



# Wireshark<sup>®</sup> Protocols and Troubleshooting

V2.2A

STUDENT MANUAL

SAMPLE COURSE  
OUTLINE

## COURSE OUTLINE

- Section 1: Course Introduction and Resources
- Section 2: Wireshark Essential Features for Troubleshooting (Course Profile)
- Section 3: Capture Methods and Capture Filters
- Section 4: Customization - Wireshark Preferences
- Section 5: Navigation, Coloring, and Reassembly
- Section 6: Detect Application and Path Delays (Working with Time)
- Section 7: Extract and Interpret Essential Trace File Statistics
- Section 8: Focus on Traffic Using Display Filters
- Section 8: TCP/IP Communications Overview
- Section 10: Analyze Domain Name System (DNS) Traffic
- Section 11: Analyze Address Resolution Protocol (ARP) Traffic
- Section 12: Analyze Internet Protocol (IPv4) Traffic
- Section 13: Analyze Internet Control Message Protocol (ICMP) Traffic
- Section 14: Analyze User Datagram Protocol (UDP) Traffic
- Section 15: Analyze Transmission Control Protocol (TCP) Traffic
- Section 16: Analyze Hypertext Transfer Protocol (HTTP) Traffic
- Section 17: Decrypting Traffic
- Section 18: Command-Line and 3<sup>rd</sup>-Party Tools
- Appendix A: Advanced Display Filters
- Appendix B: Analyze VoIP Traffic
- Appendix C: Analyze Dynamic Host Configuration Protocol (DHCP) Traffic
- Appendix D: Analyze File Transfer Protocol (FTP) Traffic

## LAB LIST

- Lab 1: Create Your Troubleshooting Profile
- Lab 2: Use GeoIP Mapping to Find an Issue
- Lab 3: Build a Coloring Rule to Differentiate DNS Traffic
- Lab 4: Detect and Differentiate Delays
- Lab 5: Find the Top Talkers and Protocols/Applications on a Network
- Lab 6: Create and Use an I/O Graph to Spot Performance Issues
- Lab 7: Practice Display Filtering
- Lab 8: Catch DNS Errors and Slow DNS Responses
- Lab 9: Find the Fault – Network Disconnects
- Lab 10: Filter on Problem Addresses
- Lab 11: Analyze and Color ICMP Traffic
- Lab 12: Analyze UDP-based Multicast Streams and Queuing Delays
- Lab 13: Use an IO Graph to Locate TCP Performance Issues
- Lab 14: Determine the Cause of Slow Page Loading
- Lab 15: Create a Button to Detect HTTP Error Responses
- Lab 16: Export an HTTP Object (Carving)
- Lab 17: Decrypt HTTPS Communications
- Lab 18: Evaluate, Extract, and Capture with CLI Tools

**SAMPLE  
COURSE  
OUTLINE**

**Chappell University® Course:  
Wireshark® Protocols and Troubleshooting Student Manual**

Copyright 2024 Protocol Analysis Institute, Inc. All rights reserved. No part of this Student Manual, or related materials for this training course, including interior design, cover design and trace files, may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) without the prior written permission of the publisher.

ISBN13: N/A

Student Manual Part Number: TR6L-A v3.1B

Distributed worldwide for Chappell University through Protocol Analysis Institute, Inc.

For general information on Chappell University or Protocol Analysis Institute, Inc, including information on corporate licenses, updates, future titles, or courses, contact Protocol Analysis Institute, Inc. at [info@chappellU.com](mailto:info@chappellU.com).

For authorization to photocopy items for corporate, personal or educational use, contact Protocol Analysis Institute, Inc. at [info@chappellU.com](mailto:info@chappellU.com).

Trademarks: All brand names and product names used in this book or mentioned in this course are trade names, service marks, trademarks, or registered trademarks of their respective owners. Protocol Analysis Institute, Inc. is the exclusive course developer for Chappell University.

Limit of Liability/Disclaimer of Warranty. The author and publisher have used their best efforts in preparing this Student Manual and the related materials used in this training course. Protocol Analysis Institute, Inc., Chappell University and the author(s) make no representations or warranties or merchantability or fitness for a particular purpose. Protocol Analysis Institute, Inc. and Chappell University assume no liability for any damages caused by following instructions or using the techniques or tools listed in this Student Manual or related materials used in this training course. Protocol Analysis Institute, Inc., Chappell University and the author(s) make no representations or warranties that extend beyond the descriptions contained in this paragraph. No warranty may be created or extended by sales representatives or written sales materials. The accuracy or completeness of the information provided herein, and the opinions stated herein are not guaranteed or warranted to produce any particular result and the advice and strategies contained herein may not be suitable for every individual. Protocol Analysis Institute, Inc., Chappell University, and author(s) shall not be liable for any loss of profit or any other commercial damages, including without limitation special, incidental, consequential, or other damages.

Copy Protection. In all cases, reselling or duplication of this Student Manual and related materials used in this training course without explicit written authorization is expressly forbidden.

Protocol Analysis Institute, Inc.  
dba Chappell University  
720 N. 10<sup>th</sup> Street, Suite A352  
Renton, WA 98057 USA

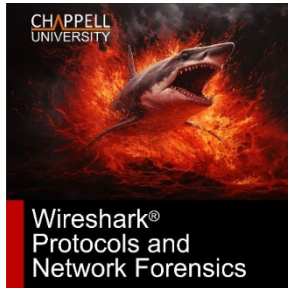
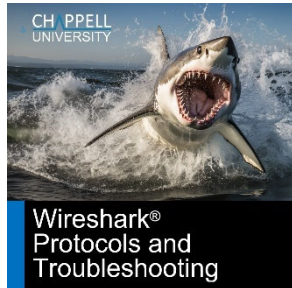
Chappell University®  
720 N. 10<sup>th</sup> Street, Suite A352  
Renton, WA 98057 USA  
[info@chappellU.com](mailto:info@chappellU.com)  
[www.chappellU.com](http://www.chappellU.com)

**SAMPLE  
COURSE  
OUTLINE**

## ADD-ONS

---

**All-Access Pass** The All Access Pass provides full-time access to recorded courses focusing on Wireshark functionality, network troubleshooting, network forensics, and more. Visit <https://chappellu.com> for more information.



**WCNA Exam Vouchers** Purchase in bulk to take the WCNA Exam (online proctored or at a Kryterion testing center worldwide). The WCNA Certification Exam focuses on analyzing packets and protocols, for network troubleshooting, optimization, and security. For more information, visit <https://wcnacertification.com>.



For more information, email [info@chappellu.com](mailto:info@chappellu.com).

SAMPLE  
COURSE  
OUTLINE

**About the Course Author**  
**Chappell University Founder**

**Laura Chappell**

Founder, Chappell University  
Sr. Protocol Analyst, Protocol Analysis Institute, Inc.  
Creator, WCNA Certification Program

Ms. Chappell researches, documents, and presents information on network protocols, analysis, Wireshark, network forensics, and interplanetary communications. Ms. Chappell is the creator of the WCNA Certification program (formerly referred to as the Wireshark Certified Network Analyst Certification program). Ms. Chappell also founded the original Wireshark University, Wireshark University Instructor Program, and Wireshark University Training Partner Program.

Ms. Chappell is often called in to analyze more complex network problems that require visibility into the communications system. Her clients include the U.S. Navy, IBM Corporation, Apple, Cisco Systems, Disney, U.S. Court of Appeals, United Bank of Switzerland, Australian High Tech Crime Centre, Capital One Financial Services, U.S. Armory, Hong Kong Police Department, Symantec Corporation, McAfee Corporation, Microsoft, Bank of San Francisco, Beth Israel Medical Center (Harvard), U.S. Joint Warfare Analysis Center, and the Federal Aviation Administration (FAA).

Ms. Chappell mixes onsite analysis services with live analysis training to develop self-sufficient IT teams within her client organizations.

As a member of the High Technology Crime Investigation Association (HTCIA) and the FBI's Infragard, Ms. Chappell has trained local, regional, national, and international law enforcement officers, as well as corporate security professionals on the methods and tools used to attack and defend networks. Ms. Chappell is also a voting member of Institute for Electrical and Electronics Engineers (IEEE) (member since 1990).

Ms. Chappell's enthusiasm for her topics, sense of humor and preference for working "live" during sessions has consistently ranked her as a top presenter at numerous industry conferences including Microsoft TechEd North America, Microsoft TechEd Europe, HP Technical Forum, Cisco Live, HTCIA International Conference, SharkFest, and InterOp.

In addition, Ms. Chappell is currently an active member of the Interplanetary Networking Special Interest Group focused on the documentation of deep space networking communication protocols. Ms. Chappell regularly lectures on the Deep Space Network (DSN) and Delay and Disruption Tolerant Networking (DTN).

Ms. Chappell can be reached via email at [laura@chappellu.com](mailto:laura@chappellu.com).

**SAMPLE  
COURSE  
OUTLINE**

## HOW TO PURCHASE A CUSTOM COURSE

Bring Laura Chappell online or onsite to speed up your team's troubleshooting and forensics processes.

Complete and submit the [Course Estimator/Quote Request](#) (Course Designer) document or simply let us know the following:

1. **Course Focus:** Do you want the course to focus on troubleshooting, network forensics, and/or general Wireshark functionality
2. **Course Length:** Minimum course length is 2 days. Laura's maximum course length is 10 days.
3. **Date Range:** Let us know which in which months you'd like the course delivered. We typically need at least 2 months advance preparation time.

**COURSE ESTIMATOR/QUOTE REQUEST**  
**CHAPPELL UNIVERSITY**

Ready to train your team on Wireshark, TCP/IP analysis, troubleshooting, and network forensics? Complete Part I of this Course Estimator and Quote Request Form to determine the cost of training.

Training is available in three formats:

- Onsite (Onsite delivery is temporarily on hold)
- Onsite Live (Instructor led, lab-based, connected via the internet - requires with your own traffic files)
- On-Demand (online recording, available 24/7, transcripts, one-year All Access Pass subscriptions)

Please contact us at [info@chappellu.com](mailto:info@chappellu.com) if you have any questions.  
Email completed forms to: Pat Tibboney [pat@chappellu.com](mailto:pat@chappellu.com)

**Part I: Training Project Info (Required for Formal Quotes)**

Use this form for group pricing for onsite, online or on-demand training.

Project Title: \_\_\_\_\_  
Contact Name: \_\_\_\_\_  
Company: \_\_\_\_\_  
Phone Number: \_\_\_\_\_  
Email Address: \_\_\_\_\_  
Billing Address for Quote: \_\_\_\_\_  
Desired Course Format:  Onsite Live  
 Onsite Live (On-Hold)  
 On-Demand (All Access Pass Subscriptions)  
 Other \_\_\_\_\_  
Course Delivery Timeline:  Within 3 months  
 3-4 months  
 4+ months  
 I have specific dates in mind (see next item)  
Desired Training Dates: \_\_\_\_\_  
Course Location (if known): \_\_\_\_\_

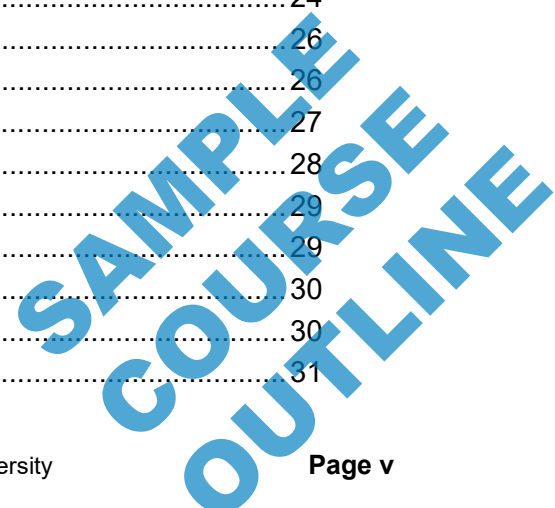
Watch [Change Sheet](#) (on-site)

Questions? Contact us at [info@chappellu.com](mailto:info@chappellu.com).

**SAMPLE  
COURSE  
OUTLINE**

## Table of Contents

About the Course Author Chappell University Founder.....	iii
<b>Section 1: Course Introduction and Resources .....</b>	<b>1</b>
Course Logistics .....	3
Course Content.....	3
Course Supplements .....	4
The Golden Rule of Troubleshooting.....	5
Top Causes of Performance Problems.....	6
About the Network Forensics 3-Day Labs-Only Course .....	7
<b>Section 2: Wireshark Essential Elements and Features (Course Profile) .....</b>	<b>9</b>
The Wireshark License .....	11
Get the Latest Version of Wireshark.....	12
Stable Release Version/Subversion Numbering.....	13
Developer Release Version/Subversion Numbering.....	13
Capturing Traffic: Link-Layer Interfaces.....	14
Opening Trace Files .....	15
Processing Packets .....	16
Core Engine .....	16
Dissectors, Plugins and Display Filters.....	16
The Qt Framework Provides the User Interface .....	16
The Qt Interface Overview.....	17
Using Linked Panes.....	18
The Main Toolbar.....	19
The Related Packets Indicator.....	20
Master the Intelligent Scroll Bar.....	21
The Changing Status Bar .....	22
First Step: Create a Troubleshooting Profile.....	23
Lab 1: Create Your Troubleshooting Profile.....	24
Right-Click Functionality .....	26
Click-and-Drag Functionality.....	26
Build Display Filter Buttons to Spot Problems Faster .....	27
Keyboard Shortcuts (Accelerators).....	28
General Analyst Resources .....	29
How to Use <i>ask.wireshark.org</i> .....	29
Your First Task When You Leave Class - Baseline.....	30
Use Trace File and Packet Comments (Annotations).....	30
Use Logical Naming Conventions for Trace Files.....	31



**Section 3: Capture Methods and Capture Filters.....35**

Analyzer Placement: Switches ..... 37

Walk-Through a Sample SPAN Configuration ..... 38

Analyze Full-Duplex Links with a Network TAP ..... 39

Dealing with Encrypted Traffic via Proxy ..... 40

Analyzing Wireless Networks ..... 41

USB Capture (USBPcap)..... 42

Initial Analyzing Placement..... 43

Identify Active Capture Interfaces Using Sparklines..... 44

Save Directly to Disk..... 45

    Save to File Sets for Manageable File Sizes ..... 45

    Use a Ring Buffer to Avoid Filling a Drive ..... 45

Capture Output and Options..... 46

    Define the Criteria to Create a New File ..... 46

    Define Auto-Stop Criteria ..... 47

    Set a Location for Your Temporary Trace File ..... 47

Limit Your Capture with Capture Filters ..... 48

Examine Key Capture Filters ..... 49

**Section 4: Customization - Wireshark Preferences ..... 53**

Customize the User Interface ..... 55

Manage Your Columns ..... 56

Set Your Global Capture Preferences ..... 57

Define Name Resolution Preferences ..... 58

Lab 2: GeolP Mapping to Find an Issue..... 60

Configure Individual Protocol Preferences ..... 64

Search for Advanced Preferences ..... 65

**Section 5: Navigation, Coloring, and Reassembly ..... 69**

Move Around Quickly: Navigation Techniques ..... 71

Find a Packet Based on Various Characteristics..... 72

    “Search In” Panes (Used with String and Regular Expression Searches)..... 72

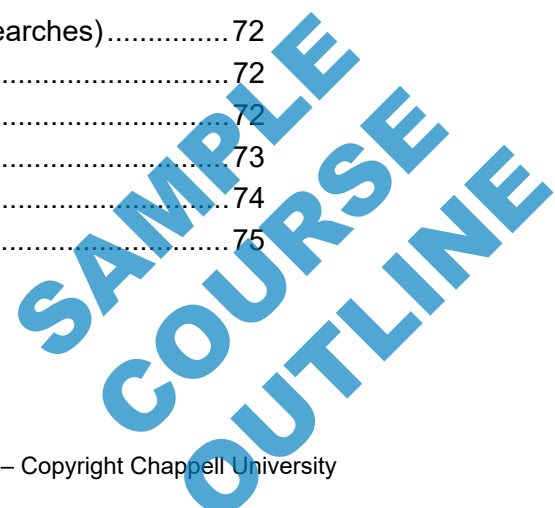
    String Search Options..... 72

    Search Format Options..... 72

Build Permanent Coloring Rules..... 73

Identify a Coloring Source ..... 74

Use the Intelligent Scroll Bar with Custom Coloring Rules ..... 75





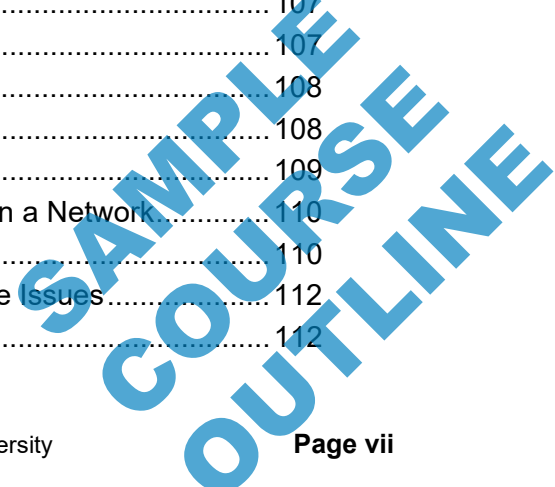
Apply Temporary Coloring .....	76
Mark Packets of Interest .....	77
Follow TCP Streams to Reassemble Data .....	78
Lab 3: Build a Coloring Rule to Differentiate DNS Traffic .....	79

**Section 6: Detect Application and Path Delays (Working with Time) ..... 83**

Examine the Delta Time .....	85
Set a Time Reference .....	85
Reading Time Values .....	86
Compare Timestamp Values .....	87
Seconds Since First Captured Packet (default: <code>frame.time_relative</code> ) .....	87
Seconds Since Previous Captured Packet ( <code>frame.time_delta</code> ) .....	87
Compare Timestamps of Filtered Traffic .....	88
Seconds Since Previous Displayed Packet ( <code>frame.time_delta_displayed</code> ) ..	88
Application Response Time Fields .....	88
Use TCP Conversation Timestamps .....	89
Compare TCP Conversation Timestamp Values .....	90
Determine the Initial Round Trip Time (iRTT) .....	91
Troubleshooting Example Using Time .....	92
Wire Latency (aka Path Latency) .....	92
Processing Latency .....	92
Analyzing Delay Types .....	93
Lab 4: Detect and Differentiate Delays .....	95
Trace File <i>lab-timeanalysis.pcapng</i> .....	95

**Section 7: Extract and Interpret Essential Trace File Statistics ..... 103**

Capture File Properties .....	105
View Active Protocols .....	106
Filter On or Colorize Protocol Traffic .....	106
Graph Throughput to Spot Performance Problems Quickly .....	107
Distinguish Traffic with Various Styles .....	107
Locate the Most Active Conversations and Endpoints .....	108
Kibibyte (KiB) and Mebibytes (MiB)? .....	108
Numerous Other Statistics Are Available .....	109
Lab 5: Find the Top Talkers and Protocols/Applications on a Network .....	110
Trace File <i>lab-gentraffic.pcapng</i> .....	110
Lab 6: Create and Use an I/O Graph to Spot Performance Issues .....	112
Trace File <i>lab-iograph.pcapng</i> .....	112



**Section 8: Focus on Traffic Using Display Filters ..... 117**

Overview of Display Filters ..... 119

Filter on Conversations/Endpoints ..... 120

Fast Filtering Based on Fields ..... 121

Comparison/Membership Operators ..... 122

Backslashes and Smart Quotes ..... 123

Filter on Text Strings ..... 124

Regular Expressions 101 ..... 125

Build Display Filter Buttons ..... 126

Watch for Common Display Filter Mistakes ..... 127

    Filter Error Checking ..... 127

Lab 7: Practice Display Filtering ..... 128

Trace File *lab-http-espn-b.pcapng* ..... 128

**Section 9: TCP/IP Communications Overview ..... 133**

TCP/IP Functionality Overview ..... 135

When Everything Goes Right ..... 136

The Multi-Step Resolution Process ..... 137

    Port Number Resolution ..... 138

    Name Resolution ..... 138

    Location Resolution ..... 139

    Local – MAC Address Resolution ..... 139

    Remote – Route Resolution ..... 140

    Remote – MAC Address Resolution for a Gateway ..... 140

Resolution Helped Build the Packet ..... 141

Where Can Faults Occur? ..... 142

Wireshark Features for Issue Detection ..... 143

**Section 10: Analyze Domain Name System (DNS) Traffic ..... 147**

DNS Overview ..... 149

DNS Packet Structure ..... 150

    Transaction ID ..... 150

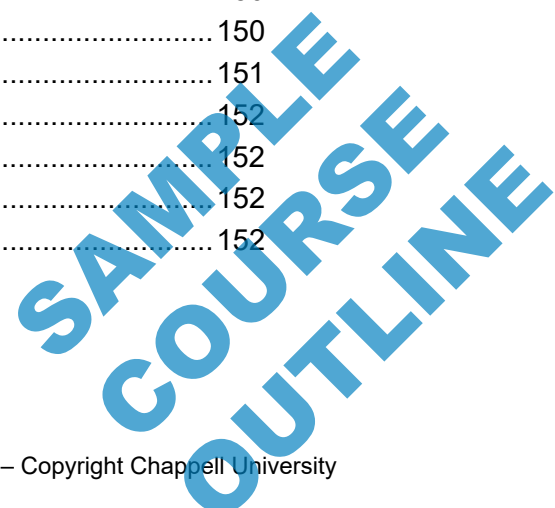
    Flags ..... 151

    Questions ..... 152

    Answer Resource Records (RRs) ..... 152

    Authority RRs ..... 152

    Additional RRs ..... 152



DNS Queries..... 152  
 Name ..... 152  
 Type ..... 152  
 Class ..... 152  
 Answer RRs ..... 152  
 Authority RRs..... 153  
 Additional RRs ..... 153  
 DoT, DoH, and DoQ Detection ..... 154  
 Filter on DNS and DNS Variations..... 155  
 Lab 8: Catching DNS Errors and Slow DNS Responses ..... 156  
 Trace Files *lab-dns-errors-partial.pcapng*; *dns-notgreat.pcapng* ..... 156

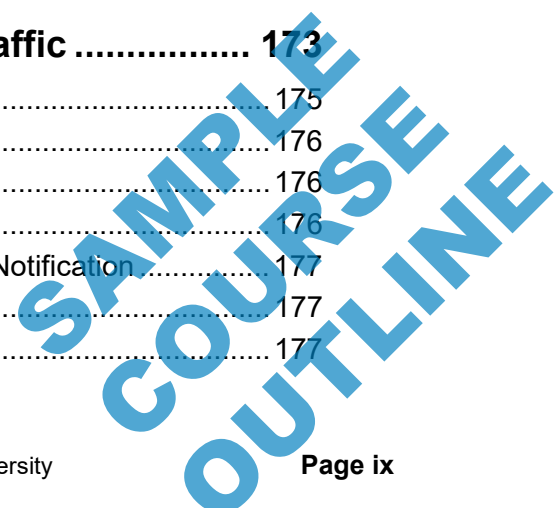
**Section 11: Analyze Address Resolution**

**Protocol (ARP) Traffic..... 161**

ARP Overview ..... 163  
 ARP Variations..... 163  
 ARP on the IPv4 Client Bootup..... 164  
 169.254 Addressing..... 164  
 ARP Packet Structure..... 165  
 Hardware Type ..... 165  
 Protocol Type..... 166  
 Hardware Size ..... 166  
 Protocol Size..... 166  
 Opcode ..... 166  
 Sender MAC Address ..... 166  
 Sender IP Address..... 166  
 Target MAC Address ..... 166  
 Target IP Address ..... 166  
 Filter on ARP Traffic ..... 167  
 Lab 9: Find the Fault – Network Disconnects ..... 168  
 Trace File *scott-knockoff.pcapng* Config File *ScottConfig.txt*..... 168

**Section 12: Analyze Internet Protocol (IPv4) Traffic ..... 173**

IPv4 Overview..... 175  
 IPv4 Packet Structure ..... 176  
 Version..... 176  
 Header Length ..... 176  
 Differentiated Services Codepoint and Explicit Congestion Notification..... 177  
 Total Length ..... 177  
 Identification..... 177



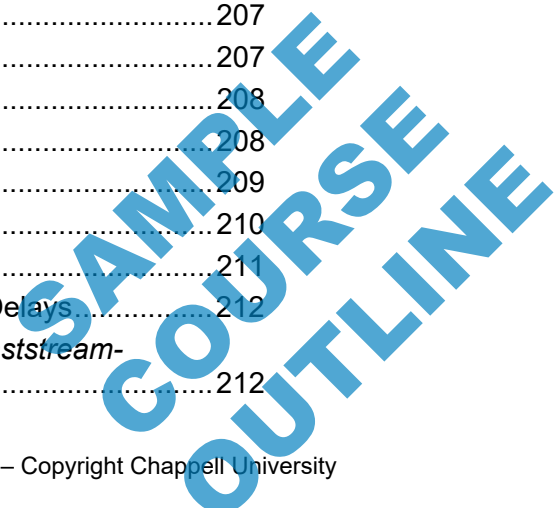
Flags .....	177
Fragment Offset .....	178
Time to Live .....	178
Protocol .....	179
Header Checksum .....	179
Source Address .....	179
Destination Address .....	180
Options .....	180
Analyze Broadcast/Multicast Traffic .....	181
How Many Broadcasts/Multicasts Are Too Many? .....	182
Filter on IPv4 Traffic .....	183
IP Protocol Preferences .....	183
Lab 10: Filter on Problem Addresses .....	184
Trace File <i>lc-cutoff3.pcapng</i> .....	184

**Section 13: Analyze Internet Control Message Protocol (ICMP) Traffic ..... 189**

ICMP Overview .....	191
ICMP Packet Structure .....	192
Checksum .....	192
Type .....	193
Code .....	194
ICMP Type 3/Code 4 .....	196
Filter on ICMP Traffic .....	197
Lab 11: Analyze and Color ICMP Traffic .....	198
Trace Files <i>icmp-tracing.pcapng</i> ; .....	198

**Section 14: Analyze User Datagram Protocol (UDP) Traffic ..... 203**

UDP Overview .....	205
Watch for Service Refusals .....	206
UDP Packet Structure .....	207
Source Port .....	207
Destination Port .....	207
Length .....	208
Checksum .....	208
Filter on UDP Traffic .....	209
Follow UDP Streams to Reassemble Data .....	210
UDP Multicast Stream Analysis .....	211
Lab 12: Analyze UDP-based Multicast Streams and Queuing Delays .....	212
Trace Files <i>lab-udp-mcaststream-queued2.pcapng</i> ; <i>lab-udp-mcaststream-queued3.pcapng</i> .....	212



**Section 15: Analyze Transmission Control Protocol (TCP) Traffic ..... 217**

- TCP Overview..... 219
- The TCP Connection Process ..... 220
- Watch Service Refusals..... 221
- TCP Packet Structure ..... 222
  - Source Port ..... 222
  - Destination Port ..... 222
  - Sequence Number ..... 222
  - Acknowledgment Number ..... 223
  - Data Offset Field (Header Length)..... 223
  - Flags ..... 223
  - Window Field ..... 224
  - Checksum ..... 224
  - Urgent Pointer..... 224
  - TCP Options ..... 224
- TCP Segmentation Offload (TSO)..... 226
- The TCP Sequencing/Acknowledgment Process ..... 227
- Packet Loss Detection ..... 228
- Retransmission Detection..... 229
- Fast Recovery/Fast Retransmission Detection..... 230
- Spurious Retransmission Detection..... 231
- Out-of-Order Segment Detection ..... 232
- Selective Acknowledgement (SACK) Overview..... 233
- TCP Sliding Window Overview ..... 234
- Window Scaling Overview ..... 236
- Window Size Issue: Receive Buffer Problem ..... 237
- Window Size Issue: Unequal Window Size Beliefs ..... 238
- Troubleshoot TCP Quickly with Expert Information ..... 239
  - TCP Expert Information Details Sample ..... 240
  - Expert Information Classifications..... 240
  - What Triggers *TCP Retransmissions*?..... 241
  - What Triggers *Fast Retransmission*?..... 241
  - What Triggers *Spurious Retransmissions*?..... 241
  - What Triggers *Previous Segment Not Captured*?..... 241
  - What Triggers *ACKed Unseen Segment*? ..... 241
  - What Triggers *Keep-Alive*? ..... 241
  - What Triggers *Duplicate ACK*? ..... 242
  - What Triggers *Zero Window*? ..... 242
  - What Triggers *Zero Window Probe*?..... 242
  - What Triggers *Zero Window Probe ACK*? ..... 242

SAMPLE COURSE OUTLINE

What Triggers *Keep-Alive ACK*? ..... 242

What Triggers *Out-of-Order*? ..... 242

What Triggers *Window Update*? ..... 242

What Triggers *Window Full*? ..... 243

What Triggers *TCP Ports Reused*? ..... 243

Filter on TCP Traffic and TCP Problems ..... 244

Properly Set TCP Preferences ..... 245

    Validate the TCP checksum if possible ..... 245

    Allow subdissector to reassemble TCP streams ..... 245

    Calculate conversation timestamps ..... 245

Advanced I/O Graphing ..... 246

    SUM(Y Field) Graphing ..... 246

    MAX(Y Field), MIN(Y Field), and AVG(Y Field) Graphing ..... 247

    COUNT FRAMES(Y Field) ..... 248

    COUNT FIELDS(Y Field) ..... 249

    LOAD(Y Field) Graphing ..... 250

Graph Round Trip Times ..... 251

Graph TCP Throughput ..... 252

    Throughput vs. Goodput ..... 252

Find Problems Using TCP Time Sequence Graphs ..... 253

    Identify TCP Window Size Problems ..... 254

    Identify Retransmissions ..... 255

Lab 13: Use an IO Graph to Locate TCP Performance Issues ..... 256

Trace File *lab-http-download-good.pcapng*; *lab-http-browse-ok.pcapng* ..... 256

Lab 14: Determine the Cause of Slow Page Loading ..... 261

Trace File *lab-slowdownload.pcapng* ..... 261

**Section 16: Analyze Hypertext Transfer Protocol (HTTP) Traffic..... 265**

HTTP Overview ..... 267

HTTP Response Codes ..... 267

HTTP Packet Structure ..... 268

    HTTP Methods ..... 268

Filter on HTTP Traffic ..... 269

Reassembling HTTP Objects ..... 270

HTTP Statistics ..... 271

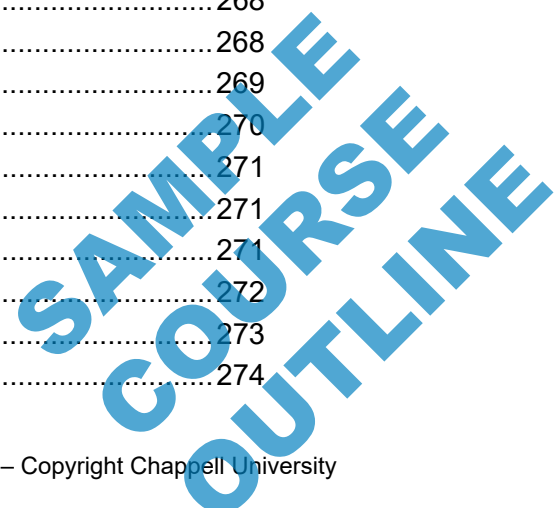
    Load Distribution ..... 271

    Packet Counter ..... 271

    Requests ..... 272

HTTP Response Time ..... 273

Overview of HTTP/2 ..... 274



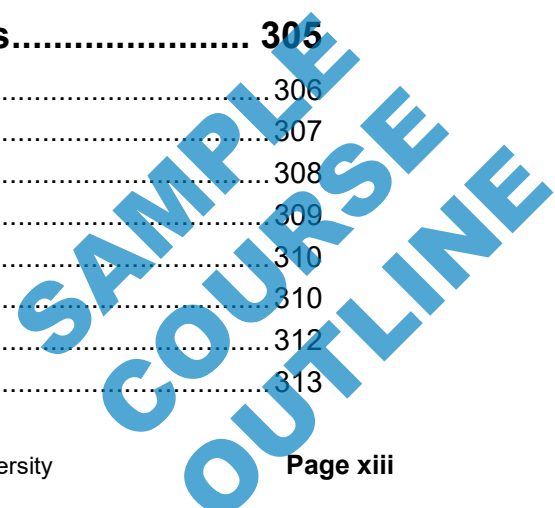
Binary vs. Textual Function.....	274
Multiplexed.....	275
Header Compression.....	275
Push Response.....	275
HTTP/2 Analysis Fundamentals.....	276
Unsecure HTTP/2 Communication Flow.....	276
Secure HTTP/2 Communication Flow (HTTP/2 over TLS).....	277
HTTP/2 Frame Format.....	278
HTTP/2 Type Field.....	278
HTTP/2 Stream Identifier.....	279
HTTP/2 Error Codes.....	280
Filter on HTTP/2 Traffic.....	281
Preparing for HTTP/3 and QUIC.....	281
Lab 15: Create a Button to Detect HTTP Error Responses.....	282
Trace File <i>lab-http-chappellu-b.pcapng http-chappellu101.pcapng</i> <i>http2-errors.pcapng</i> .....	282
Lab 16: Export an HTTP Object (Carving).....	284
Trace File <i>lab-http-chappellu-b.pcapng</i> .....	284

**Section 17: Decrypting Traffic ..... 289**

Dealing with Encrypted Traffic via Proxy.....	291
Analyzing Unencrypted Traffic.....	292
The TLS Handshake Process.....	293
TLS Handshake Packets.....	294
Catching Encrypted Alerts.....	295
Decrypt Traffic with an RSA Key.....	296
Decrypt Traffic with Session Keys.....	297
Inject, Extract, and Discard Secrets.....	298
Filter on TLS.....	299
Lab 17: Decrypt HTTPS Communications.....	300
Trace File <i>lab-rsasnakeoil2.pcapng</i> .....	300

**Section 18: Command-Line and 3rd Party Tools..... 305**

Tshark and Dumpcap Command-Line Tools.....	306
Capinfos Command-Line Tool.....	307
Editcap Command-Line Tool.....	308
Mergecap Command-Line Tool.....	309
Lab 18: Evaluate, Extract, and Capture with CLI Tools.....	310
Trace File <i>violet2.pcapng</i> .....	310
NetworkMiner and CapLoader.....	312
Sanitize Trace Files.....	313



**Appendix A: Advanced Display Filters ..... 315**

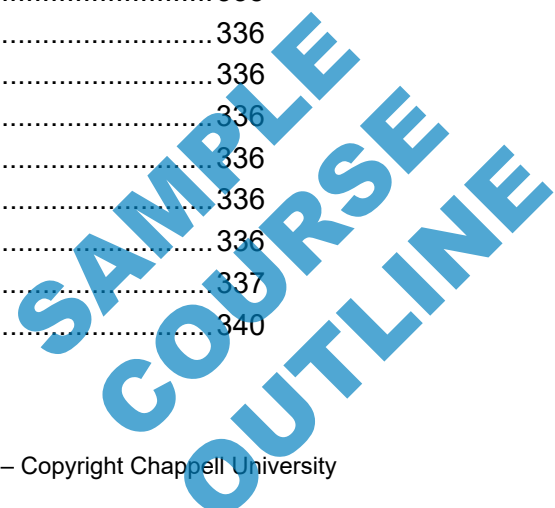
Byte-Offset Filtering ..... 316  
The Slice Operator ..... 317  
Negative Slice Offsets ..... 318  
Bitwise AND (&) (Bit-Masking) ..... 319  
Combine Slice and Bit-Masking ..... 320

**Appendix B: Analyze Voice over IP (VoIP)Traffic ..... 321**

Quick Overview of VoIP Traffic Analysis ..... 322  
    Watch for Error Codes and Packet Loss ..... 323  
SIP and RTP Analysis Overview ..... 324  
SIP Call Setup ..... 325  
Analyzing Call Setup with SIP ..... 326  
Session Bandwidth and RTP Port Definition ..... 327

**Appendix C: Analyze Dynamic Host Configuration Protocol (DHCP) Traffic ..... 329**

Overview of DHCP ..... 330  
DHCP During the Bootup Process ..... 331  
DHCP Relay Agents ..... 334  
Dissect the DHCP Packet Structure ..... 335  
    Message Type ..... 335  
    Hardware Type ..... 335  
    Hardware Length ..... 335  
    Hops ..... 335  
    Transaction ID ..... 335  
    Seconds Elapsed ..... 335  
    BOOTP Flags ..... 335  
    Client IP Address ..... 335  
    Your (Client) IP Address ..... 335  
    Next Server IP Address ..... 335  
    Relay Agent IP Address ..... 336  
    Client MAC Address ..... 336  
    Server Host Name ..... 336  
    Boot File Name ..... 336  
    Magic Cookie ..... 336  
    Option ..... 336  
An Introduction to DHCPv6 ..... 337  
Filter on DHCP Traffic ..... 340





**Appendix D: Analyze File Transfer**

**Protocol (FTP) Traffic..... 341**

- FTP Overview ..... 342
- FTP Packet Structure ..... 343
- Analyze Active Mode Connections ..... 345
- Analyze Passive Mode Connections ..... 346
- Filter on FTP Traffic ..... 347

**SAMPLE  
COURSE  
OUTLINE**

## HOW TO PURCHASE A CUSTOM COURSE

Bring Laura Chappell online or onsite to speed up your team's troubleshooting and forensics processes.

Complete and submit the [Course Estimator/Quote Request](#) (Course Designer) document or simply let us know the following:

1. **Course Focus:** Do you want the course to focus on troubleshooting, network forensics, and/or general Wireshark functionality
2. **Course Length:** Minimum course length is 2 days. Laura's maximum course length is 10 days.
3. **Date Range:** Let us know which in which months you'd like the course delivered. We typically need at least 2 months advance preparation time.

**COURSE ESTIMATOR/QUOTE REQUEST**  
**CHAPPELL UNIVERSITY**

Ready to train your team on Wireshark, TCP/IP analysis, troubleshooting, and network forensics? Complete Part I of this Course Estimator and Quote Request Form to determine the cost of training.

Training is available in three formats:

- Onsite (Onsite delivery is temporarily on hold)
- Onsite Live, instructor-led, lab-based, conducted via the Internet - requires you have your own traffic files
- On-Demand, online recorded, available 24/7, transcripts, one-year All Access Pass subscriptions

Please contact us at [info@chappellu.com](mailto:info@chappellu.com) if you have any questions.  
Email completed forms to: Pat Tibboney [pat@chappellu.com](mailto:pat@chappellu.com)

**Part I: Training Project Info (Required for Formal Quotes)**

Use this form for group pricing for onsite, online or on-demand training

Project Title: \_\_\_\_\_

Contact Name: \_\_\_\_\_

Company: \_\_\_\_\_

Phone Number: \_\_\_\_\_

Email Address: \_\_\_\_\_

Billing Address for Quote: \_\_\_\_\_

Desired Course Format:  Onsite Live  
 Onsite Live (Default)  
 On-Demand (All Access Pass Subscriptions)  
 Other

Course Delivery Timeline:  Within 3 months  
 3-4 months  
 4+ months  
 I have specific dates in mind (see next item)

Desired Training Dates: \_\_\_\_\_

Course Location (if known): \_\_\_\_\_

Watch Complete Course (on-site)

Questions? Contact us at [info@chappellu.com](mailto:info@chappellu.com).

**SAMPLE  
COURSE  
OUTLINE**