

Table of Contents

Who is this Book For?	vi
What Prerequisite Knowledge do I Need?	vi
What Versions of Wireshark does this Book Cover?	vi
Does this Book Explain How to Troubleshoot My Network Applications?	vi
Where Can I Get the Book Trace Files and Other Supplements?	vii
Where Can I Learn More about Wireshark and Network Analysis?	vii
List of Labs	xxi
List of Network Problems and Symptoms	1
1. TCP Connection Refused by Server	3
2. Application Request Refused	3
3. Connection Blocked by a Host-Based or Network Firewall	4
4. Slow Application at Server	4
5. Slow Load of Remote Content	5
6. Server Application Fault	5
7. Content Redirection	5
8. TCP Receive Buffer Full	6
9. Send Buffer Full	6
10. Altered TCP Connection Attributes Along a Path	7
11. Mismatched TCP Parameters across a Proxy Device	8
12. Routing Loops	9
13. Weak Signal (WLAN)	9
14. Asymmetric Routing	9
15. Packet Loss	10
16. High Path Latency	10
17. Lousy Routing Path	11
18. Bandwidth Throttling	11
19. Delayed ACKs	12
20. Queued Packets (Overloaded Router)	12
21. Route Redirections	13
22. Broadcast or Multicast Storms	13
23. Switch Loop	13
24. Virus/Malware on Network Hosts	14
25. Network Name Resolution Problems	14
26. Network Address Resolution Problems	15
27. Hardware Address Resolution Problems	15
28. No Support for Selective Acknowledgment (SACK)	16
29. No Support for Window Scaling	16
30. Client Misconfiguration	17
31. Low Packet Size/Low MTU Size	17
32. TCP Port Number Reuse	17
33. Slow Application	18

Part 1: Preparing for Problems 19

Chapter 1: Use Efficient Troubleshooting Methods 21

- A Sample Four-Part Analysis Methodology 23
 - Task 1: Define the Problem 23
 - Task 2: Collect System, Application and Path Information 24
 - Task 3: Capture and Analyze Packet Flows 24
 - Task 4: Consider Other Tools 26
- Use a Troubleshooting Checklist 27
 - Verify Trace File Integrity and Basic Communications 27
 - Focus on Complaining User's Traffic 27
 - Detect and Prioritize Delays 27
 - Look for Throughput Issues 28
 - Check Miscellaneous Traffic Characteristics 28
 - TCP-Based Application: Determine TCP Connection Issues/Capabilities 29
 - TCP-Based Application: Identify TCP Issues 29
 - UDP-Based Application: Identify Communication Issues 29
 - Spot Application Errors 29

Chapter 2: Master these Key Wireshark Troubleshooting Tasks 31

- Create a Troubleshooting Profile 33
 - Wireshark Lab 1: Create Your Troubleshooting Profile 33
- Enhance the Packet List Pane Columns 35
 - Wireshark Lab 2: Add and Use a Custom Column to Locate HTTP Delays 36
- Change the Time Column Setting 39
 - Wireshark Lab 3: Set the Time Column to Detect Path Latency 39
- Filter on a Host, Subnet or Conversation 42
 - Wireshark Lab 4: Extract and Save a Single Conversation 42
- Filter on an Application Based on Port Number 45
 - Wireshark Lab 5: Filter Traffic Based on a Port Number 45
- Filter on Field Existence or a Field Value 47
 - Wireshark Lab 6: Filter on the HTTP Request Method Field To View Client Requests 47
 - Wireshark Lab 7: Filter on the Calculated Window Size Field to Locate Buffer Problems 48
- Filter OUT "Normal" Traffic (Exclusion Filters) 51
 - When to Use ! and == and When to Use != 51
 - Wireshark Lab 8: Filter Out Applications and Protocols 51
- Create Filter Expression Buttons 53
 - Wireshark Lab 9: Create a Button to Detect Missing TCP Functionality 53
- Launch and Navigate Through the Expert Infos 56
 - Wireshark Lab 10: Use Expert Infos to Identify Network Problems 56
- Change Dissector Behavior (Preference Settings) 59
 - Wireshark Lab 11: Change the TCP Dissector Reassembly Setting to Properly Measure HTTP Response Times 59

COLOR IN EBOOK VERSION ONLY

Find the Top Talkers	65
Wireshark Lab 12: Find the Most Active Conversation (Byte Count)	65
Build a Basic IO Graph	67
Wireshark Lab 13: Quickly Spot a Throughput Problem in an IO Graph	67
Add a Coloring Rule	69
Wireshark Lab 14: Build a Coloring Rule to Highlight DNS Errors	69
Chapter 3: Use the Right Capture Technique	75
Tips on Choosing a Capture Location	77
Capture Options for a Switched Network	78
Install Wireshark (or Other Capture Tool) on the User's Machine	78
Switch Port Spanning	79
Use a Test Access Port ("Tap")	79
The Final Choice – a Hub	80
Capture on High Traffic Rate Links	81
Consider Your Wireless Capture Options	82
Determine Your Native Adapter Capabilities	82
Wireshark Lab 15: Test Your WLAN Native Adapter Capture Capabilities	82
Consider the AirPcap Adapter	83
Capture to a File Set in High Traffic Rate Situations	85
Wireshark Lab 16: Capture and Work with File Sets	85
Use Capture Filters when Necessary	88
Wireshark Lab 17: Create and Apply a MAC Address Filter	88
Part 2: Symptom-Based Troubleshooting	91
Chapter 4: Resolution Problems	93
Silence is NOT Golden: Verify the Target Host Traffic	95
Check Your Capture Process	95
Consider the TCP/IP Resolution Flow Chart	96
Port Resolution	97
Name Resolution	97
Location Resolution - Local or Remote	97
MAC Address Resolution - Local Target	97
Route Resolution	97
MAC Address Resolution - Remote Target	97
Resolution Problems Can Cause a Silent Client	98
Name Resolution Problems	98
Route Resolution Problems	98
MAC Address Resolution Problems	99
Wireshark Lab 18: Identify a Name Resolution Problem	99
Wireshark Lab 19: Find Local Address Resolution Problems	100

Analyze a Lack of Server Responses.....	101
Wireshark Lab 20: No Response to TCP Connection Request	101
Wireshark Lab 21: No Response to Service Request.....	103
Chapter 5: Troubleshoot with Time	105
Do not Focus on “Normal” or Acceptable Delays	107
Delays before DNS Queries	107
Delays before TCP FIN or Reset Packets	108
Delays before a Client Sends a Request to a Server	108
Delays before Keep-Alive or Zero Window Probes	108
Delays before TLS Encrypted Alert Followed by a TCP FIN or RST.....	108
Delays before a Periodic Set of Packets in a Connection that is Otherwise Idle.....	108
Watch for the Delays that DO Matter.....	109
Delays before a Server Responds with a SYN/ACK	109
Delays before a Client Completes the 3-Way TCP Handshake	109
Delays before a Server Sends a Response	109
Delays before the Next Packet in a Data Stream.....	110
Delays before an ACK from a TCP peer	110
Delays before a Window Update	110
Detect Delays in UDP Conversations.....	112
Display Filter Value	112
UDP Delay Detection Methods.....	112
Wireshark Lab 22: Obtain UDP Conversation Statistics and Filter on a UDP Conversation.....	112
Wireshark Lab 23: Add/Sort a Delta Time Column	114
Wireshark Lab 24: Add/Sort a Delta Displayed Time Column	116
Wireshark Lab 25: Graph UDP Delays	117
Detect Delays in TCP Conversations	119
Display Filter Value	119
TCP Preference: <i>Calculate Conversation Timestamps</i>	119
Wireshark Lab 26: Obtain TCP Conversation Statistics.....	120
Wireshark Lab 27: Filter on a TCP Conversation Using the Stream Index Field	122
Wireshark Lab 28: Add a TCP Stream Index Column.....	123
Wireshark Lab 29: Add/Sort a TCP Delta Time Column	123
Wireshark Lab 30: Add a “TCP Delay” Button	125
Wireshark Lab 31: Obtain the Round Trip Time (RTT) Using the TCP Handshake.....	128
Filter for SYN and SYN/ACK Packets (Packet 1 and 2 of the TCP Handshake).....	129
Filter for SYN/ACK and ACK Packets (Packet 2 and 3 of the TCP Handshake).....	130
Filter for SYN and ACK Packets (Packet 1 and 3 of the TCP Handshake).....	130
Wireshark Lab 32: Obtain RTT using Display Filters	131
Wireshark Lab 33: Graph TCP Delays.....	132

Identify High DNS Response Time	135
Display Filter Value	135
Wireshark Lab 34: Add/Sort a <code>dns.time</code> Column to Find DNS Response Times	135
Wireshark Lab 35: Create a Button to Detect High DNS Response Times	137
Wireshark Lab 36: Graph DNS Response Times	138
Identify High HTTP Response Time	139
Display Filter Value	139
Wireshark Lab 37: Disable the <i>Allow Subdissector to Reassemble TCP Streams</i> Preference Setting	140
Wireshark Lab 38: Add/Sort an HTTP Response Time Column to Find HTTP Response Times ..	141
Wireshark Lab 39: Create a Button to Detect High HTTP Response Times	143
Wireshark Lab 40: Graph HTTP Response Times	144
Identify High SMB Response Time	145
Display Filter Value	145
Wireshark Lab 41: Add/Sort an SMB Response Time Column	145
Wireshark Lab 42: Quickly Examine all SMB Statistics (Statistics Service Response Times SMB)	148
Wireshark Lab 43: Create a Button to Detect High SMB and SMB2 Response Times	149
Wireshark Lab 44: Graph SMB Response Times	149
Chapter 6: Identify Problems Using Wireshark's Expert	151
Overview of Wireshark's Expert Infos System	153
Previous Segment Not Captured	154
Display Filter Value	154
Overview of Wireshark's Packet Loss Detection Process	154
What Causes Packet Loss?	155
Packet Loss Recovery Method #1 – Fast Recovery	156
Packet Loss Recovery Method #2 – Sender Retransmission Timeout (RTO)	157
<i>packet-tcp.c</i> Code and Comments	157
Wireshark Lab 45: Use a Filter to Count Previous Segment Not Captured Indications	158
Wireshark Lab 46: Add TCP Sequencing Columns	159
Wireshark Lab 47: Build a “Bad TCP” Filter Expression Button	161
Wireshark Lab 48: Find Packet Loss Counts with Expert Infos	162
Wireshark Lab 49: Find Out Where Packets are Being Dropped	163
Duplicate ACKs	166
Display Filter Value	166
Traffic Analysis Overview	166
What Causes Duplicate ACKs?	167
<i>packet-tcp.c</i> Code and Comments	168
Wireshark Lab 50: Use a Filter to Count Duplicate ACKs	169
Wireshark Lab 51: Find Duplicate ACKs with Expert Infos	170
Wireshark Lab 52: Determine if Selective ACK (SACK) is in Use	172

Out-of-Order Packets	174
Display Filter Value	174
Traffic Analysis Overview	174
What Causes Out-of-Order Packets?	174
<i>packet-tcp.c</i> Code and Comments	175
Wireshark Lab 53: Use a Filter to Count Out-of-Order Packets	178
Wireshark Lab 54: Find Out-of-Order Packets with Expert Infos	179
Fast Retransmissions	180
Display Filter Value	180
Traffic Analysis Overview	180
What Causes Fast Retransmissions?	181
<i>packet-tcp.c</i> Code and Comments	181
Wireshark Lab 55: Use a Filter to Count Fast Retransmission Packets	183
Wireshark Lab 56: Find Fast Retransmission Packets with Expert Infos	184
Retransmissions	186
Display Filter Value	186
Traffic Analysis Overview	186
What Causes Retransmissions?	186
<i>packet-tcp.c</i> Code and Comments	187
Wireshark Lab 57: Use a Filter to Count Retransmission Packets	188
Wireshark Lab 58: Find Retransmission Packets with Expert Infos and Use a Time Reference to Compare Expert Infos Designations	189
ACKed Unseen Segment	191
Display Filter Value	191
Traffic Analysis Overview	191
What Causes ACKed Unseen Segment?	191
<i>packet-tcp.c</i> Code and Comments	192
Wireshark Lab 59: Use a Filter to Count ACKed Unseen Segment Warnings	193
Wireshark Lab 60: Find ACKed Unseen Segment Indications Using Expert Infos	193
Keep Alive and Keep Alive ACK	195
Display Filter Values	195
Traffic Analysis Overview	195
What Causes Keep Alives?	195
<i>packet-tcp.c</i> Code and Comments	196
Wireshark Lab 61: Use a Filter to Count Keep Alive/Keep Alive ACK Packets	197
Wireshark Lab 62: Find Keep Alive/Keep Alive ACK Packets with Expert Infos	198
Wireshark Lab 63: Identify Keep Alive Packets used in Zero Window Conditions	199

Zero Window 201

 Display Filter Value 201

 Traffic Analysis Overview 201

 What Causes a Zero Window Condition? 201

 Window Size Value Field vs. Calculated Window Size Field 202

packet-tcp.c Code and Comments 203

 Wireshark Lab 64: Use a Filter and Column to Count and Analyze Zero Window Packets 203

 Wireshark Lab 65: Find Zero Window Packets with Expert Infos 204

 Window Full Precedes the Problem 205

 Wireshark Lab 66: Measure the Delay Caused by a Window Full Condition 206

Window Full 208

 Display Filter Value 208

 Traffic Analysis Overview 208

 What Causes Window Full? 208

packet-tcp.c Code and Comments 209

 Wireshark Lab 67: Use a Filter to Count Window Full Packets 210

 Wireshark Lab 68: Find Window Full Packets with Expert Infos 211

 Wireshark Lab 69: Use Bytes in Flight to Watch a “Stuck” Application 212

Zero Window Probe and Zero Window Probe ACK 215

 Display Filter Value 215

 What Causes Zero Window Probes? 215

packet-tcp.c Code and Comments 215

 Wireshark Lab 70: Use a Filter to Count Zero Window Probe and Zero Window Probe ACK Packets 216

 Wireshark Lab 71: Find Zero Window Probe and Zero Window Probe ACK Packets with Expert Infos 217

Window Update 218

 Display Filter Value 218

 Traffic Analysis Overview 218

 What Causes Window Updates? 218

packet-tcp.c Code and Comments 218

 Wireshark Lab 72: Use a Filter to Count Window Update Packets 219

 Wireshark Lab 73: Find Window Update Packets with Expert Infos 220

Reused Ports 222

 Display Filter Value 222

 Traffic Analysis Overview 222

 What Causes Reused Ports? 223

packet-tcp.c Code and Comments 223

 Wireshark Lab 74: Use a Filter to Count Reused Port Packets 224

 Wireshark Lab 75: Find Reused Ports with Expert Infos 225

Checksum Errors 229
 Display Filter Value 229
 Traffic Analysis Overview 229
 What Causes Checksum Errors? 229
packet-tcp.c Code and Comments 230
 Wireshark Lab 76: Detect Checksum Errors with Expert Infos 231

Chapter 7: Identify Application Errors 235

Detect DNS Errors 237
 Display Filter Value 237
 Traffic Analysis Overview 237
 Wireshark Lab 77: Create and Use a “DNS Errors” Filter Expression Button 238
 Detect HTTP Errors 241
 Display Filter Value 241
 Traffic Analysis Overview 241
 Wireshark Lab 78: Create and Use an “HTTP Errors” Filter Expression Button 243
 Detect SMB/SMB2 Errors 245
 Display Filter Value 245
 Traffic Analysis Overview 245
 Wireshark Lab 79: Create and Use an “SMB/SMB2 Errors” Filter Expression Button 248
 Detect SIP Errors 250
 Display Filter Value 250
 Traffic Analysis Overview 250
 Wireshark Lab 80: Create and Use a “SIP Errors” Filter Expression Button 253
 Detect Error Responses of Other Applications 255
 Wireshark Lab 81: Build Other Application Error Filters and Filter Expression Buttons 255

Part 3: Use Graphs to Detect Problems 259

Chapter 8: Master Basic and Advanced IO Graph Functions 261

Graph Individual Conversations 263
 Wireshark Lab 82: Graph and Compare Throughput of Two Conversations 263
 Graph all Traffic for a Single Application 267
 Wireshark Lab 83: Graph and Compare Traffic for Two Applications 267
 Use CALC Functions on the Advanced IO Graph 270
 Wireshark Lab 84: Graphing the TCP Payload Throughput with an Advanced IO Graph 271

Chapter 9: Graph Throughput Problems	273
Detect Consistently Low Throughput due to Low Packet Sizes.....	275
Wireshark Lab 85: Graph Low Throughput Due to Itty Bitty Stinkin' Packets.....	275
Identify Queuing Delays along a Path.....	277
Wireshark Lab 86: Identify the Queued Traffic Pattern in an IO Graph.....	277
Correlate Drops in Throughput with TCP Problems (the "Golden Graph")	280
Wireshark Lab 87: Identify Network Problems with the "Golden Graph"	280
Chapter 10: Graph Time Delays	283
Graph High Delta Times (UDP-Based Application)	285
Wireshark Lab 88: Graph a Slow DHCP Server Response.....	285
Graph High TCP Delta Time (TCP-Based Application)	286
Wireshark Lab 89: Graph and Analyze High TCP Delta Times.....	286
Chapter 11: Graph Other Network Problems	289
Graph Window Size Problems.....	291
Wireshark Lab 90: Graph Window Size Issues Using TCP Analysis Filters.....	291
Wireshark Lab 91: Graph Window Size Issues Using the Calculated Window Size Field and Window Size Graph	293
Graph Packet Loss and Recovery	295
Wireshark Lab 92: Graph Packet Loss and Recovery Using TCP Analysis Filters	295
Wireshark Lab 93: Graph Packet Loss and Recovery Using the TCP Time-Sequence Graph.....	297
Chapter 12: Export Traffic to Graph in 3rd Party Tools	299
Export Packet List Pane Columns to CSV Format.....	301
Wireshark Lab 94: Export All Columns to CSV Format	301
Export Your Trace File/Packet Comments Report.....	305
Wireshark Lab 95: Add and Export Trace File and Packet Comments	305
Export Packets to TXT Format.....	308
Wireshark Lab 96: Export Unusual DNS Server Failures.....	308
 Part 4: Final Tips for Troubleshooting with Wireshark.....	 311
Chapter 13: Final Tips.....	313
Tips for Working with Large Trace Files	315
Split Large Files with Editcap	315
Create a Trace File Subset with Tshark and Display Filters	315
Open Large Trace Files in Cascade Pilot (aka "Pilot").....	316
Tips for Naming Your Trace Files	319
Tips for Detecting Security vs. Performance Issues	320

Tips for Quickly Creating the “Golden Graph”	321
Wireshark Lab 97: Save a Bad TCP Display Filter for the Golden Graph.....	321
Tips for Analyzing TCP-Based Applications	323
Tips for Locating the Cause of Intermittent Problems	324
Tips for Detecting WLAN Problems.....	325
Capture Management, Control and Data Frames	325
Prepend Radiotap or PPI Headers	325
Capture the 802.11 Header	325
Wireshark Lab 98: Filter on WLAN Retries and Examine Signal Strength.....	326
Tips for Sanitizing Trace Files	329
Edit Trace Files with a Hex Editor	329
Use TraceWrangler	330
Tips for Faster Problem Detection.....	331
Tips to Learn How TCP/IP Works.....	332
Analyze Your Own Traffic.....	332
Tips for When You Get Stuck	334
Appendix A: Create a Complete Wireshark Troubleshooting Profile.....	335
Import Laura’s Troubleshooting Profile.....	337
Wireshark Lab 99: Import a Troubleshooting Profile	337
Do It Yourself: Build Your New Troubleshooting Profile	339
Wireshark Lab 100: Create a Troubleshooting Profile	339
Appendix B: Trace File Descriptions	345
Appendix C: Network Analyst’s Glossary	351
Index	369

LIST OF LABS

Wireshark Lab 1: Create Your Troubleshooting Profile.....	33
Wireshark Lab 2: Add and Use a Custom Column to Locate HTTP Delays	36
Wireshark Lab 3: Set the Time Column to Detect Path Latency	39
Wireshark Lab 4: Extract and Save a Single Conversation.....	42
Wireshark Lab 5: Filter Traffic Based on a Port Number.....	45
Wireshark Lab 6: Filter on the HTTP Request Method Field To View Client Requests	47
Wireshark Lab 7: Filter on the Calculated Window Size Field to Locate Buffer Problems	48
Wireshark Lab 8: Filter Out Applications and Protocols	51
Wireshark Lab 9: Create a Button to Detect Missing TCP Functionality	53
Wireshark Lab 10: Use Expert Infos to Identify Network Problems.....	56
Wireshark Lab 11: Change the TCP Dissector Reassembly Setting to Properly Measure HTTP Response Times.....	59
Wireshark Lab 12: Find the Most Active Conversation (Byte Count)	65
Wireshark Lab 13: Quickly Spot a Throughput Problem in an IO Graph.....	67
Wireshark Lab 14: Build a Coloring Rule to Highlight DNS Errors	69
Wireshark Lab 15: Test Your WLAN Native Adapter Capture Capabilities	82
Wireshark Lab 16: Capture and Work with File Sets.....	85
Wireshark Lab 17: Create and Apply a MAC Address Filter	88
Wireshark Lab 18: Identify a Name Resolution Problem.....	99
Wireshark Lab 19: Find Local Address Resolution Problems	100
Wireshark Lab 20: No Response to TCP Connection Request.....	101
Wireshark Lab 21: No Response to Service Request	103
Wireshark Lab 22: Obtain UDP Conversation Statistics and Filter on a UDP Conversation.....	112
Wireshark Lab 23: Add/Sort a Delta Time Column	114
Wireshark Lab 24: Add/Sort a Delta Displayed Time Column.....	116
Wireshark Lab 25: Graph UDP Delays.....	117
Wireshark Lab 26: Obtain TCP Conversation Statistics.....	120
Wireshark Lab 27: Filter on a TCP Conversation Using the Stream Index Field	122
Wireshark Lab 28: Add a TCP Stream Index Column.....	123
Wireshark Lab 29: Add/Sort a TCP Delta Time Column	123
Wireshark Lab 30: Add a “TCP Delay” Button.....	125
Wireshark Lab 31: Obtain the Round Trip Time (RTT) Using the TCP Handshake	128
Wireshark Lab 32: Obtain RTT using Display Filters	131
Wireshark Lab 33: Graph TCP Delays.....	132
Wireshark Lab 34: Add/Sort a <code>dns.time</code> Column to Find DNS Response Times	135
Wireshark Lab 35: Create a Button to Detect High DNS Response Times.....	137
Wireshark Lab 36: Graph DNS Response Times.....	138
Wireshark Lab 37: Disable the <i>Allow Subdissector to Reassemble TCP Streams</i> Preference Setting	140
Wireshark Lab 38: Add/Sort an HTTP Response Time Column to Find HTTP Response Times	141
Wireshark Lab 39: Create a Button to Detect High HTTP Response Times.....	143

Wireshark Lab 40: Graph HTTP Response Times	144
Wireshark Lab 41: Add/Sort an SMB Response Time Column	145
Wireshark Lab 42: Quickly Examine all SMB Statistics (Statistics Service Response Times SMB)	148
Wireshark Lab 43: Create a Button to Detect High SMB and SMB2 Response Times	149
Wireshark Lab 44: Graph SMB Response Times	149
Wireshark Lab 45: Use a Filter to Count Previous Segment Not Captured Indications	158
Wireshark Lab 46: Add TCP Sequencing Columns	159
Wireshark Lab 47: Build a “Bad TCP” Filter Expression Button	161
Wireshark Lab 48: Find Packet Loss Counts with Expert Infos	162
Wireshark Lab 49: Find Out Where Packets are Being Dropped	163
Wireshark Lab 50: Use a Filter to Count Duplicate ACKs	169
Wireshark Lab 51: Find Duplicate ACKs with Expert Infos	170
Wireshark Lab 52: Determine if Selective ACK (SACK) is in Use	172
Wireshark Lab 53: Use a Filter to Count Out-of-Order Packets	178
Wireshark Lab 54: Find Out-of-Order Packets with Expert Infos	179
Wireshark Lab 55: Use a Filter to Count Fast Retransmission Packets	183
Wireshark Lab 56: Find Fast Retransmission Packets with Expert Infos	184
Wireshark Lab 57: Use a Filter to Count Retransmission Packets	188
Wireshark Lab 58: Find Retransmission Packets with Expert Infos and Use a Time Reference to Compare Expert Infos Designations	189
Wireshark Lab 59: Use a Filter to Count ACKed Unseen Segment Warnings	193
Wireshark Lab 60: Find ACKed Unseen Segment Indications Using Expert Infos	193
Wireshark Lab 61: Use a Filter to Count Keep Alive/Keep Alive ACK Packets	197
Wireshark Lab 62: Find Keep Alive/Keep Alive ACK Packets with Expert Infos	198
Wireshark Lab 63: Identify Keep Alive Packets used in Zero Window Conditions	199
Wireshark Lab 64: Use a Filter and Column to Count and Analyze Zero Window Packets	203
Wireshark Lab 65: Find Zero Window Packets with Expert Infos	204
Wireshark Lab 66: Measure the Delay Caused by a Window Full Condition	206
Wireshark Lab 67: Use a Filter to Count Window Full Packets	210
Wireshark Lab 68: Find Window Full Packets with Expert Infos	211
Wireshark Lab 69: Use Bytes in Flight to Watch a “Stuck” Application	212
Wireshark Lab 70: Use a Filter to Count Zero Window Probe and Zero Window Probe ACK Packets	216
Wireshark Lab 71: Find Zero Window Probe and Zero Window Probe ACK Packets with Expert Infos	217
Wireshark Lab 72: Use a Filter to Count Window Update Packets	219
Wireshark Lab 73: Find Window Update Packets with Expert Infos	220
Wireshark Lab 74: Use a Filter to Count Reused Port Packets	224
Wireshark Lab 75: Find Reused Ports with Expert Infos	225
Wireshark Lab 76: Detect Checksum Errors with Expert Infos	231
Wireshark Lab 77: Create and Use a “DNS Errors” Filter Expression Button	238
Wireshark Lab 78: Create and Use an “HTTP Errors” Filter Expression Button	243
Wireshark Lab 79: Create and Use an “SMB/SMB2 Errors” Filter Expression Button	248
Wireshark Lab 80: Create and Use a “SIP Errors” Filter Expression Button	253
Wireshark Lab 81: Build Other Application Error Filters and Filter Expression Buttons	255
Wireshark Lab 82: Graph and Compare Throughput of Two Conversations	263
Wireshark Lab 83: Graph and Compare Traffic for Two Applications	267
Wireshark Lab 84: Graphing the TCP Payload Throughput with an Advanced IO Graph	271
Wireshark Lab 85: Graph Low Throughput Due to Itty Bitty Stinkin’ Packets	275
Wireshark Lab 86: Identify the Queued Traffic Pattern in an IO Graph	277

Wireshark Lab 87: Identify Network Problems with the “Golden Graph”	280
Wireshark Lab 88: Graph a Slow DHCP Server Response	285
Wireshark Lab 89: Graph and Analyze High TCP Delta Times.....	286
Wireshark Lab 90: Graph Window Size Issues Using TCP Analysis Filters	291
Wireshark Lab 91: Graph Window Size Issues Using the Calculated Window Size Field and Window Size Graph	293
Wireshark Lab 92: Graph Packet Loss and Recovery Using TCP Analysis Filters.....	295
Wireshark Lab 93: Graph Packet Loss and Recovery Using the TCP Time-Sequence Graph.....	297
Wireshark Lab 94: Export All Columns to CSV Format.....	301
Wireshark Lab 95: Add and Export Trace File and Packet Comments	305
Wireshark Lab 96: Export Unusual DNS Server Failures.....	308
Wireshark Lab 97: Save a Bad TCP Display Filter for the Golden Graph.....	321
Wireshark Lab 98: Filter on WLAN Retries and Examine Signal Strength.....	326
Wireshark Lab 99: Import a Troubleshooting Profile	337
Wireshark Lab 100: Create a Troubleshooting Profile	339