



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

Table of Contents

Acknowledgments	i
Dedication	ii
About this Book	iii
Who is this Book For?	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
Foreword by Gerald Combs	v
Chapter 0 Skills: Explore Key Wireshark Elements and Traffic Flows	1
Quick Reference: Key Wireshark Graphical Interface Elements	2
0.1. Understand Wireshark's Capabilities	3
General Analysis Tasks.....	4
Troubleshooting Tasks	4
Security Analysis (Network Forensics) Tasks	5
Application Analysis Tasks	5
0.2. Get the Right Wireshark Version	6
0.3. Learn how Wireshark Captures Traffic	7
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 Graphical Toolkit Provides the User Interface.....	8
The Wiretap Library is Used to Open Saved Trace Files	8
0.4. Understand a Typical Wireshark Analysis Session	9
0.5. Differentiate a Packet from a Frame	10
Recognize a Frame	10
Recognize a Packet.....	10
Recognize a Segment	10
0.6. Follow an HTTP Packet through a Network	12
Point 1: What Would You See at the Client?.....	13
Point 2: What Would You See on the Other Side of the First Switch?	13
Point 3: What Would You See on the Other Side of the Router?	14
Point 4: What Would You See on the Other Side of the Router/NAT Device?	14
Point 5: What Would You See at the Server?	15







Where You Capture Traffic Matters.....	15
Beware of Default Switch Forwarding	16
0.7. Access Wireshark Resources	17
Use the Wireshark Wiki Protocol Pages.....	17
Get Your Questions Answered at <i>ask.wireshark.org</i>	18
0.8. Analyze Traffic Using the Main Wireshark View	20
Open a Trace File (Using the Main Toolbar, Please)	20
Know When You Must Use the Main Menu.....	21
Learn to Use the Main Toolbar Whenever Possible	22
Master the Filter Toolbar	22
Summarize the Traffic Using the Packet List Pane	23
Dig Deeper in the Packet Details Pane	28
Get Geeky in the Packet Bytes Pane	29
Pay Attention to the Status Bar	30
<input type="checkbox"/> Lab 1: Use Packets to Build a Picture of a Network.....	32
0.9. Analyze Typical Network Traffic.....	38
Analyze Web Browsing Traffic.....	38
Analyze Sample Background Traffic	40
<input type="checkbox"/> Lab 2: Capture and Classify Your Own Background Traffic.....	43
0.10. Open Trace Files Captured with Other Tools.....	44
<input type="checkbox"/> Lab 3: Open a Network Monitor .cap File.....	45
Chapter 0 Challenge	46
Chapter 1 Skills: Customize Wireshark Views and Settings.....	47
Quick Reference: Overview of wireshark.org	48
1.1. Add Columns to the Packet List Pane	49
Right-Click Apply as Column (the “easy way”)	49
Edit Preferences Columns (the “hard way”)	50
Hide, Remove, Rearrange, Realign, and Edit Columns	50
Sort Column Contents	51
Export Column Data	52
<input type="checkbox"/> Lab 4: Add the HTTP Host Field as a Column	53

1.2. Dissect the Wireshark Dissectors	54
The Frame Dissector	54
The Ethernet Dissector Takes Over	55
The IPv4 Dissector Takes Over.....	55
The TCP Dissector Takes Over.....	56
The HTTP Dissector Takes Over	56
1.3. Analyze Traffic that Uses Non-Standard Port Numbers	57
When the Port Number is Assigned to Another Application	57
Manually Force a Dissector on the Traffic	57
When the Port Number is not Recognized	58
How Heuristic Dissectors Work	58
Adjust Dissections with the Application Preference Settings (if possible)	59
 Lab 5: Configure Wireshark to Dissect Port 81 Traffic as HTTP	60
1.4. Change how Wireshark Displays Certain Traffic Types	61
Set User Interface Settings.....	61
Set Name Resolution Settings.....	61
Define Filter Expression Buttons	61
Set Protocol and Application Settings	62
 Lab 6: Set Key Wireshark Preferences (IMPORTANT LAB).....	63
1.5. Customize Wireshark for Different Tasks (Profiles)	67
The Basics of Profiles	67
Create a New Profile	67
 Lab 7: Create a New Profile Based on the <i>Default</i> Profile	68
1.6. Locate Key Wireshark Configuration Files	69
Your Global Configuration Directory.....	69
Your Personal Configuration (and <i>profiles</i>) Directory	70
 Lab 8: Import a DNS/HTTP Errors Profile	71
1.7. Configure Time Columns to Spot Latency Problems	73
The Indications and Causes of Path Latency	73
The Indications and Causes of Client Latency	74
The Indications and Causes of Server Latency.....	75
Detect Latency Problems by Changing the Time Column Setting.....	75
Detect Latency Problems with a New TCP Delta Column.....	77
Don't Get Fooled – Some Delays are Normal	80
 Lab 9: Spot Path and Server Latency Problems	82
Chapter 1 Challenge	85





Chapter 2 Skills: Determine the Best Capture Method and Apply Capture Filters... 87

Quick Reference: Capture Options	88
2.1. Identify the Best Capture Location to Troubleshoot Slow Browsing or File Downloads	89
The Ideal Starting Point.....	89
Move if Necessary	90
2.2. Capture Traffic on Your Ethernet Network	91
2.3. Capture Traffic on Your Wireless Network	92
What can Your Native WLAN Adapter See?	92
Use an AirPcap Adapter for Full WLAN Visibility.....	92
2.4. Identify Active Interfaces	94
Determine Which Adapter Sees Traffic	94
Consider Using Multi-Adapter Capture.....	95
2.5. Deal with TONS of Traffic	96
Why are You Seeing So Much Traffic?	96
This is the Best Reason to Use Capture Filters.....	96
Capture to a File Set.....	96
Open and Move around in File Sets	97
Consider a Different Solution—Cascade Pilot®	98
<input type="checkbox"/> Lab 10: Capture to File Sets	99
2.6. Use Special Capture Techniques to Spot Sporadic Problems	101
Use File Sets and the Ring Buffer	101
Stop When Complaints Arise.....	102
<input type="checkbox"/> Lab 11: Use a Ring Buffer to Conserve Drive Space	103
2.7. Reduce the Amount of Traffic You have to Work With	105
Detect When Wireshark Can't Keep Up	105
Detect when a Spanned Switch Can't Keep Up	106
Apply a Capture Filter in the Capture Options Window	107
2.8. Capture Traffic based on Addresses (MAC/IP)	108
Capture Traffic to or from a Specific IP Address	108
Capture Traffic to or from a Range of IP Addresses	109
Capture Traffic to Broadcast or Multicast Addresses	109
Capture Traffic based on a MAC Address.....	110
<input type="checkbox"/> Lab 12: Capture Only Traffic to or from Your IP Address	111
<input type="checkbox"/> Lab 13: Capture Only Traffic to or from Everyone Else's MAC Address.....	113

2.9. Capture Traffic for a Specific Application	116
It's all About the Port Numbers	116
Combine Port-based Capture Filters	117
2.10. Capture Specific ICMP Traffic	118
☐ Lab 14: Create, Save and Apply a DNS Capture Filter	119
Chapter 2 Challenge	121
Chapter 3 Skills: Apply Display Filters to Focus on Specific Traffic.....	123
Quick Reference: Display Filter Area.....	124
3.1. Use Proper Display Filter Syntax	125
The Syntax of the Simplest Display Filters	125
Use the Display Filter Error Detection Mechanism	127
Learn the Field Names	128
Use Auto-Complete to Build Display Filters.....	130
Display Filter Comparison Operators	131
Use Expressions to Build Display Filters	132
☐ Lab 15: Use Auto-Complete to Find Traffic to a Specific HTTP Server	133
3.2. Edit and Use the Default Display Filters.....	137
☐ Lab 16: Use a Default Filter as a “Seed” for a New Filter.....	139
3.3. Filter Properly on HTTP Traffic.....	140
Test an Application Filter Based on a TCP Port Number	140
Be Cautious Using a TCP-based Application Name Filter	141
☐ Lab 17: Filter on HTTP Traffic the Right Way	143
3.4. Determine Why Your dhcp Display Filter Doesn't Work	145
3.5. Apply Display Filters based on an IP Address, Range of Addresses, or Subnet.....	146
Filter on Traffic to or from a Single IP Address or Host	146
Filter on Traffic to or from a Range of Addresses.....	147
Filter on Traffic to or from an IP Subnet	147
☐ Lab 18: Filter on Traffic to or from Online Backup Subnets	148
3.6. Quickly Filter on a Field in a Packet	149
Work Quickly – Use Right-Click Apply as Filter	149
Be Creative with Right-Click Prepare a Filter	151
Right-Click Again to use the “...” Filter Enhancements	152
☐ Lab 19: Filter on DNS Name Errors or HTTP 404 Responses.....	155

3.7. Filter on a Single TCP or UDP Conversation.....	156
Use Right-Click to Filter on a Conversation.....	156
Use Right-Click to Follow a Stream.....	157
Filter on a Conversation from Wireshark Statistics.....	158
Filter on a TCP Conversation Based on the Stream Index Field.....	159
 Lab 20: Detect Background File Transfers on Startup.....	160
3.8. Expand Display Filters with Multiple Include and Exclude Conditions.....	161
Use Logical Operators.....	161
Why didn't my <code>ip.addr != filter</code> work?.....	161
Why didn't my <code>!tcp.flags.syn==1</code> filter work?.....	162
3.9. Use Parentheses to Change Filter Meaning.....	163
 Lab 21: Locate TCP Connection Attempts to a Client.....	164
3.10. Determine Why Your Display Filter Area is Yellow.....	166
Red Background: Syntax Check Failed.....	166
Green Background: Syntax Check Passed.....	166
Yellow Background: Syntax Check Passed with a Warning (!=).....	166
3.11. Filter on a Keyword in a Trace File.....	167
Use <code>contains</code> in a Simple Keyword Filter through an Entire Frame.....	167
Use <code>contains</code> in a Simple Keyword Filter based on a Field.....	167
Use <code>matches</code> and <code>(?i)</code> in a Keyword Filter for Upper Case or Lower Case Strings.....	168
Use <code>matches</code> for a Multiple-Word Search.....	168
 Lab 22: Filter to Locate a Set of Key Words in a Trace File.....	169
3.12. Use Wildcards in Your Display Filters.....	170
Use Regex with <code>.</code>	170
Setting a Variable Length Repeating Wildcard Character Search.....	170
 Lab 23: Filter with Wildcards between Words.....	171
3.13. Use Filters to Spot Communication Delays.....	172
Filter on Large Delta Times (<code>frame.time_delta</code>).....	172
Filter on Large TCP Delta Times (<code>tcp.time_delta</code>).....	172
 Lab 24: Import Display Filters into a Profile.....	174
3.14. Turn Your Key Display Filters into Buttons.....	176
Create a Filter Expression Button.....	176
Edit, Reorder, Delete, and Disable Filter Expression Buttons.....	177
Edit the Filter Expression Area in Your <i>preferences</i> File.....	177
 Lab 25: Create and Import HTTP Filter Expression Buttons.....	179
Chapter 3 Challenge.....	181

Chapter 4 Skills: Color and Export Interesting Packets	183
Quick Reference: Coloring Rules Interface.....	184
4.1. Identify Applied Coloring Rules	185
<input type="checkbox"/> Lab 26: Add a Column to Display Coloring Rules in Use	186
4.2. Turn Off the Checksum Error Coloring Rule.....	188
Disable Individual Coloring Rules.....	188
Disable All Packet Coloring	189
4.3. Build a Coloring Rule to Highlight Delays.....	190
Create a Coloring Rule from Scratch.....	190
Use the Right-Click Method to Create a Coloring Rule	192
<input type="checkbox"/> Lab 27: Build a Coloring Rule to Highlight FTP User Names, Passwords, and More	193
4.4. Quickly Colorize a Single Conversation.....	195
Right-Click to Temporarily Colorize a Conversation.....	195
Remove Temporary Coloring	196
<input type="checkbox"/> Lab 28: Create Temporary Conversation Coloring Rules	197
4.5. Export Packets that Interest You	198
<input type="checkbox"/> Lab 29: Export a Single TCP Conversation	200
4.6. Export Packet Details	202
Export Packet Dissections.....	202
Define What should be Exported.....	203
Sample Text Output.....	203
Sample CSV Output	204
<input type="checkbox"/> Lab 30: Export a List of HTTP Host Field Values from a Trace File.....	205
Chapter 4 Challenge	208
Chapter 5 Skills: Build and Interpret Tables and Graphs.....	209
Quick Reference: IO Graph Interface	210
5.1. Find Out Who's Talking to Whom on the Network	211
Check Out Network Conversations	211
Quickly Filter on Conversations.....	213
5.2. Locate the Top Talkers.....	214
Sort to Find the Most Active Conversation	214
Sort to Find the Most Active Host.....	215
<input type="checkbox"/> Lab 31: Filter on the Most Active TCP Conversation	216
<input type="checkbox"/> Lab 32: Set up GeoIP to Map Targets Globally	218

5.3. List Applications Seen on the Network	220
View the Protocol Hierarchy	220
Right-Click Filter or Colorize any Listed Protocol or Application	220
Look for Suspicious Protocols, Applications or “Data”	221
Decipher the Protocol Hierarchy Percentages	222
 Lab 33: Detect Suspicious Protocols or Applications	225
5.4. Graph Application and Host Bandwidth Usage	226
Export the Application or Host Traffic before Graphing	226
Apply <code>ip.addr</code> Display Filters to the IO Graph	227
Apply <code>ip.src</code> Display Filters to the IO Graph	228
Apply <code>tcp.port</code> or <code>udp.port</code> Display Filters to the IO Graph	229
 Lab 34: Compare Traffic to/from a Subnet to Other Traffic	230
5.5. Identify TCP Errors on the Network	231
Use the Expert Infos Button on the Status Bar	231
Deal with “Unreassembled” Indications in the Expert	231
Filter on TCP Analysis Flag Packets	232
5.6. Understand what those Expert Infos Errors Mean	233
Packet Loss, Recovery, and Faulty Trace Files	233
Asynchronous or Multiple Path Indications	234
Keep-Alive Indication	234
Receive Buffer Congestion Indications	234
TCP Connection Port Reuse Indication	235
Possible Router Problem Indication	235
Misconfiguration or ARP Poisoning Indication	236
 Lab 35: Identify an Overloaded Client	237
5.7. Graph Various Network Errors	238
Graph all TCP Analysis Flag Packets (Except Window Updates)	238
Graph Separate Types of TCP Analysis Flag Packets	239
 Lab 36: Detect and Graph File Transfer Problems	240
Chapter 5 Challenge	243

Chapter 6 Skills: Reassemble Traffic for Faster Analysis	245
Quick Reference: File and Object Reassembly Options	246
6.1. Reassemble Web Browsing Sessions	247
Use Follow TCP Stream.....	247
Use Find, Save, and Filter on a Stream.....	248
<input type="checkbox"/> Lab 37: Use Reassembly to Find a Web Site's Hidden HTTP Message.....	249
6.2. Reassemble a File Transferred via FTP	251
<input type="checkbox"/> Lab 38: Extract a File from an FTP File Transfer.....	253
6.3. Export HTTP Objects Transferred in a Web Browsing Session	256
Check Your TCP Preference Settings First!.....	256
View all HTTP Objects in the Trace File.....	256
<input type="checkbox"/> Lab 39: Carve Out an HTTP Object from a Web Browsing Session.....	258
Chapter 6 Challenge	260
Chapter 7 Skills: Add Comments to Your Trace Files and Packets	261
Quick Reference: File and Packet Annotation Options	262
7.1. Add Your Comments to Trace Files	263
7.2. Add Your Comments to Individual Packets	264
Use the .pcapng Format for Annotations.....	265
Add a Comment Column for Faster Viewing.....	265
<input type="checkbox"/> Lab 40: Read Analysis Notes in a Malicious Redirection Trace File.....	266
7.3. Export Packet Comments for a Report	267
First, Filter on Packets that Contain Comments.....	267
Next, Export Packet Dissections as Plain Text.....	268
<input type="checkbox"/> Lab 41: Export Malicious Redirection Packet Comments.....	270
Chapter 7 Challenge	272
Chapter 8 Skills: Use Command-Line Tools to Capture, Split, and Merge Traffic .	273
Quick Reference: Command-Line Tools Key Options	274
8.1. Split a Large Trace File into a File Set	275
Add the Wireshark Program Directory to Your Path.....	275
Use Capinfos to Get the File Size and Packet Count.....	275
Split a File Based on Packets per Trace File.....	276
Split a File Based on Seconds per Trace File.....	277
Open and Work with File Sets in Wireshark.....	278
<input type="checkbox"/> Lab 42: Split a File and Work with Filtered File Sets.....	279

8.2. Merge Multiple Trace Files	282
Ensure the Wireshark Program Directory is in Your Path	282
Run Mergecap with the <code>-w</code> Parameter	282
<input type="checkbox"/> Lab 43: Merge a Set of Files using a Wildcard	283
8.3. Capture Traffic at Command Line	284
Dumpcap or Tshark?	284
Capture at the Command Line with Dumpcap.....	284
Capture at the Command Line with Tshark	285
Save Host Information and Work with Existing Trace Files.....	285
<input type="checkbox"/> Lab 44: Use Tshark to Capture to File Sets with an Autostop Condition	286
8.4. Use Capture Filters during Command-Line Capture	289
8.5. Use Display Filters during Command-Line Capture.....	290
<input type="checkbox"/> Lab 45: Use Tshark to Extract HTTP GET Requests.....	291
8.6. Use Tshark to Export Specific Field Values and Statistics from a Trace File.....	292
Export Field Values	292
Export Traffic Statistics.....	293
Export HTTP Host Field Values.....	295
<input type="checkbox"/> Lab 46: Use Tshark to Extract HTTP Host Names and IP Addresses	296
8.7. Continue Learning about Wireshark and Network Analysis.....	297
Chapter 8 Challenge	298
Appendix A: Challenge Answers.....	299
Chapter 0 Challenge Answers.....	300
Chapter 1 Challenge Answers.....	303
Chapter 2 Challenge Answers.....	306
Chapter 3 Challenge Answers.....	308
Chapter 4 Challenge Answers.....	311
Chapter 5 Challenge Answers.....	314
Chapter 6 Challenge Answers.....	317
Chapter 7 Challenge Answers.....	319
Chapter 8 Challenge Answers.....	321
Appendix B: Trace File Descriptions	323
Network Analyst's Glossary	329
Index	343