

INDEX

!= warnings, 51

A

ACKed Unseen Segment. *See also TCP*

- cause of, 191
- defined in *tcp-packet.c* file, 192
- filter for, 193
- in Expert Infos window, 193
- overview, 191
- warning before analyzing, 192

Acknowledgment Number column, 159, *See also TCP*

address resolution

- host names, 42
- problems, 100

Address Resolution Protocol. *See ARP*

Advanced IO Graphs. *See also graphs*

- define impact of packet loss (*tcp.analysis* filters), 295
- determine throughput (*tcp.len*), 271
- identify general delays
(*frame.time_delta_displayed*), 118
- identify TCP delays (*tcp.time_delta*), 132
- overview of Calc functions, 270
- Window Size problems, 291, 293

AirPcap adapter, 83, 353, 367, *See also capture*

Allow subdissector to reassemble TCP streams, 62, *See also protocol preferences*

annotations

- definition of, 353, 362
- Expert Infos Packet Comments, 56
- file annotation button versions, 305
- recommendations for using, 319

application

- causing Zero Window conditions, 212
- keep alives, 108

- service refusals, 3
- slow DHCP responses, 285
- slow DNS responses, 137
- slow HTTP server responses, 143
- slow SMB/SMB2 responses, 145
- symptoms of slow applications, 18
- symptoms of slow servers, 4

Apply as Filter. *See also display filters*
ARP

- description of protocol, 353
- Request, 97
- resolution problem, 100

ask.wireshark.org, 329, 334, *See also web sites*

asterisk on Title Bar, 306

asymmetric routing, 191

- definition of, 353
- overview of problems, 9

B

background traffic, definition of, 353

Bad TCP

- button, 161
- coloring rule, 161
- the "Golden Graph", 280

Bae, Hansang, 12, 110

bandwidth throttling, 11

baselines, 14, 331

Bongertz, Jasper, 26, 330

**Bootstrap Protocol (BOOTP),
definition of**, 354

BPF (Berkeley Packet Filtering) syntax, 353

broadcasts

- capturing from switches, 78
- definition of, 354
- storms, 13

browser timeout, 103

butt-ugly coloring rule, 70

Bytes in Flight, 6

adding column for, 212

definition of, 354

detect "stuck" application, 212

C

Calculate conversation timestamps setting.

See also protocol preferences

Calculated window size field. See also TCP

Capinfos

description of, 354

for trace file details, 315

use before Editcap, 81

capture

802.11 header, 83

aggregating taps, 80

AirPcap adapters, 83

capture filters, 88

Capture Options window, 85

dropped packets, 81

dumpcap, 81

half-duplex hubs, 80

high traffic rate links, 81

location tips, 24, 77, 81

maximum file size, 81

monitor port, 79

on target machine, 78

oversubscribed switch, 79

possible problems, 95

switched network options, 78

tcpdump or dumpcap, 24

to file sets, 85

using a tap, 79

WLAN options, 82

capture devices

AirPcap adapters, 26

hubs, 80

Shark Appliance, 81

taps, 80

Capture Engine, description of, 354

capture filters

description of, 354

dropping desired traffic, 95

MAC address, 88

use sparingly, 88

capture interface, description of, 354

Cascade Pilot

description of, 354

detecting suspect traffic, 318

favorite Views, 317

open large trace files, 316

recommended tool, 26

sample network analysis report, 318

TCP Flags Distribution View, 320

Chanalyzer software, 328

Checksum Errors. See also Ethernet, TCP, and IP

cause of, 229

caused by task offloading, 229

defined in *tcp-packet.c* file, 230

description of, 355

in Expert Infos window, 231

overview, 229

checksum validation

disabling, 339

settings, 229

CIDR (Classless Interdomain Routing),

definition of, 355

colorfilters file. See coloring rules

coloring rules

background color, 71

colorfilters file, 69

disabling, 73

DNS Error, 72

order of, 72

columns

adding, 35

change column name, 115

create delta time column, 114

displaying, 38

hiding, 38

HTTP response time, 37, 141

preferences file location, 38

renaming, 37

resizing, 115

SMB response time, 145

stream index, 101

TCP Sequence Number field, 159

comparison operators, description of, 355

connection refusals. See TCP

conversations

- Conversations window, 65
- display filter, 65
- filtering on a UDP conversation, 112
- graphing, 263
- statistics, 120

core engine, description of, 355

CSV (Comma-Separated Value) format, description of, 355

D

default gateway, 97

Degioanni, Loris, 26, 354, 367

delayed ACKs

- description of, 355
- Hansang Bae presentation about, 12
- problems related to, 110
- problems with Nagle algorithm, 6
- timers, 110

delays. See also DHCP, DNS, HTTP, SMB, TCP

- affect on Duplicate ACK count, 57
- before FIN/RST packets, 108
- before Keep Alives, 108
- before Window Updates, 110
- between SYN and SYN/ACK, 10, 109
- between SYN/ACK and ACK, 10, 109
- caused by delayed ACK, 110
- caused by lousy routing paths, 11
- checklist for detecting client issues, 28
- checklist for measuring, 28
- create a delta time column, 114
- create a displayed delta time column, 116
- delayed ACK issues, 6, 12, 110
- in the middle of a data stream, 110
- in UDP communications, 112
- measuring path latency, 39
- measuring round trip time (RTT), 128
- measuring with the TCP handshake, 132
- measuring with the Time column, 39
- normal and acceptable, 107
- path latency problems, 10, 109
- preceding application Keep Alives, 108

- preceding client requests, 108
- preceding DNS queries, 107
- preceding FIN/RST packets, 108
- preceding server responses, 109
- preceding TCP Keep Alives, 108
- preceding TLSv1 Encrypted Alerts, 108
- preceding Window Update, 110
- queuing along a path, 174, 277
- TCP Delay button, 125
- tips for measuring, 323
- tracking TCP conversation timestamps, 120

delta time (frame time)

- column, 117
- description of, 355

delta time (TCP). See also TCP

- description of, 356

dfilters file. See display filters

DHCP (Dynamic Host Configuration Protocol)

- definition of, 356
- relation to BOOTP, 354

Differentiated Services Code Point (DSCP), definition of, 356

display filters

- != warning, 71
- application name, 46
- Apply as Filter, 353
- bootp, 354
- conversation, 44
- definition of, 356
- dfilters file, 322, 356
- DNS, 99
- exclusion filter, 51
- field existence, 47
- field value, 47
- from the Conversation window, 65
- in Tshark (-Y parameter), 249
- inclusion filter, 359
- IPv4 address, 95
- IPv4 subnet, 43
- IPv6 address, 95
- MAC address, 95
- port number, 45
- Prepare a Filter, 363
- remove DNS and DHCP, 52

TCP handshake first two packets, 129
 TCP handshake second packet, 130
 TCP handshake's last two packets, 130
 TCP Stream Index, 122

dissectors

definition of, 356
packet-dns.c file, 237
packet-http.c file, 241
packet-smb.c file, 245
packet-smb2.c file, 245
packet-tcp.c file, 56, 153, 157

DNS

"DNS Errors" filter expression button, 238
 definition of, 356
 delta time, 136
 detecting delays, 112, 135
 display filter, 99
 dns.flags.rcode > 0 filter, 47, 71, 237
 dns.flags.rcode > 0 filter expression
 button, 308
 dns.time field, 41, 112
 dns.time filter, 135
 error responses, 47, 69
 graph delays, 138
 name errors, 237
 No Such Name response, 99
 overview of traffic, 135
 Query Name column, 239
 Reply Code field, 70
 Reply Codes, 237
 response time, 41
 server error example, 240
 server failures, 237
 traffic overview, 237
 Transaction ID field, 69

DoS attack captured, 81**Dropbox traffic, 52****dumpcap**

definition of, 356
 for high traffic rate networks, 25
 location of, 81
 used by Wireshark, 81

Duplicate ACKs. See also TCP

cause of, 57, 167
 containing SACK Left Edge/Right Edge
 details, 171
 defined in Acknowledgment Number
 field, 166
 defined in *tcp-packet.c* file, 168
 filter for, 169
 high number of, 57
 in Expert Infos window, 170
 overview, 166

E**Editcap, 81**

definition of, 357
 splitting trace files into a file set, 315

EKG pattern in IO Graph, 12**error responses**

DNS, 47, 237
 FTP, 255
 HTTP, 241
 SIP, 250
 SMB/SMB2, 245

Ethereal, 357**Ethernet**

definition of, 357
 header, 357
 trailer, 357
Validate the Ethernet checksum if possible
 preference, 233

exclusion filter. See also display filters

definition of, 357
 example, 51

Expert Infos, 357. See also TCP

Chats tab, 56
 Checksum Errors, 56, 231
 Comments tab, 56
 Count column, 58
 Details tab, 56
 Errors tab, 56
 Fast Retransmissions, 184
 Notes tab, 56
 Out-of-Order Packets, 179
 overview, 56

- Previous Segment not Captured, 162
- Reused Ports, 225
- Warnings tab, 56
- Window Update, 220
- Zero Window Probe, 217
- Zero Window Probe ACK, 217

export

- columns to CSV format, 301
- objects, preference settings for, 63
- packet details, 309
- packets, 27
- packets to .txt format, 308
- trace file and packet comments, 305

F

Fast Recovery process, 156, *See also* **TCP**

Fast Retransmissions. *See also* **TCP**

- 20 ms arrival time, 181
- also marked as Retransmissions, 183
- cause of, 181
- defined in *tcp-packet.c* file, 181
- filter for, 183
- in Expert Infos window, 184
- overview, 180
- vs. Out-of-Order packet, 167

file sets, 85

File Transfer Protocol. *See* **FTP**

filter expression buttons

- Bad TCP, 161
- DNS delays, 137
- DNS Errors, 69, 238
- editing, 54
- HTTP Errors, 243
- HTTP response time, 143
- overview, 53
- removing GET from TCP delay button, 127
- SIP Errors, 253
- SMB/SMB2 Errors, 248
- TCP delays, 126
- TCP handshake, 130

firewall blocking TCP connection, 4, 101

flat-line graph appearance, 293

Follow TCP Stream, 243

frame, 357

frame.time_delta, 112

frame.time_delta_displayed, 112, 115, 117

Franklin, Benjamin, 105

FTP

- command channel, 45
- data channel, 45
- definition of, 358
- download, 45
- FTP Errors filter, 255
- ftp.response.code > 399, 257
- ftp.response.code >= 400, 257
- PASV command, 45
- predefined Response Codes, 255

G

GIMP graphical toolkit, 358

Go To First Packet function, 115

Golden Graph. *See* **graphs**

graphs

- basic function, 67
- Calc COUNT FRAMES(*), 270
- Calc LOAD(*), 270
- Calc MIN, AVG and MAX(*), 270
- Calc SUM(*), 270
- compare HTTP and FTP downloads, 268
- conversations, 264
- DHCP Offer packets, 285
- DNS delays, 138
- exported data in Excel, 304
- flat-line ceiling, 293
- Golden Graph, 280
- graph line ordering, 287
- high delta times of a TCP-based application, 286
- high delta times of a UDP-based application, 285
- HTTP response time, 144
- logarithmic scale, 269
- low throughput, 275
- name resolution, 267
- packet loss, 295
- packet loss in multicast stream, 279
- queuing delays in multicast streams, 277
- single application traffic, 267
- SMB response times, 149
- TCP delta time, 132

TCP payload only, 271
 TCP window size problems, 291
 tcp.analysis.duplicate_ack, 295
 tcp.analysis.lost_segment, 295
 tcp.analysis.retransmission, 295
 tcp.analysis.window_full, 291
 tcp.analysis.window_update, 291
 tcp.analysis.zero_window, 291
 tcp.time_delta, 286
 Time-Sequence Graph (tcptrace), 297
 UDP traffic, 117
 using to navigate, 68
 Window Scaling Graph, 294
 with port-based filters, 267

H

hardware address resolution problems, 15
heuristic dissector, description of, 358
hexadecimal, 358
hosts file, 97, 358
HP OfficeJet traffic analysis, 210
HTTP
 "HTTP Errors" filter expression button, 243
 3xx Redirection, 5, 241
 4xx Client Errors, 241
 5xx Server Errors, 241
 conversation analysis, 103
 delay before response, 109
 detect delays, 139
 GET Request Method, 47
 http.request.method filter, 47, 133
 http.response.code > 399 filter, 241
 http.response.code >= 400 filter, 241
 http.time column, 37, 141
 http.time field, 59
 http.time filter, 139, 143
 incorrect response time, 61
 POST Request Method, 47
 reassembling objects, 63
 Response Code on wrong packet, 59
 Response Codes (Status Codes), 241
 response packet hyperlink, 60
 response time column, 141
 response time measurement, 59, 139

TCP preference setting effect on http.time results, 139
 traffic overview, 139, 241

HTTPS

definition of, 358
 sample trace file, 275
 TCP preferences recommendation, 141
Hypertext Transfer Protocol Secure. See HTTPS

I

IANA (Internet Assigned Numbers Authority), 358

ICMP

definition of, 359
 Neighbor Solicitation, 100
 Redirect, 13
 Router Advertisements, 98
 Router Solicitation, 98, 100
 Type 3/Code 3 (Destination Unreachable/Port Unreachable), 3

ifconfig, 88

inclusion filter, 359, *See also display filters*

Internet Control Messaging Protocol.

See ICMP

Internet Protocol. See IP

IP

addresses, definition of, 359
 definition of (IPv4/v6), 359
 IP address filter, 359
 IP header, 356
 ip.checksum_bad==1 filter, 229
 IPv4 *Validate the IPv4 checksum if possible*, 231

ipconfig, 88

K

Keep Alive ACKs (TCP). See also TCP

defined in *tcp-packet.c* file, 196
 filter for, 197
 in Expert Infos window, 198
 overview, 195

Keep Alive Probe packets. See Keep Alives (TCP)

Keep Alives (TCP)
 cause of, 195
 defined in *tcp-packet.c* file, 196
 filter for, 197
 in Expert Infos window, 198
 overview, 195
 used in Window Zero situations, 199

key hosts, 359

L

latency. See also delays
 definition of, 359

libpcap, definition of, 359

link-layer driver, definition of, 359

location resolution, 97

logical operators, description of, 359

lost packets. See Previous Segment Not Captured

low Maximum Segment Size (MSS) problems, 275

low window size, 7, **See also window size**

Lyon, Gordon (Nmap Founder), 361

M

MAC address
 capture filter, 88
 definition of, 360
 resolution, 97

malware symptoms, 14

manuf file, 360

Maximum Segment Size (MSS), definition of, 360

Maximum Transmission Unit (MTU), definition of, 360

Mergecap, definition of, 360

metadata, 360

Microsoft Open Specification, 145

Monitor Mode, 83

multicasts
 capturing from switches, 78
 definition of, 360
 delayed by queuing, 277
 packet loss detection, 279
 storms, 13

N

Nagle algorithm, 6, 110

name resolution. See also DNS
 definition of, 361
hosts file, 358
 in Conversations window, 112
 overview, 97
 problems, 14, 47, 98
 resolution flow chart, 96
 transport name resolution, 361
 Wireshark function, 361

Netgroup Packet Filter, 229

network address resolution. See name resolution

Network Address Translation (NAT), 361

Network Basic Input/Output System (NetBIOS), 361

network interface card (NIC), 361

Next Sequence Number
 field. **See** TCP, Next Sequence Number

nextseq value, 154

Nmap, 361

O

Out-of-Order packets. See also TCP
 3 ms arrival time, 176
 cause of, 174
 defined in *tcp-packet.c* file, 175
 filter for, 178
 in Expert Infos window, 57, 179
 overview, 174
 vs. Retransmissions and Fast Retransmissions, 175

overloaded router, 12

oversubscribed switches
 ACKed Unseen Segments, 27
 definition of, 361

P

Packet Bytes pane
 definition of, 362
 SACK missing fields, 172

packet comments. See annotations

Packet Details pane

- definition of, 362
- expanding sections, 36
- Frame section metadata definition, 360
- packet comments, 353

Packet List pane

- add custom columns, 36
- default columns, 35
- definition of, 362
- export column data, 301

packet loss. See also TCP, Previous Segment Not Captured

- calculating missing byte count, 160
- cause of, 155
- detection by Wireshark, 155
- find location of, 163
- move downstream, 164
- move upstream, 164

packet size

- example of low throughput due to, 275
- finding average, 276
- graphing issues with, 275
- Length column, 28
- low MTU size issues, 17
- tcp.len field, 276

packet, definition of, 361

pcap, definition of, 362

pcapng, definition of, 362

Per-Packet Interface (PPI), definition of, 363

personal configuration folder, 69

pkt_comment filter, 353

port number reused. See Reused Ports

port resolution, 97

port spanning, definition of, 362

port-based filters, 45, 267

PPI header, 325

preference settings. See protocol preferences

Prepare a Filter, 47

Previous Segment not Captured. See also TCP

- cause of, 155
- defined in *tcp-packet.c* file, 157
- filter for, 158
- in Expert Infos window, 57, 162
- overview, 154

printing, analyzing "ink drying" problem, 213

prioritize troubleshooting tasks, 67

profiles

- classic option, 34
- creating new, 33
- Default, 33
- definition of, 363
- import Laura's Troubleshooting Profile, 337
- step-by-step instructions, 339

Protection Against Wrapped Sequence Numbers (PAWS), 48

Protocol Data Unit (PDU), definition of, 363

Protocol Hierarchy, definition of, 363

protocol preferences

- Allow subdissector to reassemble TCP streams,* 59, 61, 139, 140, 339
- Calculate conversation timestamps,* 119, 120, 123, 339, 356
- definition of, 363
- preferences file, 363
- Relative sequence numbers,* 226
- right-click method for setting, 64
- set using Edit menu item, 141
- set using the Edit Preferences button, 141
- TCP reassembly, 59
- Validate the Ethernet checksum if possible,* 233, 339
- Validate the IPv4 checksum if possible,* 57, 231, 233, 339
- Validate the TCP checksum if possible,* 231, 233, 339
- Validate the UDP checksum if possible,* 231, 233, 339

proxy devices

- definition of, 363
- mismatched parameters across, 8

Q

Quality of Service (QoS), 363

queuing along a path, 12, 174, 277

R

Radio Frequency (RF), definition of, 364

Radiotap header

- example of, 326
- prepending, 325

recommendations

- analyzing TCP-based applications, 323
- ask for help, 334
- Cascade Pilot, 316
- create baselines, 331
- intermittent problem analysis, 324
- learn TCP/IP well, 332
- maximum file size, 315
- naming trace files, 319
- quickly build the Golden Graph with a Bad TCP display filter, 321
- sanitize trace files, 329
- trace file log book, 319
- use a ring buffer, 324
- use annotations, 319
- WLAN capture, 325

redirection

- definition of, 364
- HTTP 3xx responses, 5
- route, 13

relative start (Rel.Start), 364**responses, lack of, 103****Retransmission Time Out (RTO). See****Retransmissions****Retransmissions. See also TCP**

- cause of, 186
- defined in *tcp-packet.c* file, 187
- definition of, 364
- filter for, 188
- in Expert Infos window, 189
- overview, 186
- Retransmission Time Out (RTO), 186
- Retransmission Timeout (RTO) timer, 157
- vs. original packet, 165
- vs. Out-of-Order packet, 167

Reused Ports. See also TCP

- cause of, 223
- defined in *tcp-packet.c* file, 223
- filter for, 224
- in Expert Infos window, 225
- overview, 222

RFCs

- RFC 1122, "Requirements for Internet Hosts -- Communication Layers", 12, 355
- RFC 1323, "TCP Extensions for High Performance", 16, 48, 202

RFC 2018, "TCP Selective Acknowledgment Options", 16

RFC 5681, "TCP Congestion Control", 166

RFC 793, "Transmission Control Protocol", 104

ring buffer, 324**round trip time (RTT)**

- causes for high RTT, 41
- example measuring, 333
- graphing, 132
- measuring, 39, 40, 131
- measuring with TCP handshake, 109, 128
- RTO timer use of, 186
- tips for using, 323

route resolution, 97**routing loops, 9****routing path problems, 11****S****sanitize trace files**

- using a hex editor, 329
- using TraceWrangler, 330

Selective ACK

- in Duplicate ACKs, 172
- missing in Duplicate ACKs, 7
- missing in handshake, 53
- Unsupported, 16

Selective Acknowledgment (SACK). See Selective ACK**Sequence Number field. See TCP, Sequence Number****server**

- application fault, 5
- DNS error messages, 69
- HTTP error messages, 241

Server Message Block (SMB). See SMB**Server Message Block Version 2. See SMB2****service request, no response to, 103****Service Response Time (SRT) statistics, 148****services file, 97, 364****Session Initiation Protocol (SIP). See SIP****Set Time Reference**

- bug in resetting Time column, 207
- measuring delay impact, 189
- measuring Zero Window delays, 206

Shark Appliance (Cascade), 81

Sharkfest conference

- demonstration of TraceWrangler, 26
- DoS attack during, 81
- information about, v
- Jasper Bongertz, 330

Simple Network Management Protocol (SNMP), definition of, 364**SIP**

- "SIP Errors" filter expression button, 253
- 3xx Redirection, 5, 250
- 4xx Client Error, 250
- 5xx Server Error, 250
- 6xx Global Failure, 250
- sip.Status-Code > 299 &&
sip.Status-Code < 400, 5
- Status Codes (Response Codes), 250
- traffic overview, 250

slow server response. See delays**SMB**

- "SMB Errors" filter expression button, 248
- definition of, 364
- detecting delays, 145
- Negotiate Protocol response, 248
- NT Status codes, 245
- reassembling objects, 63
- Service Response Time, 145, 148
- smb.nt_status > 0 ||
smb2.nt_status > 0, 245
- smb.time, 145
- traffic overview, 145, 245
- version 2, 145

SMB2

- "SMB2 Errors" filter expression button, 248
- smb2.time, 145
- traffic overview, 245

Snort, definition of, 365**spanning. See switches****Spanning Tree Protocol (STP), definition of, 365****Status Bar**

- active profile, 33
- annotation button versions, 305
- current profile, 363
- displayed packet count, 43

Stream index, definition of, 365**stream reassembly, definition of, 365****subdissector, definition of, 365****subnet filter, 43****subnet, definition of, 365****Summary statistics, 276****suspicious traffic, 14****switches**

- loop problems, 13
- oversubscription description, 361
- oversubscription symptom, 191
- port spanning, 79

SYN bit. See TCP, SYN bit**T****TAP ("Test Access Port")**

- definition of, 365
- recommendation, 79

task offloading

- checksum errors symptom, 229
- definition of, 365
- disable checksum validation, 233

TCP

- Acknowledgments, definition of, 353
- attributes altered along path, 7
- Bytes in Flight column, 6, 212
- connection refusal, 3, 101
- Conversations window, 65
- delays
 - before FIN/RST packets, 108
 - before final handshake packet, 109
 - before Keep Alives, 108
 - before SYN/ACKs, 109
 - before TLS Encrypted Alerts, 108
 - before Window Updates, 110
 - delayed ACK issues, 6, 12, 110

Expert Infos filters

- tcp.analysis.ack_lost_segment, 191
- tcp.analysis.duplicate_ack, 166, 169
- tcp.analysis.fast_retransmission, 180
- tcp.analysis.flags, 161
- tcp.analysis.flags &&
!tcp.analysis.window_update, 280
- tcp.analysis.keep_alive, 195
- tcp.analysis.keep_alive_ack, 195
- tcp.analysis.lost_segment, 154, 155, 158
- tcp.analysis.out_of_order, 174, 178
- tcp.analysis.retransmission, 186

- tcp.analysis.reused_ports, 222
- tcp.analysis.window_full, 208
- tcp.analysis.window_update, 161, 218
- tcp.analysis.zero_window, 201
- tcp.analysis.zero_window_probe, 215
- tcp.analysis.zero_window_probe_ack, 215
- FIN
 - acceptable delays preceding, 108
 - FIN (Finish) bit, definition of, 357
 - WAIT states, 103
- graphs
 - TCP delta time, 132
 - tcp.analysis.duplicate_ack, 295
 - tcp.analysis.lost_segment, 295
 - tcp.analysis.retransmission, 295
 - tcp.analysis.window_full, 291
 - tcp.analysis.window_update, 291
 - tcp.analysis.zero_window, 291
 - tcp.time_delta, 286
 - Window Size problems, 291
- handshake analysis
 - missing SACK, 53
 - missing Window Scaling, 53
 - tips, 323
- illogical flags set, 320
- low Window Size problems, 48
- multiple simultaneous connections, 102
- Next Sequence Number
 - column, 159
 - Duplicate ACK detection, 166
 - field definition, 154
 - nextseq* in *packet-tcp.c*, 154, 157
- packet loss, 58, 154
- preference settings
 - Calculate conversation timestamps*, 119
 - reassembly preference setting, 59
 - Track Number of Bytes in Flight*, 212
 - Validate the TCP checksum if possible*, 231
- receive buffer full, 6
- relative sequence numbers, 226
- RST
 - acceptable delays preceding, 108
 - RST (Reset) flag, definition of, 364
- Sequence Number
 - column, 159
 - field, 154
- Stream Index
 - column, 123
 - field, 101
 - filter, 122
- SYN
 - SYN (Synchronize Sequence Numbers)
 - flag, definition of, 365
 - SYN bit filter, 53
 - SYN retransmissions, 102
- tcp.ack filter, 131
- tcp.checksum_bad==1 filter, 229
- tcp.flags.ack filter, 131
- tcp.flags.fin filter, 131
- tcp.flags.syn filter, 131
- tcp.len > 0 filter, 131, 276
- tcp.len value, 271
- tcp.options.sack_perm filter, 53
- tcp.options.wscale.multiplier filter, 53
- tcp.port==80 filter, 267
- tcp.seq filter, 131
- tcp.stream field, 119
- tcp.stream filter, 122
- tcp.time_delta column, 123
- tcp.time_delta field, 120
- tcp.time_delta filter, 128
- tcp.time_relative field, 120
- tcp.window_size filter, 48
- Time-Sequence Graph (tcptrace), 297
- unsuccessful connections, 124
- Window Scaling missing in handshake, 53
- Zero Window conditions, 199, 201, 204, 206, 208
- Zero Window Probes, 200, 215
- Zero Window Updates, 200
- TCP handshake. See TCP, handshake analysis**
- tcpdump, 25, 81**
- throughput**
 - definition of, 366
 - graphing, 264
 - measuring, 67
- time. See delays**
- Time column**
 - default, 114
 - measure delays, 68
 - precision, 40
 - settings, 39
- time stamps, 39**

Time to Live (TTL) field, description of, 366

TLS

- Close Encrypted Alert, 108
- delays before TLSv1 Encrypted Alerts, 108
- Encrypted Alerts, 108

top talkers, 65

trace files

- description of, 366
- integrity, 25, 27
- on *www.wiresharkbook.com*, 345
- referenced in this book, 347

TraceWrangler, 26, 330, 366

Transmission Control Protocol. See TCP

Transmission Control Protocol/Internet Protocol (TCP/IP), definition of, 366

Transport Layer Security (TLS), description of, 366

Trivial File Transfer Protocol (TFTP), definition of, 366

troubleshooting checklist, 27

troubleshooting profile, 33

Troubleshooting_Book_Profile.zip, 337

Tshark

- creating trace file subsets, 315
- definition of, 366
- display filters in, 249

U

UDP

- conversation delays, 112
- definition of, 366
- graphing delays, 117
- header format, 112
- most active conversation, 112
- udp.checksum_bad==1 filter, 229
- Validate the UDP checksum if possible, 231*

Uniform Resource Indicator (URI), definition of, 367

unknown hardware address, 78

User Datagram Protocol. See UDP

V

virus symptoms, 14

W

weak signal, 9

web sites

- bit.ly/delayedack, 110*
- wiki.wireshark.org/CaptureFilters, 90*
- wiki.wireshark.org/CaptureSetup/WLAN, 83*
- wiki.wireshark.org/Development/PcapNg, 362*
- www.insecure.org, 240*
- www.lovemytool.com, 330*
- www.metageek.net, 328*
- www.nmap.org, 240*
- www.riverbed.com, 26, 318*
- www.snort.org, 365*
- www.tracewrangler.com, 26*
- www.wiresharkbook.com/resources.html, 26, 334*
- www.wiresharkbook.com/troubleshooting.html, 318*

Window Full. See also TCP

- cause of, 208
- defined in *tcp-packet.c* file, 209
- example of, 213
- filter for, 210
- in Expert Infos window, 211
- overview, 208

Window Scaling. See also TCP

- graph, 294
- Shift Count, 202
- unsupported, 16, 53

window size. See also TCP

- above 65,535 bytes, 53
- window size low, 48
- Window Size Value field, 202

Window Update. See also TCP

- cause of, 218
- defined in *tcp-packet.c* file, 218
- delays preceding, 50
- example of, 206, 220
- excluded from, 218
- filter for, 219
- in Expert Infos window, 220
- near a delay, 68
- overview, 218

Window zero. See Zero Window

WinPcap, 229, 359
 definition of, 367
Wireless Local Area Network (WLAN),
 definition of, 367
Wireless Toolbar, 84
Wiretap library, definition of, 367
Wi-Spy adapter, 328
WLAN
 malformed frames, 327
 Management, Control and Data frames, 82
 Monitor Mode, 83
 native adapter capture, 82
 native adapter problems, 325
 PPI header, 83
 Radiotap header, 83
 Retries, 9, 326
 SSI (Signal Strength Indication) Signal
 (dBm) value, 326
 weak signal, 9
 wlan.fc.retry == 1, 326

X

X-Slogan detection, 89

Z

Zero Window. See also TCP
 cause of, 201
 defined in *tcp-packet.c* file, 203
 example of, 204
 filter for, 203
 graphing recovery from, 291
 in Expert Infos window, 204
 measure delays, 206
 overview, 201
 preceded by Window Full, 205
Zero Window Probe. See also TCP
 analyzing with a Bytes in Flight
 column, 217
 cause of, 215
 defined in *tcp-packet.c* file, 215
 filter for, 216
 in Expert Infos window, 217
 overview, 215
Zero Window Probe ACK. See also TCP
 cause of, 215
 defined in *tcp-packet.c* file, 215
 filter for, 216
 in Expert Infos window, 217
 overview, 215