Wireshark® 101
Essential Skills for Network Analysis

1st Edition

Always ensure you have proper authorization before you listen to and capture network traffic.

Protocol Analysis Institute, Inc
5339 Prospect Road, # 343
San Jose, CA 95129 USA
www.packet-level.com

Chappell University
info@chappellU.com
www.chappellU.com

Index

!= filter operator, 161–62
4 NOPs in a Row warning, 235
6to4 traffic, 329
ACKed Lost Packet warnings, 233
addresses. See IP (Internet Protocol) or MAC (Media Access Control)
AirPcap adapter, 92–93, 329, 342
Allen, Lanell, 245
Allow subdissector to reassemble TCP streams setting, 62–65, 80, 133, 197, 231–32, 246, 249, 256, 258, 309, 317
analysis steps (typical), 9
annotations
  button on Status Bar, 30
  comment column, 265
  definition of, 329
  exporting comments, 267
  packet and file options, 262
  packet comments, 264–65
  pcapng format required, 265
application analysis
  capture filters, 116–20
  techniques, 220–29
ARP (Address Resolution Protocol)
  description of protocol, 329
  display filter, 125
  example, 33
  exclusion display filter, 154, 161
  poisoning, 236
  Source and Destination columns, 24
ASCII (American Standard Code for Information Interchange), 29, 203, 329
ask.wireshark.org web site, 18–19
auto-complete mechanism, 130
autostop condition, 286–88
background traffic
  definition of, 330
  example analysis of, 40–45
  file transfers on startup, 160
bandwidth usage, 226
Bejtlich, Richard, 1
Blok, Sake, 209
Bootstrap Protocol (BOOTP), 125, 145, 330
BPF (Berkeley Packet Filtering) syntax, 8, 107–8, 116, 126, 289, 330
broadcasts
  background traffic, 43
  capture filter, 109
  definition of, 330
  DHCP ACK example, 40
  Dropbox example, 35
  switches forward, 16
Broman, Anders, 261
build a network picture from packets, 32
Calculate conversation timestamps setting, 62–63, 65, 68, 77, 172–73, 304, 331
Capinfos, 275
capture
  locations, 12–16, 89–95
  options, 111, 113, 119
  options quick reference, 88
  process overview, 7
  to file sets, 99
  with ring buffer, 103
Capture Engine
  description, 330
  functionality, 7
  reduce load on, 105

capture filters, 107–21
applying, 88
based on ICMP Type/Code numbers, 118
description, 330
listing available, 119
purpose of, 96, 105
recommendation to avoid, 105
with command-line capture, 289
capture interface description, 330
Cascade Pilot, 98, 270, 331
cfilters (capture filters) file, 69, 175
checksum errors
coloring rule, 188–89
description, 331
CIDR (Classless Interdomain Routing)
definition of, 331
subnet display filtering, 147
client latency, 74
colorfilters (coloring rules) file, 69
coloring rules
adding a column, 186–87
checksum errors, 188–89
creating, 190, 192
disabling, 188
highlighting conversations, 195–97
highlighting delays with, 190–92
highlighting FTP passwords, 193–94
right-click method, 192
which coloring rule is applied, 185
columns
Apply as Column, 49, 53, 77, 83, 134, 159
create using Preferences, 50
creating, 49–53
description of defaults, 24
editing, 50
hide/display/rename/remove, 26
removing using Preferences, 204
reordering, 25
sorting, 25, 51, 52
Combs, Gerald, 3
comparison operators, 131, 147, 331
configuration files, 69
conversation
filtering, 156–59, 213
most active, 216–17
statistics, 158, 160, 211, 214
core engine
description, 331
functionality, 8, 54
Degioanni, Loris, 47, 98, 331, 342
delays considered "normal", 80–81
delta time
coloring rule, 190
column, 52, 76
filters, 172
general description, 331
TCP delta time, 172
TCP description, 331
troubleshooting with, 75–84
dfilters (display filters) file, 69, 138, 175
DHCP (Dynamic Host Configuration Protocol)
definition of, 332
display filter not recognized, 145
host name display filter, 126
relation to BOOTP, 330
using `bootp` display filter, 145
display filters. See also dfilters file
… and Not Selected, 153
… and Selected, 153
… or Not Selected, 153
… or Selected, 153
Apply as Filter, 149–50, 329
color-coding (red, green, yellow), 166
definition of, 332
editing defaults, 137
excluding an IP address, 146
field name filters, 149–54
Filter Expression buttons, 176–80
importing, 174–75
`ip.addr !=` filter problem, 161
keyword detection, 167–69
logical operators, 161
on key words, 169
Prepare a Filter, 151, 338

range of addresses, 147
single IP address or host, 146
spotting traffic delays, 172–73
subnet, 147
syntax, 125–26
toolbar, 22
using "..." enhancements, 152–54
using "contains", 167
using "matches", 168
using host names, 146
using wildcards, 170–71
with auto-complete, 130, 133
with case insensitivity, 168
with command-line capture, 290

dissectors
definition of, 332
forcing, 57
functionality, 54–56
heuristic, 58
non-standard port numbers, 57–60

DNS (Domain Name System)
capture filters, 119–20
name error display filter, 155

dropped packets during capture, 105–7

DSCP (Differentiated Services Code Point), 332

DuBois, Betty, 87

Dumpcap
definition of, 332
overview, 284–85
stop conditions, 8

Duplicate ACKs notes, 233

Duplicate IP Address Configured warning, 236

Editcap
definition of, 332
key options, 274

Endpoint statistics, 215

error detection mechanism, 127

Ethereal, 3, 332

Ethernet
definition of, 333
dissector functionality, 55

exclusion filter, 150, 154, 333

Expert Infos, 30, 232, 265, 333
color-coded button on status bar, 30, 231
definitions, 233–36
display filters, 232
unreassembled indications, 231

exporting
conversations, 198–201
host names, 205–7
HTTP objects, 256
packet comments, 267–69
packet dissections, 52, 202, 268
packets, 172, 198–201
to CSV format, 52, 202, 204

expressions (display filter), 132

Fast Retransmission notes, 233

field names, 128

file sets, 99–100

Filter Expression buttons
creating, 176–80
definition of, 61
GET/POST button, 179
preferences file location, 177–80

filter toolbar (display filters), 22, 132

Fortunato, Tony, 323

frame definition, 10

Frame section
dissector, 54
metadata, 28

FTP (File Transfer Protocol)
argument display filter, 167
case-insensitive display filter, 168
command/data channel capture filter, 117
commands display filter, 126
definition of, 333
detect passwords, 193–94
filtering in IO Graph, 229
over a non-standard port number, 57
port number-based capture filter, 116
reassemble transferred files, 251–55
transport name resolution, 61
wildcard display filter, 171

Gentil, Lionel, 183
GeoIP
configuration, 218–19
location services, 215, 218
GIMP graphical toolkit, 8, 334
Gonder, John, 273
graphical interface elements, 2
heuristic dissector
description, 334
functionality, 58
missing, 57, 221
high traffic rates, 96–98
hosts file, 61, 285, 334
HTTP (Hypertext Transfer Protocol)
404 display filter, 155
add a Host field column, 53
analysis of slow browsing, 82–84
analyze a sample session, 38
auto-complete filtering, 130
basic display filter, 126
dissector, 56
error profile, 71
export objects, 256–59
File | Export Objects, 21
GET display filter, 128
GET filter using "contains", 131
GET/POST Filter Expression button, 179–80
headers preceding, 10
Host field display filter, 126, 133–36
normal .ico delays, 80
normal GET delays, 80
port number-based capture filter, 116
port number-based display filters, 140–44
preference setting, 59–60
reassembly techniques, 249–50
server delays, 80
String-Matching Capture Filter Generator tool, 117
TCP handshake preceding, 33
TCP preference settings effect, 62
traffic paths, 12
IANA (Internet Assigned Numbers Authority), 334
ICMP (Internet Control Message Protocol), 125, 334, 340
ifconfig, 111, 113, 139
importing profiles, 71–72
installation, 6
interfaces for capture, 92, 94
Internet Storm Center (ISC), 335
IO Graph
changing an axis, 226
file transfer problems, 240
`ip.addr` graphing, 227
`ip.src` graphing, 228
network errors, 238–39
port graphing, 229
quick reference, 210
subnet graphing, 230
IP (Internet Protocol)
dissector, 55
exclusion display filters, 146
IP address capture filter, 108–12
IP address filter, 335
IP header, 10, 332
low TTL display filter, 131
packet forwarding, 12–16
subnet capture filter, 109
subnet display filters, 146–48
Time to Live field, 14
`ip.addr != filter problem, 161`
ipconfig, 111, 113, 139
IPv6
address range display filter example, 147
capture filter, 109, 111
DNS AAAA record query, 38
GeoIP mapping, 218
ICMPv6 Neighbor Notification, 40
in Protocol Hierarchy Statistics, 220, 224
indication at *wireshark.org*, 48
most active conversation, 214
most active host, 215
multicast capture filter, 109

multicast example, 32
protocol display filter, 125
Router Advertisement, 40
single address display filter, 146
source/destination addresses in IO Graphs, 228
subnet capture filter, 109
toggle Interfaces view, 94
IRC (Internet Relay Chat) detection in Protocol Hierarchy, 221
Keels, Jennifer, 299
Keep-Alive ACK notes, 234
Keep-Alive warnings, 234
key hosts, 335
keyword filtering, 167–69
latency (client, server and path), 73–84
legal concerns, 5
libpcap, 6–7, 335
link-layer driver, 7, 335, 342
location for capture, 89–95
logical operators, 161, 335
Lyon, Gordon (Nmap Founder), 123, 337
MAC (Media Access Control) address
capture filter, 113–15
definition of, 335
frame definition, 11
local addressing only, 13
Main Toolbar, 22
manuf file, 61, 335
marking packets, 198
***matches** operator, 167–70, See also regex*
Menu Bar, 21
Mergecap, 282, 336
key options, 274
merging trace files, 282, See also Mergecap
metadata, 8, 28, 54, 92–93, 336
multi-adapter capture, 95
multicasts, 109
background traffic, 43
capture filter, 109
definition of, 336
IPv6 all hosts capture filter, 109
IPv6 all routers capture filter, 109
IPv6 example, 32
multiple file capture, 96–104, 119
name resolution settings, 61
NAT (Network Address Translation), 12, 336
NetBIOS (Network Basic Input/Output System), 336
network interface card (NIC), 337
Network Monitor .cap file format, 45
network name resolution, 61, 334, 336
Nmap, 337
Out-of-Order warnings, 234
overloaded client detection, 237
Packet Bytes pane, 49–53
definition of, 337
example of use, 136
overview, 29
packet comments. See also annotations
packet comments, see also annotations, 30, 263–66, 268, 337
packet definition, 10
Packet Details pane
analyzing background traffic in, 40–41
building a network picture from, 32
building columns using, 53
coloring rules in Frame section, 186
definition of, 337
effect on Status Bar, 30
enable TCP timestamp fields, 62
enable *Track number of bytes in flight*, 62
exporting contents, 203
Frame section metadata definition, 336
learning field names, 128
overview, 28
packet comments, 329
right-click coloring rules, 192
right-click filtering, 49, 149
right-click protocol settings, 64–66
TCP Delta filter, 172
Packet List pane. See also columns
overview, 23–27
right-click functionality, 27

packet loss condition
ACKed Lost Packet, 233
ACKed Lost Segment, 105
Duplicate ACKs, 233
Fast Retransmissions, 233
IO Graphing, 239
move your analyzer, 90
not dropped by Wireshark, 106
Previous Segment Not Captured, 105, 233
Retransmissions, 233
TCP analysis flags filter, 126
Tshark statistics, 294
path latency, 9, 73
pcapng
definition of, 337
purpose, 8
required for annotations, 30
personal configuration directory, 70
port number capture filters, 116–20
port spanning, 91, 338
preference settings
checksum validation settings, 188–89
definition of, 338
Filter Expressions buttons, 61
HTTP port numbers, 59
key protocol settings, 62–66
name resolution settings, 61
preferences file, 338
TCP settings, 77, 80, 172
user interface settings, 61
Previous Segment Not Captured warnings, 233
profiles
column on Status Bar, 31
creating, 67–72
definition of, 338
folder locations, 179
importing elements, 174–75
Protocol Data Unit (PDU)
definition of, 338
TCP setting effect on, 80
TCP setting effect on, 39
Protocol Hierarchy
"data" listing, 59
definition of, 338
launching, 220
suspicious traffic, 221
understanding listed percentages, 222
QoS (Quality of Service), 339
reassemble HTTP objects, 258
reassembly of conversations (following streams), 212, 247–55
receive buffer congestion indications, 234
Regex
definition of, 339
PERL definition of, 338
Use with ".", 170
using the `matches` operator, 168
relative start (Rel.Start), 339
Retransmission notes, 233
Reused Ports note, 235
ring buffer, see also multiple file capture, 101, 103
router
forwarding process, 14
problem indication, 235
removes/applies MAC header, 13
router/NAT forwarding process, 14
Router Advertisement packets, 40
RST (Reset), definition of, 339
security
analysis tasks, 5
capture techniques, 96
coloring rule naming, 192
creating special profile for, 67
detect suspicious protocols or applications, 225
proximity filtering, 171
Reused Ports Expert Infos note, 235
risks and vulnerabilities list, 335
Wireshark security fixes, 6
segment definition, 10
server latency, 74–75
services file, 61, 212, 339
settings. See preference settings

slow browsing, 16, 89, 96
SMB (Server Message Block)
definition of, 339
Status field display filter, 132
SNMP (Simple Network Management Protocol), 339
Snort, 340
Source and Destination columns, 24
split trace files, 275–81
sporadic network problems, 101
Start Page, 20
Status Bar, 30–31
Stream index, 247, 340
stream reassembly, 340
suspicious protocols/applications, 221, 225
switches, 13, 16, 106
SYN (Synchronize Sequence Numbers)
definition of, 333, 340
detecting delays with, 81
flag filter, 161–62
handshake example, 41
measure time with, 73
summary line filter, 164
wrong time column for delays, 79
taps for full-duplex capture, 91
TCP (Transmission Control Protocol)
analysis flags, 238
analysis flags display filter, 126
auto-complete filtering, 130
conversation filtering, 156–59
delay detection, 75–79
delta time column, 77–79
delta time setting, 83
dissector, 56
Follow a Stream, 157
graphing analysis flags, 238–42
handshake analysis, 164
large TCP delta time filter, 172
preference settings, 256
reassembly (following streams), 247
small window size display filter, 131
Stream index filtering, 159
TCP Segment of a Reassembled PDU listing, 62
zero window display filter, 126
Teredo IPv6 traffic, 341
TFTP (Trivial File Transfer Protocol)
detect in Protocol Hierarchy, 221
display filter, 126
throughput analysis, 242, 326
Time column, troubleshooting with, 75–79
Time to Live field
adding a column for, 50
description, 341
top talkers, 214–15
trace files. See also annotations
convert .pcapng to .pcap, 259
on *www.wiresharkbook.com*, 324
other formats, 44
splitting, 276
using Capinfos for details, 275
work with file sets, 278
Track number of bytes in flight setting, 62–63, 65, 68
traffic paths, 12–16
transport name resolution, 336
troubleshooting
"T-" coloring rule names, 192
packet loss, 233
receive buffer congestion indications, 234
recognize background traffic, 40
recommended analyzer placement, 93
router introducing problems, 235
UDP-based applications, 172
with the Expert Infos window, 233–36
Tshark
definition of, 341
exporting statistics, 292–96
extract GET Requests, 291–96
key options, 274
overview, 285

UDP (User Datagram Protocol)
conversation display filtering, 156–59
conversation filtering, 158
definition of, 341
Follow a Stream, 157
URI (Uniform Resource Indicator)
definition of, 341
display filter, 149, 151
web browsing. See also HTTP
adding a Host column, 136
capture techniques, 96
detecting 404 errors, 155
DNS overhead, 127
export objects, 256–59
filtering on requests, 128–29
find hidden messages, 249–50
ideal filters for, 140, 143–44
reassembling traffic, 247
sample analysis, 38–40
TCP delta times, 84
wiki.wireshark.org web site, 17
wildcard filters, 170–71
Window Full notes, 234
window updates, 238
Window Updates chats, 235
WinPcap, 7, 48, 98, 335, 339, 342
Wireshark (general)
awards, 3
capabilities, 3
directories, 69, 71, 138, 275, 282, 284
downloading, 6
mailing list, 6
supported OSes, 3, 6
Wireshark 1.9.x
Comment Summary copy feature, 267
Network Name Resolution feature, 61
Wireshark tasks
application analysis, 5
general analysis, 4
security analysis, 5
troubleshooting, 4
wiretap library, 8, 342
WLAN (Wireless Local Area Network)
adapters, 92
capture techniques, 92–93
definition of, 342
Zero Window Probe ACK notes, 235
Zero Window Probe notes, 235
Zero Window warnings, 234