

**SAMPLE  
5-DAY COURSE OUTLINE**

# Troubleshooting and Network Forensics with Wireshark®



**CHAPPELLUNIVERSITY**

## **Chappell University™ Sample 5-Day Course: Troubleshooting and Network Forensics with Wireshark®**

Copyright © Protocol Analysis Institute, Inc. All rights reserved. No part of this Sample 5-Day Course Outline, or related materials, 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

Part No: Custom 5-Day Sample Outline

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 408/378-7841 or send email to [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.

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.

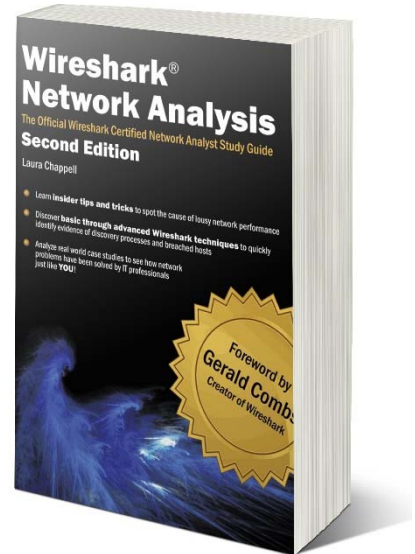
Protocol Analysis Institute, Inc.  
59 Damonte Ranch Pkwy, B340  
Reno, NV 89521 USA  
[info@packet-level.com](mailto:info@packet-level.com)  
[www.packet-level.com](http://www.packet-level.com)

Chappell University  
59 Damonte Ranch Pkwy, B340  
Reno, NV 89521 USA  
[info@chappellU.com](mailto:info@chappellU.com)  
[www.chappellU.com](http://www.chappellU.com)

## Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide – Second Edition

This book focuses on practical use of the Wireshark Certified Network Analyst Exam objectives. For more information, visit [www.wiresharkbook.com](http://www.wiresharkbook.com).

Author: Laura Chappell, Founder of Wireshark University  
Foreword: Gerald Combs, Creator of Wireshark  
Contributors: Numerous  
Paperback: 986 pages  
Publisher: Protocol Analysis Institute  
Website: [www.wiresharkbook.com](http://www.wiresharkbook.com)  
Language: English  
ISBN-10: 1-893939-94-4  
ISBN-13: 978-1-893939-94-3  
Dimensions: 7.44 x 9.69 inches  
Weight: 4 pounds  
Contact: [info@wiresharkbook.com](mailto:info@wiresharkbook.com)  
Exam Info: [www.wiresharktraining.com/certification](http://www.wiresharktraining.com/certification)



### ***Wireshark Certified Network Analyst Exam***

The Wireshark Certified Network Analyst program is designed to validate a professional's abilities to analyze, troubleshoot, secure and optimize networks using Wireshark.

For more information on the Wireshark Certified Network Analyst Exam, visit [www.wiresharktraining.com/certification](http://www.wiresharktraining.com/certification).

## ***About the Course Author***

### ***Wireshark University/Chappell University Founder***

Ms. Chappell is the Founder of Wireshark University and Chappell University, and the Senior Protocol/Security Analyst for the Protocol Analysis Institute, Inc., three US-based companies that research, document and present information on network and host forensics, security breaches and cutting-edge exploit tools.

Ms. Chappell is often called in to troubleshoot more complex network problems that require visibility into the communications system. Her clients include the U.S. Navy, IBM Corporation, Apple, Cisco Systems, U.S. Court of Appeals, United Bank of Switzerland, Dell Corporation, 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 Pharmacia Corporation. With her skills as both a network analyst and Instructor, 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 conferences including Microsoft TechEd North America, Microsoft TechEd Europe, HP Technical Forum, HTCIA International Conference, InterOp, Altiris ManageFusion and Novell BrainShare.

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

[This page intentionally left blank.]

## Table of Contents

Wireshark Certified Network Analyst Exam .....	ii
About the Course Author Wireshark University/Chappell University Founder .....	iii
Course Logistics .....	xvi
Course Content.....	xvi
Course Supplements .....	xvii
Wireshark Version for This Course .....	xvii

## Section 1: Introduction to Network Analysis and Wireshark® ..... 1

TCP/IP Analysis Checklist .....	3
Top Causes of Performance Problems.....	5
The Creation of Ethereal... then Move to Wireshark .....	6
The Wireshark License .....	7
Get the Latest Version of Wireshark.....	8
Stable Release Version/Subversion Numbering.....	8
Developer Release Version/Subversion Numbering.....	8
Capturing Traffic .....	9
Opening Trace Files .....	10
Processing Packets .....	11
Core Engine .....	11
Dissectors, Plugins and Display Filters.....	11
The GTK+ or Qt Framework Provide the User Interface .....	11
GKT+ Interface Overview .....	12
The Icon Toolbar.....	13
The Changing Status Bar .....	14
Right-Click Functionality .....	15
General Analyst Resources .....	16
Your First Task When You Leave Class - Baseline.....	17
Use Annotations.....	17
Use Logical Naming Conventions for Trace Files.....	18

## Section 2: Learn Capture Methods and Use Capture Filters..... 19

Checksum Issues at Capture.....	21
Analyze Switched Networks .....	22
Walk-Through a Sample SPAN Configuration.....	23
Analyze Full-Duplex Links with a Network TAP.....	24
Analyzing Wireless Networks .....	25
Initial Analyzing Placement.....	26

Identify Available Capture Interfaces .....	27
Interface Details .....	27
Save Directly to Disk.....	28
Save to File Sets for Manageable File Sizes .....	28
Use a Ring Buffer to Avoid Filling a Drive .....	28
Capture Output and Options.....	29
Define the Criteria to Create a New File .....	29
Define Auto-Stop Criteria .....	29
Limit Your Capture with Capture Filters.....	30
Examine Key Capture Filters .....	31

### **Section 3: Master Key Wireshark® Troubleshooting Tasks ..... 33**

First Step: Create a Troubleshooting Profile.....	35
Customize the User Interface .....	36
Add Custom Columns for the Packet List Pane.....	37
Set Your Global Capture Preferences .....	38
Define Name Resolution Preferences .....	39
Configure Individual Protocol Preferences .....	40
Move Around Quickly: Navigation Techniques .....	41
Find a Packet Based on Various Characteristics.....	42
“Find By” Available Characteristics .....	42
“Search In” Panes .....	42
String Search Options .....	42
Search Direction .....	42
Build Permanent Coloring Rules.....	43
Identify a Coloring Source .....	44
Apply Temporary Coloring.....	45
Mark Packets of Interest.....	46
Follow TCP Streams to Reassemble Data .....	47

### **Section 4: Troubleshooting with Time Values ..... 49**

Examine the Delta Time (End-of-Packet to End-of-Packet).....	51
Set a Time Reference.....	51
Reading Time Values .....	52
Compare Timestamp Values .....	53
Seconds Since Beginning of Capture (default; <code>frame.time_relative</code> ).....	53
Seconds Since Previous Captured Packet ( <code>frame.time_delta</code> ) .....	53
Compare Timestamps of Filtered Traffic .....	54
Seconds Since Previous Displayed Packet ( <code>frame.time_delta_displayed</code> )..	54

Enable and Use TCP Conversation Timestamps .....	55
Compare TCP Conversation Timestamp Values .....	56
Compare TCP Conversation Timestamp Values .....	57
Troubleshooting Example Using Time .....	58
Wire Latency .....	58
Processor Latency .....	58
Analyzing Delay Types .....	59
Detect DNS Delays .....	61
Detect HTTP Delays .....	62

## **Section 5: Create and Interpret Basic and Advanced Trace File Statistics ..... 63**

Examine Trace File Summary Information .....	65
View Active Protocols .....	66
Detect Compromised Hosts .....	66
Filter On or Colorize Protocol Traffic.....	66
Graph Throughput to Spot Performance Problems Quickly .....	67
Graph Specific Traffic with Filters .....	67
Distinguish Traffic with Various Styles .....	67
Locate the Most Active Conversations and Endpoints .....	68
Other Conversation Options .....	68
Graph the Traffic Flows for a More Complete View .....	69
Choose Packets (All or Displayed) .....	70
Choose Flow Type (General or TCP Flow).....	70
Choose Node Address Type (Standard or Network) .....	70
Numerous Other Statistics are Available .....	71
Quick Overview of VoIP Traffic Analysis Tools.....	72
Build Advanced IO Graphs .....	74
SUM(*) Calc .....	75
MIN(), AVG(*) and MAX(*) Calcs .....	76
COUNT FRAMES(*) or COUNT FIELDS(*) Calc.....	77
LOAD() Calc.....	78
Graph Round Trip Times .....	79
Graph TCP Throughput .....	80
Find Problems Using TCP Time-Sequence Graphs .....	81
TCP Plotting Direction.....	82
Identify TCP Window Size Problems .....	82
Identify Duplicate Acknowledgments (Duplicate ACKs).....	83
Identify Selective Acknowledgments (SACKs).....	83
Identify Retransmissions .....	84



**Section 6: Focus on Traffic Using Display Filters .....85**

- Overview of Display Filters ..... 87
- Filter on Conversations/Endpoints ..... 88
- Build Filters Based on Packets ..... 89
  - Apply as Filter (Apply Now)..... 89
  - Prepare a Filter (Manually Apply) ..... 89
  - ... Filter Options ..... 89
- Understand Display Filter Syntax ..... 90
- Use Comparison Operators and Byte-Offset Filters ..... 91
- Filter on Text Strings..... 92
- Regular Expressions 101..... 93
- Build Filters Based on Expressions ..... 94
- Build Filters Expression Buttons ..... 95
- Watch for Common Display Filter Mistakes ..... 96
  - Filter Error Checking ..... 96

**Section 7: TCP/IP Communications and Resolutions Overview ..... 97**

- TCP/IP Functionality Overview ..... 99
- When Everything Goes Right ..... 100
- The Multi-Step Resolution Process ..... 101
  - Port Number Resolution..... 102
  - Name Resolution ..... 102
  - Location Resolution ..... 103
  - Local – MAC Address Resolution ..... 103
  - Remote – Route Resolution ..... 104
  - Remote – MAC Address Resolution for a Gateway ..... 104
- Resolution Helped Build the Packet ..... 105
- Where Can Faults Occur? ..... 106

**Section 8: Analyze DNS Traffic..... 107**

- DNS Overview ..... 109
- DNS Packet Structure..... 110
  - Transaction ID..... 110
  - Flags ..... 111
  - Question Count ..... 112
  - Answer RRs Count ..... 112
  - Authority RRs Count ..... 112
  - Additional RRs Count..... 112

DNS Queries.....	112
Name .....	112
Type .....	112
Class .....	112
Answer RRs .....	112
Authority RRs.....	112
Additional RRs .....	112
Filter on DNS Traffic .....	113

## **Section 9: Analyze ARP Traffic ..... 115**

ARP Overview .....	117
ARP Packet Structure.....	118
Hardware Type .....	118
Protocol Type.....	119
Length of Hardware Address .....	119
Length of Protocol Address.....	119
Opcode .....	119
Sender's Hardware Address .....	119
Sender's Protocol Address .....	119
Target Hardware Address .....	119
Target Protocol Address .....	119
Filter on ARP Traffic .....	120

## **Section 10: Analyze IPv4 Traffic ..... 121**

IPv4 Overview.....	123
IPv4 Packet Structure .....	124
Version Field .....	124
Header Length Field .....	124
Differentiated Services Field and Event Congestion Notification .....	125
Total Length Field .....	125
Identification Field .....	125
Flags Field .....	125
Fragment Offset Field .....	126
Time to Live Field.....	126
Protocol Field .....	127
Header Checksum Field .....	127
Source Address Field.....	127
Destination Address Field .....	127
Options Field.....	128

Analyze Broadcast/Multicast Traffic.....	129
How Many Broadcasts/Multicasts Are Too Many?.....	130
Filter on IPv4 Traffic.....	131
IP Protocol Preferences.....	131

**Section 11: Analyze Internet Control Message Protocol (ICMP) Traffic ..... 133**

ICMP Overview.....	135
ICMP Packet Structure .....	136
Checksum .....	136
Type .....	137
Code .....	138
ICMP Type 3/Code 4 .....	140
Filter on ICMP Traffic.....	141

**Section 12: Analyze User Datagram Protocol (UDP) Traffic ..... 143**

UDP Overview .....	145
Watch for Service Refusals .....	146
UDP Packet Structure.....	147
Source Port Field .....	147
Destination Port Field.....	147
Length Field .....	148
Checksum Field .....	148
Filter on UDP Traffic .....	149
Follow UDP Streams to Reassemble Data.....	150

**Section 13: Analyze Transmission Control Protocol (TCP) Traffic..... 151**

TCP Overview.....	153
The TCP Connection Process .....	154
Watch Service Refusals.....	155
TCP Packet Structure .....	156
Source Port Field .....	156
Destination Port Field.....	156
Sequence Number Field .....	156
Acknowledgment Number Field .....	157
Data Offset Field .....	157
Flags Field .....	157
Window Field .....	158
Checksum Field .....	158

Urgent Pointer Field .....	158
TCP Options Field(s) .....	158
The TCP Sequencing/Acknowledgment Process .....	160
TCP Segmentation Offload (TSO) .....	161
Packet Loss Detection in Wireshark .....	162
Retransmission Detection in Wireshark .....	163
Fast Recovery/Fast Retransmission Detection in Wireshark .....	164
New Spurious Retransmission Detection .....	165
Out-of-Order Segment Detection in Wireshark .....	166
Selective Acknowledgement (SACK) Overview .....	167
TCP Sliding Window Overview .....	168
Window Scaling Overview .....	170
Window Size Issue: Receive Buffer Problem .....	171
Window Size Issue: Unequal Window Size Beliefs .....	172
Troubleshoot TCP Quickly with Expert Info .....	173
TCP Expert Information Details Sample .....	174
Expert Information Classifications .....	175
What Triggers <i>TCP Retransmissions</i> ? .....	175
What Triggers <i>Fast Retransmission</i> ? .....	175
What Triggers <i>Spurious Retransmissions</i> ? .....	175
What Triggers <i>Previous Segment Not Captured</i> ? .....	175
What Triggers <i>ACKed Lost Packet</i> ? .....	175
What Triggers <i>Keep Alive</i> ? .....	176
What Triggers <i>Duplicate ACK</i> ? .....	176
What Triggers <i>Zero Window</i> ? .....	176
What Triggers <i>Zero Window Probe</i> ? .....	176
What Triggers <i>Zero Window Probe ACK</i> ? .....	176
What Triggers <i>Keep Alive ACK</i> ? .....	176
What Triggers <i>Out-of-Order</i> ? .....	177
What Triggers <i>Window Update</i> ? .....	177
What Triggers <i>Window is Full</i> ? .....	177
What Triggers <i>TCP Ports Reused</i> ? .....	177
Filter on TCP Traffic and TCP Problems .....	178
Properly Set TCP Preferences .....	179
Validate the TCP checksum if possible .....	179
Allow subdissector to reassemble TCP streams .....	179
Calculate conversation timestamps .....	179

**Section 14: Analyze DHCP Traffic ..... 181**

DHCP Overview ..... 183

DHCP Packet Structure ..... 184

    Message Type ..... 184

    Hardware Type ..... 184

    Hardware Length ..... 184

    Hops ..... 184

    Transaction ID ..... 184

    Seconds Elapsed ..... 185

    BOOTP Flags ..... 185

    Client IP Address ..... 185

    Your (Client) IP Address ..... 185

    Next Server IP Address ..... 185

    Relay Agent IP Address ..... 185

    Client MAC Address ..... 185

    Server Host Name ..... 185

    Boot File Name ..... 185

    Magic Cookie ..... 185

    Option ..... 186

Filtering on DHCP Traffic ..... 187

Analyze Normal DHCP Traffic ..... 188

Analyze Unusual DHCP Traffic ..... 189

**Section 15: Analyze HTTP and HTTPS Traffic ..... 191**

HTTP Overview ..... 193

HTTP Packet Structure ..... 194

    HTTP Methods ..... 194

Filter on HTTP Traffic ..... 195

Reassembling HTTP Objects ..... 196

HTTP Statistics ..... 197

    Load Distribution ..... 197

    Packet Counter ..... 197

    Requests ..... 198

HTTP Response Time ..... 199

Examine/HTTPS Traffic ..... 200

    Inside the TLS Handshake ..... 201

Encrypted Alerts ..... 202

Decryption Steps ..... 203

Filter on SSL ..... 204

## **Section 16: Analyze POP/SMTP Email Traffic..... 205**

POP Overview .....	207
POP Packet Structure.....	208
POP Request Commands.....	209
POP Response Codes.....	209
Filtering on POP Traffic .....	210
SMTP Overview.....	211
SMTP Packet Structure .....	212
SMTP Commands.....	212
SMTP Response Codes .....	213
Filtering on SMTP Traffic .....	214

## **Section 17: Network Forensics with Wireshark..... 215**

Methodology and Wireshark Use.....	217
Wireshark Essentials for Forensics .....	218
The “Good Traffic” Rule .....	219
Capture Location and Methods.....	220
High Traffic Rates and Intermittent Issues.....	221
Essential Capture Filters.....	222
Offset Capture Filters.....	223
String-Matching Capture Filters .....	225
Network Forensics Profile .....	227
Determine Active Applications and Hosts.....	228
Right-Click Features used in Network Forensics.....	229
Using the Expert to Detect Anomalies .....	230
Exporting Subsets.....	231
GeoIP Mapping.....	233
Carving and Object Reassembly .....	234
Reporting with Comments .....	236
Display Filter Essentials for Forensics.....	237
Conversation Filters.....	238
Compound Filters .....	239
Keyword Filters .....	241
Regular Expression (Regex) Filters.....	242
Turn Filters into Buttons.....	244
Detect Various Scans .....	245
Anomaly Locations .....	246

Password Crack Attempts .....	248
Denial of Service.....	250
Denial of Service Analysis .....	251
Malicious Redirection.....	253
Malicious Redirection Analysis .....	254
<b>Section 18: Command-Line and 3rd Party Tools .....</b>	<b>255</b>
Tshark and Dumpcap Command-Line Tools .....	257
Capinfos Command-Line Tool .....	258
Editcap Command-Line Tool .....	259
Mergecap Command-Line Tool .....	260
Sanitize Trace Files .....	261
Other Tools .....	262

## Course Estimator and Quote Request Form

Ready to train your team on Wireshark, TCP/IP analysis, troubleshooting and network forensics? Complete Part 1 of this Cost Estimator and Quote Request Form to determine the cost of training.

Training is available in three formats:

- **Onsite:** instructor-led, lab-based at your location - customize with your own traffic files
- **Online Live:** instructor-led, lab-based connected via the Internet - customize with your own traffic files
- **On-Demand:** online recorded, available 24x7, 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 Brenda Cardinal ([brenda@chappellU.com](mailto:brenda@chappellU.com)).

### Part 1: Training Project Information (Required for Formal Quotes)

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

Project Title	
Contact Name	
Company	
Phone Number	
Your Email Address	
Company Billing Address for Quote?	
Desired Course Format	Onsite Live Online Live On-Demand (All Access Pass Subscriptions) Other
Course Delivery Timeline	Within 3 months 3-6 months 6+ months I have specific dates in mind (see next item)
Desired Training Dates	
Course Location (if known)	
Number of Students	Up to 20 students 21-30 students 31-40 students 41-50 students Over 50 students (estimated student count:        )
Course Length	Less than 2 days (online training option only) 2 days 3 days 4 days 5 days 6 or more days (estimated course length in days:        )



# CHAPPELLUNIVERSITY

## Course Objectives

Objective #1

Objective #2

Objective #3

Additional Elements to  
include in your training quote  
(optional)

Pre- and post-course quizzes

Discounted All Access Pass Group Subscriptions (online 1-year training subscription)

*Wireshark Network Analysis* book (1 per student)

*Wireshark 101: Essential Skills for Network Analysts* book (1 per student)

*Troubleshooting with Wireshark* book (1 per student)

*Wireshark Certified Network Analyst Exam Prep Guide* (1 per student)

Follow-up Live Online Webinar

*Wireshark Certified Network Analyst Exam* Vouchers

Other

Will you provide trace files  
for further customization  
of the training material?

Yes

No

Unknown

Other Requests or Comments

## Part 2: Design Your Course Content

Please let us know what topics you would like covered in your custom course. Visit [www.chappellu.com/onsite.html](http://www.chappellu.com/onsite.html) for sample course outlines. You may choose to use a sample outline with modifications if desired.

### Section 1

#### Network Analysis Overview

All items in this section  
Troubleshooting Tasks for the Network Analyst  
Security Tasks for the Network Analyst  
Application Analysis Tasks for the Network Analyst  
Security Issues Related to Network Analysis  
Legal Issues Related to Listening to Network Traffic  
Overcome the "Needle in a Haystack" Issue  
Example of a Network Analysis Session from Symptoms to Resolution  
Other

---

### Section 2

#### Wireshark Functionality Overview

All items in this section  
Capturing Packets on Wired or Wireless Networks  
Working with Trace Files from Other Capture Devices - Wiretap Library  
How Wireshark Processes Packets – Drivers, Dissectors, Filters, Plugins  
Wireshark Installation Options, Executable Files and Configuration Files  
Accessing the Wireshark Code and Updates  
Other

---

### Section 3

#### Capture Techniques: Wired/Wireless

All items in this section  
Where to Tap into the Network–Wired/WLAN, Duplex Issues, Switches  
Infrastructure Effects – NAT/PAT, QoS Routing, VLANs, APs  
Options for Remote Capture  
Using File Sets and Optimizing for Large Capture Quantity  
Conserve Memory with Command-line Capture (tshark, dumpcap)  
Using Default and Custom Capture Filters  
Filter by a Protocol, Address or Host Name  
Advanced Capture Filters (Operators and Byte Offset Filtering)  
Work with Multi-Adapter Capture  
Other

---

### Section 4

#### Customize Wireshark: Preferences and Profiles

All items in this section  
Create a Custom Profile and Share Profile Elements  
Set Global and Personal Configurations  
Customize Your User Interface Settings  
Define Your Capture Preferences  
Define IP and MAC Name Resolution  
Options for Network Name Resolution  
Define ARP, TCP, HTTP/HTTPS and Other Protocol Settings  
Use Colors to Distinguish Traffic  
Mark Packets of Interest  
Annotations and Report Generation  
Working with Columns for Efficient Analysis  
Dealing with Applications Running Over Non-Standard Port Numbers  
Using Right-Click Functionality  
Other

---

# CHAPPELLUNIVERSITY

## Section 5 Troubleshoot with Time Values and Summary Information

All items in this section  
Alter the Default Time Column  
Measure Roundtrip Time and Path Latency  
Create Additional Time Columns  
Analyze Application Response Times  
Other

---

## Section 6 Interpret Basic Trace File Statistics to Identify Trends

All items in this section  
Identify Protocols and Applications in Use  
Identify the Most Active Conversations/Endpoints  
List Endpoints and Map Them on the Earth (GeoIP Mapping)  
List Conversations or Endpoints for Specific Traffic Types  
List All UDP and TCP Ports Used  
Graph the Flow of Traffic  
Analyze HTTP Statistics  
Analyze WLAN Statistics  
Other

---

## Section 7 Create and Apply Display Filters for Efficient Analysis

All items in this section  
Create Display Filters Using Auto Complete  
Create and Apply Saved Display Filters  
Filter on a Conversation, Endpoint or Protocol  
Use Expressions for Filters of Lesser-Known Applications  
Combine Display Filters with Comparison Operators  
Alter Display Filter Meaning with Parentheses  
Filter on Specific Bytes in a Packet  
Avoid Common Display Filter Mistakes  
Manually Edit the *dfilters* File  
Add Filter Expression Buttons  
Share Display Filters with Other Wireshark Systems  
Other

---

## Section 8 Follow Streams and Reassemble Data

All items in this section  
Follow and Reassemble UDP Conversations  
Follow and Reassemble TCP Conversations  
Use Reassembly to Identify Undissected Traffic  
Use Reassembly to Extract Files Transferred Across a Network  
Identify Common File Types Based on File Identifiers  
Follow and Reassemble SSL Conversations  
Other

---

## Section 9 TCP/IP Traffic Analysis Overview - Resolutions

All items in this section  
Define Basic TCP/IP Functionality  
Define the Multistep Resolution Process  
Define Port Number Resolution  
Define Network Name Resolution  
Define Route Resolution for a Local Target  
Define Local MAC Address Resolution for a Target  
Define Route Resolution for a Remote Target  
Define Local MAC Address Resolution for a Gateway  
Other

---

# CHAPPELLUNIVERSITY

**Section 10**  
**Analyze Domain Name System (DNS) Traffic**

All items in this section  
Analyze Normal DNS Queries/Responses  
Analyze Unusual DNS Queries/Responses  
Dissect the DNS Packet Structure  
Identifying DNS Faults with Filter Expression Buttons  
Use DNS Packets in the Trace File for Wireshark Name Resolution  
Other

---

**Section 11**  
**Analyze Address Resolution Protocol (ARP) Traffic**

All items in this section  
Analyze Normal ARP Requests/Responses  
Analyze Unusual ARP Requests/Responses  
Analyze Gratuitous ARP  
Dissect the ARP Packet Structure  
Other

---

**Section 12**  
**Analyze Internet Protocol (IPv4) Traffic**

All items in this section  
Analyze Normal IPv4 Traffic  
Analyze Unusual IPv4 Traffic  
Dissect the IPv4 Header Structure  
Set Your IP Protocol Preferences  
Identify Issues Related to Fragmentation and Reassembly  
Identify Black Hole Detection Blocking Issues  
Analyze the Use of Differentiated Services Code Point (DSCP)  
IPv6 Overview and Comparison with IPv4  
Other

---

**Section 13**  
**Analyze Internet Control Messaging Protocol (ICMP) Traffic**

All items in this section  
Analyze Normal ICMP Traffic  
Analyze Unusual ICMP Traffic  
Dissect the ICMP Packet Structure  
Service Refusal Detection – Destination Unreachable  
Black Hole Detection  
ICMP Types and Codes to Catch  
Other

---

**Section 14**  
**Analyze User Datagram Protocol (UDP) Traffic**

All items in this section  
Analyze Normal UDP Traffic  
Analyze Unusual UDP Traffic  
Dissect the UDP Header Structure  
Analyze UDP-based Multicast Video Streams  
Other

---

<b>Section 15</b> <b>Analyze Transmission Control Protocol (TCP) Traffic</b>	All items in this section Access Expert Info Analyze Normal TCP Communications Analyze Unusual TCP Communications (Packet Loss, Congestion, etc.) Define the Establishment of TCP Connections (3-Way and 2-Way Handshakes) Define How TCP-based Services Are Refused TCP Sequential Packet Tracking TCP Selective ACK (SACK) Analysis TCP Window Scaling Analysis TCP Timestamp Analysis (Including PAWS) Define TCP Flow Control (Receiver Congestion, Congestion Window) Analyze the Most Common TCP Problems (See Section 16) Set TCP Protocol Parameters Work with TCP Stream Index Values Graph TCP Streams (Stevens/tcptrace) Other
---	--

---

<b>Section 16</b> <b>Use Wireshark's Expert System to Identify Anomalies</b>	All items in this section Filter on TCP Expert Information Elements Expert Info: tcp_analysis_retransmission Expert Info: tcp_analysis_fast_retransmission Expert Info: tcp_analysis_spurious_retransmission Expert Info: tcp_analysis_out_of_order Expert Info: tcp_analysis_reused_ports Expert Info: tcp_analysis_lost_packet Expert Info: tcp_analysis_ack_lost_packet Expert Info: tcp_analysis_window_update Expert Info: tcp_analysis_window_full Expert Info: tcp_analysis_keep_alive Expert Info: tcp_analysis_keep_alive_ack Expert Info: tcp_analysis_duplicate_ack Expert Info: tcp_analysis_zero_window Expert Info: tcp_analysis_zero_window_probe Expert Info: tcp_analysis_zero_window_probe_ack Interpret Developer Comments in the Wireshark Code Other
---	---

---

<b>Section 17</b> <b>Analyze Dynamic Host Configuration Protocol (DHCP) Traffic</b>	All items in this section Analyze Normal DHCP Traffic Analyze Unusual DHCP Traffic Dissect the DHCP Packet Structure Analyze Relay Agent Use Other
--	---

---

<b>Section 18</b> <b>Analyze Common Hypertext Transfer Protocol (HTTP/HTTPS) Traffic</b>	All items in this section Analyze Normal HTTP Communications Analyze Unusual HTTP Communications Filter on HTTP and HTTPS Traffic Export and Display HTTP Objects (Reassembly) Graph HTTP Traffic Flows Set HTTP Preferences Decrypt HTTPS Traffic Analyze the SSL/TLS Handshake Other
---	---

---

# CHAPPELLUNIVERSITY

## Section 19 Analyze File Transfer Protocol (FTP) Traffic

All items in this section  
Analyze Normal FTP Communications  
Analyze Unusual FTP Communications  
Reassemble FTP Data Transfers  
Colorize FTP Commands  
Other

---

## Section 20 Analyze Email Traffic Patterns

All items in this section  
Analyze Normal Email Communications  
Analyze Unusual Email Communications  
Analyze POP Traffic  
Analyze SMTP Traffic  
Other

---

## Section 21 Graph I/O Rates and TCP Trends

All items in this section  
Generate Basic I/O Graphs (All Traffic/Expert-Flagged Traffic)  
Graph Host and Application Traffic  
Use Calc Functions to Graph Field Sums, Averages, Maximums, Minimums, etc.  
Graph Roundtrip Time and Throughput Rates  
Graph TCP Window Size Issues  
Interpret Packet Loss, Duplicate ACKs and Retransmissions in Graphs  
Other

---

## Section 22 802.11 (WLAN) Analysis Fundamentals

All items in this section  
Analyze Normal 802.11 Communications  
Filter on All WLAN Traffic  
Analyze Frame Control Types and Subtypes  
Analyze Signal Strength and Interference  
Capture WLAN Traffic - Compare Monitor Mode and Promiscuous Mode  
Set up WLAN Decryption  
Prepend a Radiotap or PPI Header  
Compare Signal Strength and Signal-to-Noise Ratios  
Describe 802.11 Traffic Basics  
Other

---

## Section 23 Voice over IP (VoIP) Analysis Fundamentals

All items in this section  
Define VoIP Traffic Flows  
Analyze SIP Call Setup Traffic  
Examine RTP Call Traffic  
Detect if DSCP is Affecting Directional Traffic Flows  
Analyze VoIP Problems and Error Response Codes  
Playback Unencrypted VoIP Calls  
Other

---

## Section 24 Network Forensics Fundamentals

All items in this section  
Methodology and Wireshark Use  
The "Good Traffic" Rule  
Anomaly and Signature Locations  
Capture Location and Methods  
Methods for Avoiding Capture Detection  
Essential Capture Filters  
Offset Capture Filters  
String-Matching Capture Filters  
Building a Network Forensics Profile  
Detect Active Applications and Hosts  
Right-Click Features Used for Network Forensics  
Using the Expert to Detect Anomalies

## Network Forensics Fundamentals (continued)

- Exporting Traffic Subsets from Large Trace Files
- GeoIP Mapping
- Data Carving and Object Reassembly
- Annotating for a Network Forensics Report
- Display Filter Essentials for Network Forensics
- Applying Conversation Filters
- Building and Applying Compound Filters
- Keyword Filtering
- Regular Expression (Regex) Filters for Network Forensics
- Turn Network Forensic Filters into Buttons
- Colorize Unusual Traffic Patterns
- Check out Complementary Forensic Tools
- Other

---

## Section 25 Detect Scanning and Discovery Processes

- All items in this section
- Detect ARP Scans (aka ARP Sweeps)
- Detect ICMP Ping Sweeps
- Detect Various Types of TCP Port Scans
- Detect UDP Port Scans
- Detect IP Protocol Scans
- Define Idle Scans
- Know Your ICMP Types and Codes
- Analyze Traceroute Path Discovery
- Detect Dynamic Router Discovery
- Define Application Mapping Processes
- Use Wireshark for Passive OS Fingerprinting
- Detect Active OS Fingerprinting
- Identify Spoofed Addresses and Scans
- Other

---

## Section 26 Analyze Suspect Traffic

- All items in this section
- Define Suspicious Traffic Types
- Identify Vulnerabilities in the TCP/IP Resolution Processes
- Identify Unacceptable Traffic
- Locate .exe, .zip, .jar Files in Trace Files using Regular Expressions
- Find Maliciously Malformed Packets
- Identify Invalid or Dark Destination Addresses
- Differentiate between Flooding or Standard Denial of Service Traffic
- Find Clear Text Passwords and Data
- Identify Phone-Home Behavior
- Catch Unusual Protocols and Applications
- Detect Applications Using Non-Standard Port Numbers
- Force Dissections on Non-Standard Port Number Traffic
- Locate Route Redirection that Uses ICMP
- Catch ARP Poisoning
- Catch IP Fragmentation and Overwriting
- Spot TCP Splicing
- Watch Other Unusual TCP Traffic
- Identify Password Cracking Attempts
- Other

---

# CHAPPELLUNIVERSITY

## Section 27

### Use Command-Line Tools

All items in this section  
Use Wireshark.exe (Command-Line Launch)  
Capture Traffic with tshark  
Capture Traffic with dumpcap  
List Trace File Details with Capinfos  
Edit Trace Files with Editcap  
Merge Trace Files with Mergecap  
Other

---

### Additional Course Requests

Click **Save** when you have completed this form. Email your form to Brenda Cardinal ([brenda@chappellU.com](mailto:brenda@chappellU.com)) to receive a formal quote after we review your request.

Thank you.

Brenda Cardinal ([brenda@chappellU.com](mailto:brenda@chappellU.com))

**CHAPPELLUNIVERSITY**  
+1 408.378-7841