



# **Wireshark® 101**

## **Essential Skills for Network Analysis**

2<sup>nd</sup> Edition

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





Protocol Analysis Institute, Inc  
59 Damonte Ranch Parkway, #B340  
Reno, NV 89521 USA  
[www.packet-level.com](http://www.packet-level.com)

Chappell University  
[info@chappellU.com](mailto:info@chappellU.com)  
[www.chappellU.com](http://www.chappellU.com)

# Table of Contents

<b>Acknowledgments</b> .....	<b>i</b>
<b>Dedication</b> .....	<b>ii</b>
<b>About this Book</b> .....	<b>iii</b>
Who Should Read this Book?.....	iii
What Prerequisite Knowledge do I Need?.....	iii
What Version of Wireshark does this Book Cover?.....	iii
Where Can I Get the Book Trace Files?.....	iv
Where Can I Learn More about Wireshark and Network Analysis? .....	iv
<b>Foreword by Gerald Combs</b> .....	<b>v</b>
<b>Chapter 0 Skills: Explore Key Wireshark Elements and Traffic Flows</b> .....	<b>1</b>
<b>Quick Reference: Key Wireshark Graphical Interface Elements</b> .....	<b>2</b>
<b>0.1. Understand Wireshark's Capabilities</b> .....	<b>3</b>
General Analysis Tasks.....	4
Troubleshooting Tasks .....	4
Security Analysis (Network Forensics) Tasks .....	5
Application Analysis Tasks.....	5
<b>0.2. Get the Right Wireshark Version</b> .....	<b>6</b>
<b>0.3. Learn how Wireshark Captures Traffic</b> .....	<b>7</b>
The Capture Process Relies on Special Link-Layer Drivers.....	7
The Dumpcap Capture Engine Defines Stop Conditions .....	8
The Core Engine is the Goldmine .....	8
The Qt Framework Provides the User Interface .....	8
The GTK+ Toolkit is Being Phased Out .....	9
The Wiretap Library is Used to Open Saved Trace Files .....	9
<b>0.4. Understand a Typical Wireshark Analysis Session</b> .....	<b>10</b>
<b>0.5. Differentiate a Packet from a Frame</b> .....	<b>11</b>
Recognize a Frame .....	11
Recognize a Packet.....	11
Recognize a Segment (and Watch for Ambiguities).....	11
<b>0.6. Follow an HTTP Packet through a Network</b> .....	<b>13</b>
Point 1: What Would You See at the Client?.....	14
Point 2: What Would You See on the Other Side of the First Switch? .....	14
Point 3: What Would You See on the Other Side of the Router? .....	15
Point 4: What Would You See on the Other Side of the Router/NAT Device?.....	15







Point 5: What Would You See at the Server? .....	16
Where You Capture Traffic Matters.....	16
Beware of Default Switch Forwarding .....	17
<b>0.7. Access Wireshark Resources .....</b>	<b>18</b>
Use the Wireshark Wiki Protocol Pages.....	18
Get Your Questions Answered at <i>ask.wireshark.org</i> .....	20
<b>0.8. Analyze Traffic Using the Main Wireshark View .....</b>	<b>22</b>
Open a Trace File (Using the Main Toolbar, Please).....	22
Launch a Capture with Sparklines.....	23
Know When You Must Use the Main Menu.....	23
Use the Main Toolbar Whenever Possible .....	24
Learn the Keyboard Shortcuts.....	24
Master the Filter Toolbar .....	27
Summarize the Traffic Using the Packet List Pane .....	27
Dig Deeper in the Packet Details Pane .....	35
Get Geeky in the Packet Bytes Pane .....	36
Pay Attention to the Status Bar .....	37
<input type="checkbox"/> Lab 1: Use Packets to Build a Picture of a Network.....	39
<b>0.9. Analyze Typical Network Traffic.....</b>	<b>45</b>
Analyze Web Browsing Traffic.....	45
Analyze Sample Background Traffic .....	47
<input type="checkbox"/> Lab 2: Capture and Classify Your Own Background Traffic.....	50
<b>0.10. Open Trace Files Captured with Other Tools.....</b>	<b>52</b>
<input type="checkbox"/> Lab 3: Open a Network Monitor .cap File.....	54
<b>Chapter 0 Challenge .....</b>	<b>56</b>
<b>Chapter 1 Skills: Customize Wireshark Views and Settings.....</b>	<b>57</b>
<b>Quick Reference: Overview of <a href="http://wireshark.org">wireshark.org</a> .....</b>	<b>58</b>
<b>1.1. Add Columns to the Packet List Pane .....</b>	<b>59</b>
Right-Click   Apply as Column (the “Easy Way”).....	59
Edit   Preferences   Columns (the “Hard Way”).....	60
Hide, Remove, Rearrange, Realign, and Edit Columns .....	61
Sort Column Contents .....	62
Export Column Data .....	62
<input type="checkbox"/> Lab 4: Add the HTTP Host Field as a Column .....	63

<b>1.2. Dissect the Wireshark Dissectors</b> .....	<b>65</b>
The Frame Dissector .....	65
The Ethernet Dissector Takes Over .....	66
The IPv4 Dissector Takes Over.....	66
The TCP Dissector Takes Over.....	67
The HTTP Dissector Takes Over .....	67
<b>1.3. Analyze Traffic that Uses Non-Standard Ports</b> .....	<b>69</b>
What Happens When Non-Standard Ports are Used .....	69
How Heuristic Dissectors Work .....	70
Manually Force a Dissector on the Traffic .....	70
Adjust Dissections with the Application Preference Settings (if possible) .....	71
<b>1.4. Change how Wireshark Displays Certain Traffic Types</b> .....	<b>72</b>
Define User Interface Settings.....	72
Adjust Capture Settings.....	72
Define Filter Expression Buttons .....	72
Set Name Resolution Settings.....	73
Set Protocol and Application Settings .....	74
 Lab 5: Set Key Wireshark Preferences (IMPORTANT LAB).....	76
<b>1.5. Customize Wireshark for Different Tasks (Profiles)</b> .....	<b>81</b>
The Basics of Profiles.....	81
Create a New Profile .....	81
 Lab 6: Create a New Profile Based on the <i>Default</i> Profile .....	82
<b>1.6. Locate Key Wireshark Configuration Files</b> .....	<b>83</b>
Your Global Configuration Directory.....	83
Your Personal Configuration (and <i>profiles</i> ) Directory .....	84
 Lab 7: Import a DNS/HTTP Errors Profile .....	85
<b>1.7. Configure Time Columns to Spot Latency Problems</b> .....	<b>87</b>
The Indications and Causes of Path Latency .....	87
The Indications and Causes of Client Latency .....	88
The Indications and Causes of Server Latency.....	89
Detect Latency Problems by Changing the Time Column Setting.....	89
Detect Latency Problems with a New TCP Delta Column.....	91
Don't Get Fooled – Some Delays are Normal .....	94
 Lab 8: Spot Path and Server Latency Problems .....	96
<b>Chapter 1 Challenge</b> .....	<b>99</b>

## Chapter 2 Skills: Determine the Best Capture Method and Apply Capture Filters. 101

<b>Quick Reference: Capture Options</b> .....	<b>102</b>
<b>2.1. Identify the Best Capture Location to Troubleshoot Slow Browsing or File Downloads</b> .....	<b>103</b>
The Ideal Starting Point.....	103
Move if Necessary .....	104
<b>2.2. Capture Traffic on Your Ethernet Network</b> .....	<b>105</b>
<b>2.3. Capture Traffic on Your Wireless Network</b> .....	<b>106</b>
What can Your Native WLAN Adapter See? .....	106
Use an AirPcap Adapter for Full WLAN Visibility.....	106
Use the Npcap Driver for WLAN/Loopback Visibility .....	106
<b>2.4. Identify Active Interfaces</b> .....	<b>108</b>
Determine Which Adapter Sees Traffic .....	108
Consider Using Multi-Adapter Capture.....	109
<b>2.5. Deal with TONS of Traffic</b> .....	<b>110</b>
Why are You Seeing So Much Traffic? .....	110
This is the Best Reason to Use Capture Filters.....	110
Capture to a File Set.....	110
Open and Move around in File Sets.....	111
Consider a Different Solution—SteelCentral™ Packet Analyzer.....	111
<input type="checkbox"/> Lab 9: Capture to File Sets .....	113
<b>2.6. Use Special Capture Techniques to Spot Sporadic Problems</b> .....	<b>116</b>
Use File Sets and the Ring Buffer .....	116
Stop When Complaints Arise.....	117
<input type="checkbox"/> Lab 10: Use a Ring Buffer to Conserve Drive Space .....	118
<b>2.7. Reduce the Amount of Traffic You have to Work With</b> .....	<b>120</b>
Detect When Wireshark Can't Keep Up .....	120
Detect when a Spanned Switch Can't Keep Up .....	121
Apply a Capture Filter in the Capture Options Window .....	122
<b>2.8. Capture Traffic based on Addresses (MAC/IP)</b> .....	<b>124</b>
Capture Traffic to or from a Specific IP Address .....	124
Capture Traffic to or from a Range of IP Addresses .....	125
Capture Traffic to Broadcast or Multicast Addresses .....	125
Capture Traffic based on a MAC Address.....	126
<input type="checkbox"/> Lab 11: Capture Only Traffic to or from Your IP Address .....	127
<input type="checkbox"/> Lab 12: Capture Only Traffic to or from Everyone Else's MAC Address.....	129

<b>2.9. Capture Traffic for a Specific Application .....</b>	<b>131</b>
It's all About the Port Numbers .....	131
Combine Port-based Capture Filters .....	132
<b>2.10. Capture Specific ICMP Traffic .....</b>	<b>133</b>
☐ Lab 13: Create, Save and Apply a DNS Capture Filter .....	134
<b>Chapter 2 Challenge .....</b>	<b>136</b>
<b>Chapter 3 Skills: Apply Display Filters to Focus on Specific Traffic.....</b>	<b>137</b>
<b>Quick Reference: Display Filter Area.....</b>	<b>138</b>
<b>3.1. Use Proper Display Filter Syntax .....</b>	<b>139</b>
The Syntax of the Simplest Display Filters .....	139
Use the Display Filter Error Detection Mechanism .....	141
Learn the Field Names .....	142
Use Auto-Complete to Build Display Filters.....	143
Display Filter Comparison Operators .....	145
Use Expressions to Build Display Filters .....	146
☐ Lab 14: Use Auto-Complete to Find Traffic to a Specific HTTP Server .....	147
<b>3.2. Edit and Use the Default Display Filters.....</b>	<b>151</b>
☐ Lab 15: Use a Default Filter as a “Seed” for a New Filter.....	153
<b>3.3. Filter Properly on HTTP Traffic.....</b>	<b>154</b>
Test an Application Filter Based on a TCP Port Number .....	154
Be Cautious Using a TCP-based Application Name Filter .....	155
☐ Lab 16: Filter on HTTP Traffic the Right Way .....	157
<b>3.4. Determine Why Your dnscap Display Filter Doesn't Work .....</b>	<b>159</b>
<b>3.5. Apply Display Filters based on an IP Address, Range of Addresses, or Subnet.....</b>	<b>160</b>
Filter on Traffic to or from a Single IP Address or Host .....	160
Filter on Traffic to or from a Range of Addresses.....	161
Filter on Traffic to or from an IP Subnet .....	161
☐ Lab 17: Filter on Traffic to or from Online Backup Subnets .....	162
<b>3.6. Quickly Filter on a Field in a Packet .....</b>	<b>163</b>
Work Quickly – Use Right-Click   Apply as Filter .....	163
Be Creative with Right-Click   Prepare a Filter .....	165
Right-Click Again to use the “...” Filter Enhancements .....	165
☐ Lab 18: Filter on DNS Name Errors or HTTP 404 Responses.....	168

<b>3.7. Filter on a Single TCP or UDP Conversation.....</b>	<b>169</b>
Use Right-Click to Filter on a Conversation.....	169
Use Right-Click to Follow a Stream.....	170
Filter on a Conversation from Wireshark Statistics.....	170
Filter on a TCP or UDP Conversation Based on the Stream Index Field .....	172
 Lab 19: Detect Background File Transfers on Startup .....	173
<b>3.8. Expand Display Filters with Multiple Include and Exclude Conditions .....</b>	<b>174</b>
Use Logical Operators.....	174
Why didn't my <code>ip.addr != filter</code> work?.....	174
Why didn't my <code>!tcp.flags.syn==1 filter</code> work?.....	175
<b>3.9. Use Parentheses to Change Filter Meaning.....</b>	<b>176</b>
 Lab 20: Locate TCP Connection Attempts to a Client.....	177
<b>3.10. Determine Why Your Display Filter Area is Yellow .....</b>	<b>179</b>
Red Background: Syntax Check Failed.....	179
Green Background: Syntax Check Passed .....	179
Yellow Background: Syntax Check Passed with a Warning (!=).....	179
<b>3.11. Filter on a Keyword in a Trace File .....</b>	<b>180</b>
Use <code>contains</code> in a Simple Keyword Filter through an Entire Frame .....	180
Use <code>contains</code> in a Simple Keyword Filter based on a Field.....	180
Use <code>matches</code> and <code>(?i)</code> in a Keyword Filter for Upper Case or Lower Case Strings .....	181
Use <code>matches</code> for a Multiple-Word Search .....	181
 Lab 21: Filter to Locate a Set of Key Words in a Trace File.....	182
<b>3.12. Use Wildcards in Your Display Filters .....</b>	<b>184</b>
Use Regex with <code>.</code> .....	184
Setting a Variable Length Repeating Wildcard Character Search.....	184
 Lab 22: Filter with Wildcards between Words .....	185
<b>3.13. Use Filters to Spot Communication Delays .....</b>	<b>186</b>
Filter on Large Delta Times ( <code>frame.time_delta</code> ).....	186
Filter on Large TCP Delta Times ( <code>tcp.time_delta</code> ).....	186
 Lab 23: Import Display Filters into a Profile.....	188
<b>3.14. Turn Your Key Display Filters into Buttons .....</b>	<b>190</b>
Create a Filter Expression Button.....	190
Edit, Reorder, Delete, and Disable Filter Expression Buttons .....	192
Edit the Filter Expression Area in Your <i>preferences</i> File.....	192
 Lab 24: Create and Import HTTP Filter Expression Buttons .....	194
<b>Chapter 3 Challenge .....</b>	<b>196</b>

<b>Chapter 4 Skills: Color and Export Interesting Packets .....</b>	<b>197</b>
<b>Quick Reference: Coloring Rules Interface.....</b>	<b>198</b>
<b>4.1. Identify Applied Coloring Rules .....</b>	<b>199</b>
<input type="checkbox"/> Lab 25: Add a Column to Display Coloring Rules in Use .....	200
<b>4.2. Turn Off the Checksum Error Coloring Rule.....</b>	<b>202</b>
Disable Individual Coloring Rules.....	202
Disable All Packet Coloring .....	202
<b>4.3. Build a Coloring Rule to Highlight Delays.....</b>	<b>204</b>
Create a Coloring Rule from Scratch.....	204
Use the Right-Click Method to Create a Coloring Rule .....	206
<input type="checkbox"/> Lab 26: Build a Coloring Rule to Highlight FTP User Names, Passwords, and More .....	207
<b>4.4. Quickly Colorize a Single Conversation.....</b>	<b>209</b>
Right-Click to Temporarily Colorize a Conversation.....	209
Remove Temporary Coloring .....	210
<input type="checkbox"/> Lab 27: Create Temporary Conversation Coloring Rules .....	211
<b>4.5. Master the Intelligent Scrollbar .....</b>	<b>212</b>
Navigate Manually on the Intelligent Scrollbar .....	213
Navigate with the Intelligent Scrollbar Menu .....	213
<input type="checkbox"/> Lab 28: Use the Intelligent Scrollbar to Quickly Find Problems .....	214
<b>4.6. Export Packets that Interest You .....</b>	<b>216</b>
<input type="checkbox"/> Lab 29: Export a Single TCP Conversation .....	218
<b>4.7. Export Packet Details .....</b>	<b>220</b>
Export Packet Dissections.....	220
Define What should be Exported.....	221
Sample Text Output.....	221
Sample CSV Output.....	222
<input type="checkbox"/> Lab 30: Export a List of HTTP Host Field Values from a Trace File.....	223
<b>Chapter 4 Challenge .....</b>	<b>226</b>
<b>Chapter 5 Skills: Build and Interpret Tables and Graphs.....</b>	<b>227</b>
<b>Quick Reference: IO Graph Interface .....</b>	<b>228</b>
<b>5.1. Find Out Who's Talking to Whom on the Network .....</b>	<b>229</b>
Check Out Network Conversations .....	229
Quickly Filter on Conversations.....	230



<b>5.2. Locate the Top Talkers.....</b>	<b>232</b>
Sort to Find the Most Active Conversation .....	232
Sort to Find the Most Active Host.....	233
<input type="checkbox"/> Lab 31: Filter on the Most Active TCP Conversation .....	234
<input type="checkbox"/> Lab 32: Set up GeoIP to Map Targets Globally .....	237
<b>5.3. List Applications Seen on the Network .....</b>	<b>239</b>
View the Protocol Hierarchy .....	239
Right-Click to Filter or Colorize any Listed Protocol or Application .....	239
Look for Suspicious Protocols, Applications or “Data”.....	240
<input type="checkbox"/> Lab 33: Detect Suspicious Protocols or Applications.....	241
<b>5.4. Graph Application and Host Bandwidth Usage .....</b>	<b>242</b>
Export the Application or Host Traffic before Graphing .....	242
Apply <code>ip.addr</code> Display Filters to the IO Graph.....	243
Apply <code>ip.src</code> Display Filters to the IO Graph .....	245
Apply <code>tcp.port</code> or <code>udp.port</code> Display Filters to the IO Graph .....	246
<input type="checkbox"/> Lab 34: Compare Traffic to/from a Subnet to Other Traffic.....	247
<b>5.5. Identify TCP Errors on the Network.....</b>	<b>249</b>
Use the Expert Information Button on the Status Bar.....	249
Examine Expert Severity Levels.....	250
Filter on TCP Analysis Flag Packets .....	252
<b>5.6. Understand what those Expert Information Errors Mean .....</b>	<b>253</b>
Packet Loss, Recovery, and Faulty Trace Files .....	253
Asymmetrical or Multiple Path Indications.....	254
Keep-Alive Indication.....	254
Receive Buffer Congestion Indications.....	254
TCP Connection Port Reuse Indication.....	255
Possible Router Problem Indication .....	256
Misconfiguration or ARP Poisoning Indication.....	256
<input type="checkbox"/> Lab 35: Identify an Overloaded Client.....	257
<b>5.7. Graph Various Network Errors .....</b>	<b>259</b>
Graph all TCP Analysis Flag Packets (Except Window Updates).....	259
Graph Separate Types of TCP Analysis Flag Packets.....	260
<input type="checkbox"/> Lab 36: Detect and Graph File Transfer Problems .....	261
<b>Chapter 5 Challenge .....</b>	<b>264</b>

<b>Chapter 6 Skills: Reassemble Traffic for Faster Analysis</b> .....	<b>265</b>
<b>Quick Reference: File and Object Reassembly Options</b> .....	<b>266</b>
<b>6.1. Reassemble Web Browsing Sessions</b> .....	<b>267</b>
Use Follow   TCP Stream.....	267
Use Find, Save, and Filter on a Stream.....	268
<input type="checkbox"/> Lab 37: Use Reassembly to Find a Web Site's Hidden HTTP Message.....	269
<b>6.2. Reassemble a File Transferred via FTP</b> .....	<b>271</b>
<input type="checkbox"/> Lab 38: Extract a File from an FTP File Transfer.....	273
<b>6.3. Export HTTP Objects Transferred in a Web Browsing Session</b> .....	<b>276</b>
Check Your TCP Preference Settings First!.....	276
View all HTTP Objects in the Trace File.....	276
<input type="checkbox"/> Lab 39: Carve Out an HTTP Object from a Web Browsing Session.....	278
<b>Chapter 6 Challenge</b> .....	<b>281</b>
<b>Chapter 7 Skills: Add Comments to Your Trace Files and Packets</b> .....	<b>283</b>
<b>Quick Reference: File and Packet Annotation Options</b> .....	<b>284</b>
<b>7.1. Add Your Comments to Trace Files</b> .....	<b>285</b>
<b>7.2. Add Your Comments to Individual Packets</b> .....	<b>287</b>
Use the .pcapng Format for Annotations.....	288
Add a Comment Column for Faster Viewing.....	289
<input type="checkbox"/> Lab 40: Read Analysis Notes in a Malicious Redirection Trace File.....	290
<b>7.3. Export Packet Comments for a Report</b> .....	<b>291</b>
First, Filter on Packets that Contain Comments.....	291
Next, Export Packet Dissections as Plain Text.....	292
<input type="checkbox"/> Lab 41: Export Malicious Redirection Packet Comments.....	294
<b>Chapter 7 Challenge</b> .....	<b>296</b>
<b>Chapter 8 Skills: Use Command-Line Tools to Capture, Split, and Merge Traffic</b> .	<b>297</b>
<b>Quick Reference: Command-Line Tools Key Options</b> .....	<b>298</b>
<b>8.1. Split a Large Trace File into a File Set</b> .....	<b>299</b>
Add the Wireshark Program Directory to Your Path.....	299
Use Capinfos to Get the File Size and Packet Count.....	300
Split a File Based on Packets per Trace File.....	301
Split a File Based on Seconds per Trace File.....	301
Open and Work with File Sets in Wireshark.....	302
<input type="checkbox"/> Lab 42: Split a File and Work with Filtered File Sets.....	303

<b>8.2. Merge Multiple Trace Files .....</b>	<b>306</b>
Ensure the Wireshark Program Directory is in Your Path .....	306
Run Mergecap with the <code>-w</code> Parameter .....	306
<input type="checkbox"/> Lab 43: Merge a Set of Files using a Wildcard .....	308
<b>8.3. Capture Traffic at Command Line .....</b>	<b>310</b>
Dumpcap or Tshark? .....	310
Capture at the Command Line with Dumpcap.....	310
Capture at the Command Line with Tshark .....	311
Save Host Information and Work with Existing Trace Files.....	312
<input type="checkbox"/> Lab 44: Use Tshark to Capture to File Sets with an Autostop Condition .....	313
<b>8.4. Use Capture Filters during Command-Line Capture .....</b>	<b>316</b>
<b>8.5. Use Display Filters during Command-Line Capture.....</b>	<b>318</b>
<input type="checkbox"/> Lab 45: Use Tshark to Extract HTTP GET Requests.....	320
<b>8.6. Use Tshark to Export Specific Field Values and Statistics from a Trace File.....</b>	<b>321</b>
Export Field Values .....	321
Export Traffic Statistics.....	322
Export HTTP Host Field Values.....	324
<input type="checkbox"/> Lab 46: Use Tshark to Extract HTTP Host Names and IP Addresses .....	325
<b>8.7. Continue Learning about Wireshark and Network Analysis.....</b>	<b>326</b>
<b>Chapter 8 Challenge .....</b>	<b>327</b>
<b>Appendix A: Challenge Answers.....</b>	<b>329</b>
Chapter 0 Challenge Answers.....	330
Chapter 1 Challenge Answers.....	334
Chapter 2 Challenge Answers.....	337
Chapter 3 Challenge Answers.....	341
Chapter 4 Challenge Answers.....	344
Chapter 5 Challenge Answers.....	348
Chapter 6 Challenge Answers.....	352
Chapter 7 Challenge Answers.....	355
Chapter 8 Challenge Answers.....	357
<b>Appendix B: Trace File Descriptions .....</b>	<b>359</b>
<b>Network Analyst's Glossary .....</b>	<b>367</b>
<b>Index .....</b>	<b>381</b>