface description*, 368
- cfilters (capture filters) file*, 83, 189
- checksum errors*
 - coloring rule, 202–3
 - description, 368
 - from hex editing, 69
- checksum offloading*, 76
- CIDR (Classless Interdomain Routing)*
 - definition of, 369
 - subnet display filtering, 161
- client latency*, 88
- colorfilters (coloring rules) file*, 83
- coloring rules*
 - adding a column, 200–201, 200–201
 - checksum errors, 202–3
 - creating, 204, 206
 - disabling, 202
 - highlighting conversations, 209–13
 - highlighting delays with, 204–6
 - highlighting FTP passwords, 207–8
 - right-click method, 206
 - which coloring rule is applied, 199
- columns*
 - Apply as Column, 59, 63, 91, 97, 148, 172
 - create using Preferences, 60
 - creating, 59–64
 - description of defaults, 29
 - editing, 61
 - hide/display/rename/remove, 33
 - reordering, 32
 - sorting, 31, 62
- Combs, Gerald*, 3
- comments*
 - Capture File Properties window, 286
- comparison operators*, 145, 161, 369
- configuration files*, 83
- conversation*
 - filtering, 169–72, 230
 - most active, 234–36
 - statistics, 170, 173, 229, 232
- core engine*
 - description, 369
 - functionality, 8, 65
- Degioanni, Loris*, 57, 112, 378, 380
- delays considered "normal"*, 94–95
- delta time*
 - coloring rule, 204
 - column, 62, 90
 - filters, 186
 - general description, 369
 - TCP delta time, 186
 - TCP description, 369
 - troubleshooting with, 89–98
- dfilters (display filters) file*, 152, 189
- DHCP (Dynamic Host Configuration Protocol)*
 - definition of, 369
 - display filter not recognized, 159
 - host name display filter, 140
 - relation to BOOTP, 368
 - using bootp display filter, 159
- display filters. See also dfilters file*
 - ... and not Selected, 167
 - ... and Selected, 167
 - ... or not Selected, 167
 - ... or Selected, 167
 - Apply as Filter, 163–64, 367
 - color-coding (red, green, yellow), 179
 - definition of, 370
 - editing defaults, 151
 - excluding an IP address, 160
 - field name filters, 163–67
 - Filter Expression buttons, 190–95
 - importing, 188–89
 - ip.addr != filter problem, 174
 - keyword detection, 180–83
 - logical operators, 174
 - on key words, 182
 - Prepare a Filter, 165, 376

- range of addresses, 161
- single IP address or host, 160
- spotting traffic delays, 186–87
- subnet, 161
- syntax, 139–40
- toolbar, 24, 27
- using "..." enhancements, 165–67
- using "contains", 180
- using "matches", 181
- using host names, 160
- using wildcards, 184–85
- with auto-complete, 143, 147
- with case insensitivity, 181
- with command-line capture, 318–19
- dissectors*
 - definition of, 370
 - forcing, 70
 - functionality, 65–68
 - heuristic, 70
 - non-standard ports, 69–71
- DNS (Domain Name System)*
 - capture filters, 134–35
 - name error display filter, 168
- DO NOT EDIT THIS FILE message, 84*
- dropped packets during capture, 120–23*
- DSCP (Differentiated Services Code Point), 370*
- DuBois, Betty, 101*
- Dumpcap*
 - definition of, 370
 - overview, 310–11
 - stop conditions, 8
- Duplicate ACKs notes, 253*
- Duplicate IP Address Configured warning, 256*
- Editcap*
 - definition of, 370
 - key options, 298
- Endpoint statistics, 233*
- error detection mechanism, 141*
- Ethereal, 3, 370*
- Ethernet*
 - definition of, 370
 - dissector functionality, 66
- exclusion filter, 164, 167, 371*
- Expert Information, 37, 288, 371*
 - color-coded button on status bar, 37, 249
 - definitions, 253–56
 - display filters, 252
 - severity levels, 250
- exporting*
 - conversations, 216–19, 218
 - host names, 223–25
 - HTTP objects, 276
 - packet comments, 291–93
 - packet dissections, 62, 220, 292
 - packets, 186, 216–19
 - to CSV format, 62, 220, 222, 224
- expressions (display filter), 146*
- Fast Retransmission notes, 254*
- field names, 142*
- file sets, 113–15*
- Filter Expression buttons*
 - creating, 190–95
 - definition of, 72
 - editing, 192
 - GET/POST button, 194**
 - preferences file location, 192–95
- filter toolbar (display filters), 27, 146*
- Fortunato, Tony, 359*
- frame definition, 11*
- Frame section*
 - dissector, 65
 - metadata, 35
- FTP (File Transfer Protocol)*
 - argument display filter, 180
 - case-insensitive display filter, 181
 - command/data channel capture filter, 132
 - commands display filter, 140
 - definition of, 371
 - detect passwords, 207–8
 - over a non-standard port, 69
 - port number-based capture filter, 131
 - reassemble transferred files, 271–75

- transport name resolution, 73
- wildcard display filter, 185
- Gentil, Lionel*, 197
- GeoIP**
 - configuration, 237–38
 - location services, 237
- GIMP graphical toolkit**, 8, 9, 371
- Gonder, John*, 297
- Goyvaerts, Jan*, 181
- graphical interface elements*, 2
- heuristic dissector*
 - description, 371
 - functionality, 70
 - missing, 70, 240
- heuristic dissectors*. **See dissectors**
- high traffic rates*, 110–12
- hosts file*, 312, 372
- HTTP (Hypertext Transfer Protocol)**
 - 404 display filter, 168
 - add a Host field column, 63
 - analysis of slow browsing, 96–98
 - analyze a sample session, 45
 - auto-complete filtering, 143
 - basic display filter, 140
 - dissector, 67
 - error profile, 85
 - export objects, 276–80
 - GET display filter, 142
 - GET filter using "contains", 145
 - GET/POST Filter Expression button, 194–95
 - headers preceding, 11
 - Host field display filter, 140, 147–50
 - normal .ico delays, 94
 - normal GET delays, 94
 - port number-based capture filter, 131
 - port number-based display filters, 154–58
 - preference setting, 71
 - reassembly techniques, 269–70
 - response time, 74
 - server delays, 94
 - String-Matching Capture Filter Generator tool, 132
 - TCP handshake preceding, 40
 - TCP preference settings effect, 74
 - traffic paths, 13
- IANA (Internet Assigned Numbers Authority)**, 372
- ICMP (Internet Control Message Protocol)**, 372, 379
- ifconfig*, 127, 129, 153
- importing profiles*, 85–86
- Intelligent Scrollbar**, 29, 212–15
- Internet Storm Center (ISC)**, 372
- IO Graph**
 - changing an axis, 242
 - changing streams, 268
 - file transfer problems, 261
 - `ip.addr` graphing, 244
 - `ip.src` graphing, 245
 - network errors, 259–60, 260
 - port graphing, 246
 - quick reference, 228
 - subnet graphing, 247
- io_graphs file*, 83
- IP (Internet Protocol)**
 - dissector, 66
 - exclusion display filters, 160
 - IP address capture filter, 124–28
 - IP address display filter, 373
 - IP header, 11, 370
 - low TTL display filter, 145
 - packet forwarding, 13–17
 - subnet capture filter, 125
 - subnet display filters, 160–62
 - Time to Live field, 15
- ip.addr != filter problem*, 174
- ipconfig*, 127, 129, 153
- IPv6**
 - address range display filter, 161
 - capture filter, 125, 127
 - DNS AAAA record query, 45
 - GeoIP mapping, 237
 - ICMPv6 Neighbor Notification, 47

- in Protocol Hierarchy Statistics, 239
- most active conversation, 232
- most active host, 233
- multicast capture filter, 125
- multicast example, 39
- protocol display filter, 139
- Router Advertisement, 47
- single address display filter, 160
- source/destination addresses in IO Graphs, 245
- subnet capture filter, 125
- toggle Interfaces view, 108
- IRC (Internet Relay Chat) detection in Protocol Hierarchy, 239–40**
- Kali Linux**
 - www.kali.org, 6
- Keels, Jennifer, 329**
- Keep-Alive ACK notes, 254**
- Keep-Alive warnings, 254**
- key hosts, 373**
- keyboard shortcuts, 24**
- keyword filtering, 180–83**
- latency (client, server and path), 87–98**
- legal concerns, 5**
- libpcap, 6–7, 373**
- link-layer driver, 7, 8, 373, 380**
- location for capture, 103–9**
- logarithmic scale, 228, 262, 263**
- logical operators, 174, 373**
- Lyon, Gordon (Nmap Founder), 137, 374**
- MAC (Media Access Control) address**
 - capture filter, 129–30
 - definition of, 373
 - frame definition, 12
 - local addressing only, 14
- Main Toolbar, 24**
- manuf file, 73, 373**
- marking packets, 217**
- matches operator, 180–84, See also Regex**
- Menu Bar, 23**
- Mergecap, 306, 373**
 - key options, 298
 - merging trace files, 306, **See also Mergecap metadata, 8, 35, 65, 106–7, 374**
 - Microsoft Message Analyzer, 54**
 - multi-adapter capture, 109**
 - multicasts, 125**
 - background traffic, 50
 - capture filter, 125
 - definition of, 374
 - IPv6 all hosts capture filter, 125
 - IPv6 all routers capture filter, 125
 - IPv6 example, 39
 - multiple file capture, 110–19**
 - name resolution settings, 73**
 - NAT (Network Address Translation), 13, 374**
 - NetBIOS (Network Basic Input/Output System), 374**
 - Netresec, 280**
 - network interface card (NIC), 374**
 - Network Monitor .cap file format, 54**
 - network name resolution, 73, 372, 374**
 - NetworkMiner, 280**
 - Nmap, 181, 374**
 - Out-of-Order warnings, 254**
 - overloaded client detection, 257**
 - Packet Bytes pane, 59–64**
 - definition of, 375
 - example of use, 150
 - overview, 35–36
 - packet comments, 292, See also annotations**
 - packet comments, see also annotations, 37, 285–90, 292, 375**
 - packet definition, 11**
 - Packet Details pane**
 - analyzing background traffic in, 47–48
 - building a network picture from, 39
 - building columns using, 63
 - coloring rules in Frame section, 200
 - definition of, 375
 - effect on Status Bar, 37
 - enable TCP timestamp fields, 75
 - enable *Track number of bytes in flight*, 74
 - exporting contents, 221

- Frame section metadata definition, 374
- learning field names, 142
- overview, 35
- packet comments, 367
- right-click coloring rules, 206
- right-click filtering, 59, 163
- right-click protocol settings, 78–80
- TCP Delta filter, 186
- Packet List pane. *See also columns***
 - overview, 27–34
 - right-click functionality, 34
- packet loss condition**
 - ACKed Segment that Wasn't Captured, 253
 - Duplicate ACKs, 253
 - Fast Retransmissions, 254
 - IO graphing, 260
 - move your analyzer, 104
 - not dropped by Wireshark, 121
 - Previous Segment Not Captured, 253
 - Retransmissions, 253
 - TCP analysis flags filter, 140
 - Tshark statistics, 323
- path latency, 10, 87**
- pcapng**
 - definition of, 375
 - purpose, 8, 9
 - required for annotations, 37
- personal configuration directory, 84**
- port number capture filters, 131–35**
- port spanning, 105, 376**
- preference settings**
 - definition of, 376
 - Filter Expressions buttons, 72
 - HTTP port numbers, 71
 - key protocol settings, 74–80
 - name resolution settings, 73
 - preferences file, 376
 - TCP settings, 94
 - user interface settings, 72
- Previous Segment Not Captured warnings, 253**
- profiles**
 - column on Status Bar, 38
 - copying, 82
 - creating, 81–86
 - definition of, 376
 - folder locations, 194
 - importing elements, 188–89
 - Manage Profiles option, 82
- Protocol Data Unit (PDU)**
 - definition of, 376
 - TCP setting effect on, 46, 94
- Protocol Hierarchy**
 - "data" listing, 71
 - definition of, 376
 - launching, 239
 - suspicious traffic, 240
- QoS (Quality of Service), 376**
- reassemble HTTP objects, 278**
- reassembly of conversations (following streams), 229, 267–75**
- receive buffer congestion indications, 254**
- Regex**
 - definition of, 377
 - PERL definition of, 375
 - Regex Buddy, 181
 - Regex Magic, 181
 - Use with ".", 184
 - using the matches operator, 181
 - www.regular-expressions.info, 181
- Related Packets Indicator, 28–31, 46**
- relative start (Rel.Start), 377**
- Retransmission notes, 253**
- Reused Ports note, 255**
- ring buffer, *see also multiple file capture*, 116, 118**
- Riverbed, 58**
- router**
 - forwarding process, 15
 - problem indication, 256
 - removes/applies MAC header, 14
 - router/NAT forwarding process, 15
- Router Advertisement packets, 47**
- RST (Reset), definition of, 377**
- security**

- analysis tasks, 5
- capture techniques, 110
- coloring rule naming, 206
- creating special profile for, 81
- detect suspicious protocols or applications, 241
- proximity filtering, 185
- Reused Ports Expert Information note, 255
- risks and vulnerabilities list, 372
- segment definition*, 11
- SEQ/ACK analysis section*, 74
- server latency*, 88–89
- services file*, 73, 377
- settings*. *See preference settings*
- SharkFest*, 58
- slow browsing*, 17, 103, 110
- SMB (Server Message Block)*
 - definition of, 377
 - Status field display filter, 146
- Smoothed Moving Average (SMA)*, 228
- SNMP (Simple Network Management Protocol)*, 377
- Snort*, 181, 377
- Source and Destination columns*, 29
- sparklines*, 23, 106
- split trace files*. *See also Editcap \r*
- Splunk*, 181
- sporadic network problems*, 116
- Spurious Retransmission notes*, 254
- Start Page*, 22
- Status Bar*, 37–38
- SteelCentral™ Packet Analyzer*, 112
- Stream index*, 267, 378
- stream reassembly*, 378
- suspicious protocols/applications*, 240, 241
- switches*, 14, 17, 121
- SYN (Synchronize Sequence Numbers)*
 - definition of, 371, 378
 - flag filter, 174–75
 - handshake example, 48
 - measure time with, 87
 - summary line filter, 177
 - wrong time column for delays, 93
- taps for full-duplex capture*, 105
- TCP (Transmission Control Protocol)*
 - analysis flags, 259
 - analysis flags display filter, 140
 - auto-complete filtering, 144
 - conversation filtering, 169–72
 - delay detection, 89–93
 - delta time column, 91–93
 - delta time preference setting, 97
 - dissector, 67
 - Follow a Stream, 170
 - graphing analysis flags, 259–63
 - handshake analysis, 177
 - large TCP delta time filter, 186
 - Maximum Segment Size (MSS), 11
 - preference settings, 276
 - reassembly (following streams), 267
 - small window size display filter, 145
 - Stream Index field filter, 172
 - TCP Segment of a Reassembled PDU listing, 74
 - Timestamps (Wireshark), 91
 - zero window display filter, 140
- Teredo IPv6 traffic*, 379
- TFTP (Trivial File Transfer Protocol)*
 - detect in Protocol Hierarchy, 239–40
 - display filter, 139
- throughput analysis*, 263, 363
- Time column, troubleshooting with*, 89–93
- Time to Live field*
 - description, 379
- top talkers*, 232–33
- trace files*
 - convert .pcapng to .pcap, 280
 - on *www.wiresharkbook.com*, 360
 - other formats, 52
 - splitting, 301
 - using Capinfos for details, 300
 - work with file sets, 302
- Track number of bytes in flight setting*, 74–76, 79, 82

traffic paths, 13–17

transport name resolution, 374

troubleshooting

- "T-" coloring rule names, 206
- packet loss, 253
- receive buffer congestion indications, 254
- recognize background traffic, 47
- recommended analyzer placement, 107
- router introducing problems, 256
- UDP-based applications, 186
- with the Expert Information window, 253–56

Tshark

- definition of, 379
- exporting statistics, 321–25
- extract GET Requests, 320–25
- key options, 298
- overview, 311–12

UDP (User Datagram Protocol)

- conversation display filtering, 169–72
- definition of, 379
- Follow a Stream, 170

URI (Uniform Resource Indicator)

- definition of, 379
- display filter, 163, 165

web browsing. **See also HTTP**

- adding a Host column, 150
- capture techniques, 110
- detecting 404 errors, 168
- DNS overhead, 141
- export objects, 276–80
- filtering on requests, 142–43

- find hidden messages, 269–70

- ideal filters for, 154, 157–58

- reassembling traffic, 267

- sample analysis, 45–47

- TCP delta times, 98

wiki.wireshark.org web site, 18–19

wildcard filters, 184–85

Window Full notes, 255

window updates, 259

Window updates, 255

WinPcap, 7, 112, 373, 377, 380

Wireshark (general)

- awards, 3
- capabilities, 3
- Developers' Guide, 58
- directories, 83, 85, 152, 299, 306, 310
- downloading, 6
- Q&A Forum, 58
- supported OSes, 3, 6

Wireshark tasks

- application analysis, 5
- general analysis, 4
- security analysis, 5
- troubleshooting, 4

wiretap library, 9, 52, 380

WLAN (Wireless Local Area Network)

- adapters, 106
- capture techniques, 106–7
- definition of, 380

Zero Window Probe ACK notes, 255

Zero Window Probe notes, 255

Zero Window warnings, 255