



Wireshark® Workbook 1

Practice, Challenges, and Solutions

Laura Chappell

Founder, Chappell University™

Creator of the WCNA Certification Program

(formerly referred to as the Wireshark Certified Network Analyst program)

Edited by James Aragon

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

Protocol Analysis Institute, Inc.
59 Damonte Ranch Parkway, #B340
Reno, NV 89521 USA

Chappell University
info@chappellU.com
www.chappellU.com

Copyright Notice

Copyright 2020, Protocol Analysis Institute, Inc., dba Chappell University. All rights reserved. No part of this book, or related materials, may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording, or otherwise) without the prior written permission of the publisher.

To arrange bulk purchase discounts for sales promotions, events, training courses, or other purposes, please contact Chappell University (info@chappellU.com).

ISBN10: 1-893939-63-4

ISBN13: 978-1-893939-64-6

(Version 1.0a)

Distributed worldwide for Chappell University through Protocol Analysis Institute, Inc. Protocol Analysis Institute, Inc. is the educational materials distributor for Chappell University.

For general information on Chappell University or Protocol Analysis Institute, Inc., including information on corporate licenses, updates, future titles, or courses, contact the Protocol Analysis Institute, Inc., at info@chappellu.com.

For authorization to photocopy items for corporate, personal, or educational use, contact Protocol Analysis Institute, Inc., at info@chappellu.com.

Trademarks. All brand names and product names used in this book and related documents are trade names, service marks, trademarks, or registered trademarks of their respective owners. Wireshark and the “fin” logo are registered trademarks of the Wireshark Foundation. At the time this book was written, the Wireshark Foundation, Inc., only had Riverbed senior management as Officers and members of the Board of Directors. I guess Wireshark is owned by Riverbed. Sigh. Shame on you, Riverbed.

Limit of Liability/Disclaimer of Warranty. The author and publisher have used their best efforts in preparing this book and the related materials. Protocol Analysis Institute, Inc., Chappell University, and the author(s) make no representations or warranties of merchantability of fitness for a particular purpose. Protocol Analysis Institute, Inc., and Chappell University assume no liability for any damages caused by following the instructions or using the techniques or tools listed in this book and related materials. 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 the author(s) shall not be liable for any loss of profit or any other damages, including without limitation, special, incidental, consequential, or other damages.

Copy Protection. In all cases, reselling or duplication of this book and related materials without explicit written authorization is expressly forbidden. We will find you, ya know. So don’t steal or plagiarize this book.

About the Author

Laura Chappell has been a protocol analyst for almost 30 years – yes, she has gray hair! Back in the 1990s, Laura became a networking evangelist and member of the IEEE while working at Novell.

Laura is the CEO and Founder of Protocol Analysis Institute, Inc., and Chappell University.

Laura began using Wireshark as her sole network analysis tool when it was in its infancy (under the *Ethereal* name). Laura teaches courses online and onsite and continues to research and write about troubleshooting, optimization, and security techniques for both terrestrial and interplanetary network systems.

Laura's customers include many of the Fortune 100, as well as local, national, and international law enforcement agencies. Visit chappell-university.com for more information on Laura Chappell's projects, join her newsletter and read her blog (*In Laura's Lab*).

Laura's courses are available online at chappell.talentlms.com.

Ms. Chappell can be reached at laura@chappellu.com.

In 2006, with the encouragement of Gerald Combs (creator of Wireshark), Laura founded *Wireshark University* to evangelize network analysis skills and promote a baseline of knowledge with the *Wireshark Certified Network Analyst (WCNA)* program.¹

Laura Chappell remains an adamant supporter of the network analysis developer and user community and the open source Wireshark project.

Is This Book Available as a Training Course?

Yes. You can take this *Wireshark Workbook* as a pre-recorded course online through Laura Chappell's **Wireshark Training All Access Pass** training portal (chappell.talentlms.com).

Wireshark Versions Used in These Labs

This *Wireshark Workbook* was written using several Wireshark 3 versions. If you are still stuck in the world of Wireshark 1.x, it's time to update your version. Wireshark versions 2 and 3 offer numerous advantages over the earlier versions, such as a native installation for Macintosh users, USBpcap support, Intelligent Scrollbar, much better graphs, a Related Packets Indicator, Npcap support, Cisco Remote Capture, and more.

¹ In 2019, Riverbed (the "sponsor" of the Wireshark project) prompted the Wireshark Foundation to take over the "Wireshark University" name in their quest to "monetize Wireshark assets." The certification program is simply referred to as the "WCNA Certification program" because of trademark issues enforced by Riverbed's attorneys. Don't ask her what she thinks of Riverbed, their former employees who pushed to "sell off" the "Wireshark University" name for money, or her thoughts on the secretive workings of the "Wireshark Foundation."

How to Use This Wireshark Workbook 1

This *Wireshark Workbook* contains 16 sets of lab questions with fully-documented solutions to each question. It is designed to test your knowledge of Wireshark and TCP/IP analysis by focusing on your ability to locate answers to network traffic questions.

If you've participated in Laura Chappell's wildly successful Packet Challenge during *SharkFest*, the Wireshark user and developer conferences, then you know what you're in for! The difference, however, is that now you'll be able to see the step-by-step processes used to get the answer to those challenging questions.

Step 1: Lab Preparation

Start with the **Lab Preparation** section on page 1. That will walk you through creating your *Wireshark Workbook 1* profile that is referred to throughout the book.

Step 2: Book Supplements

Next, visit the book supplements page at <https://www.chappell-university.com/books> to download the trace files and blank Answer Sheet document used with this book.²

Step 3: Warm-up Lab

Finally, complete **Lab 1: Wireshark Warm-Up** to get an idea of the type of questions asked and the detail level of the solutions provided.

From that point on, feel free to skip around to different labs as you wish.

Suggested Prerequisite Knowledge to Run these Labs

Before you delve into this *Wireshark Workbook* (or network analysis in general), you should have a solid understanding of basic network concepts and TCP/IP fundamentals. For example, you should know the purpose of a switch, a router, and a firewall. You should be familiar with the concepts of Ethernet networking, basic wireless networking, and be comfortable with IP network addressing, as well.

This *Wireshark Workbook* assumes that you may not know how to use some of Wireshark's features. This is why the workbook will walk you step-by-step through the processes used to get the answers – and, in many cases, show more than one method to get the answers.

² Consider capturing your traffic when you download the book trace files! You will see where we actually keep our book supplements and have a nice file transfer trace for later analysis.

Table of Contents

Copyright Notice	i
About the Author	iii
Is This Book Available as a Training Course?	iii
Wireshark Versions Used in These Labs	iii
How to Use This Wireshark Workbook 1	iv
Suggested Prerequisite Knowledge to Run these Labs.....	iv
Lab Preparation	1
Step 1: Download the Lab trace files and Answer Sheets from www.chappell-university.com/books	1
Step 2: Create your Wireshark Workbook 001 profile	2
Step 3: Check out the online Wireshark Workbook 1 course.....	2
Lab 1: Wireshark Warm-Up.....	3
Objective: Get Comfortable with the Lab Process.	3
Skills Covered in this Lab	3
Lab 1 Solutions.....	9
Lab 2: Proxy Problem	35
Objective: Examine issues that relate to a web proxy connection problem.	35
Skills Covered in this Lab	35
Lab 2 Solutions.....	39
Lab 3: HTTP vs. HTTPS	51
Objective: Analyze and compare HTTP and HTTPS communications and errors using inclusion and field existence filters.....	51
Skills Covered in this Lab	51
Lab 3 Solutions.....	55

Lab 4: TCP SYN Analysis	67
Objective: Filter on and analyze TCP SYN and SYN/ACK packets to determine the capabilities of TCP peers and their connections.	67
Skills Covered in this Lab	67
Lab 4 Solutions	71
Lab 5: TCP SEQ/ACK Analysis	95
Objective: Examine and analyze TCP sequence and acknowledgment numbering and Wireshark's interpretation of non-sequential numbering patterns.	95
Skills Covered in this Lab	95
Lab 5 Solutions	99
Lab 6: You're Out of Order!.....	121
Objective: Examine Wireshark's process of distinguishing between out-of-order packets and retransmissions and identify mis-identifications.	121
Skills Covered in this Lab	121
Lab 6 Solutions	125
Quick Test 1	127
Quick Test 2	147
Quick Test 1 Answers.....	152
Quick Test 2 Answers.....	152
Lab 7: Sky High.....	153
Objective: Examine and analyze traffic captured as a host was redirected to a malicious site.	153
Skills Covered in this Lab	153
Lab 7 Solutions	157

Lab 8: DNS Warm-Up	183
Objective: Examine and analyze DNS name resolution traffic that contains canonical name and multiple IP address responses.	183
Skills Covered in this Lab	183
Lab 8 Solutions.....	187
Lab 9: Hacker Watch	199
Objective: Analyze TCP connections and FTP command and data channels between hosts.	199
Skills Covered in this Lab	199
Lab 9 Solutions.....	203
Lab 10: Timing is Everything.....	215
Objective: Analyze and compare path latency, name resolution, and server response times.....	215
Skills Covered in this Lab	215
Lab 10 Solutions.....	219
Lab 11: The News.....	233
Objective: Analyze capture location, path latency, response times, and keep-alive intervals between an HTTP client and server.....	233
Skills Covered in this Lab	233
Lab 11 Solutions.....	237
Lab 12: Selective ACKs	251
Objective: Analyze the process of establishing Selective acknowledgment (SACK) and using SACK during packet loss recovery.	251
Skills Covered in this Lab	251
Lab 12 Solutions.....	255

Lab 13: Just DNS.....	277
Objective: Analyze, compare, and contrast various DNS queries and responses to identify errors, cache times, and CNAME (alias) information.....	277
Skills Covered in this Lab	277
Lab 13 Solutions	281
Lab 14: Movie Time.....	297
Objective: Use various display filter types, including regular expressions (regex), to analyze HTTP redirections, end-of-field values, object download times, errors, response times and more.	297
Skills Covered in this Lab	297
Lab 14 Solutions	301
Lab 15: Crafty.....	319
Objective: Practice your display filter skills using “contains” operators, ASCII filters, and inclusion/exclusion filters, while analyzing TCP and HTTP performance parameters.	319
Skills Covered in this Lab	319
Lab 15 Solutions	323
Lab 16: Pattern Recognition.....	337
Objective: Focus on TCP conversations and endpoints while analyzing TCP sequence numbers, Window Scaling, keep-alive, and Selective Acknowledgment capabilities.	337
Skills Covered in this Lab	337
Lab 16 Solutions	339
Index	345

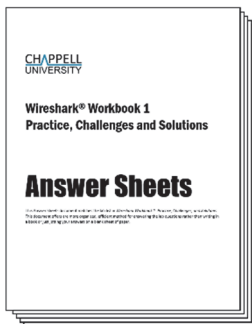
Lab Preparation

Hello fellow Wireshark and packet analyst enthusiasts!

If you've ever joined me at *SharkFest*, the Wireshark user and developer conference, you've likely seen and hopefully participated in my Packet Challenge. I began the packet challenge many, many years ago as a contest at the conference. The shark fin awards would be presented on the last day of the conference to the contestants who were the closest to 100% correct on their answer sheets.

This book is based on my Packet Challenges, but I've included lots of detail on how I got the answers. There are often many ways to get the answers, so you might find alternatives – as long as we get the same answer, that's ok!

Step 1: Download the Lab trace files and Answer Sheets from www.chappell-university.com/books



The *Answer Sheets* document does not contain the answers. The *Answer Sheets* document offers an organized, efficient method for answering the lab questions rather than writing in a book or just jotting your answers on a blank sheet of paper.

Download the *Answer Sheets* document and the set of *Wireshark Workbook 1* trace files from www.chappell-university.com/books.



*I recommend that you write your answer **and** make a note of how you got that answer. Did you add a specific column? Did you use a certain display filter? Did you look at one of the statistics windows? When you look at the answers, you will see how I got the answer and you can compare your method to mine. Quite often there is more than one way to get an answer.*

2 Lab Preparation

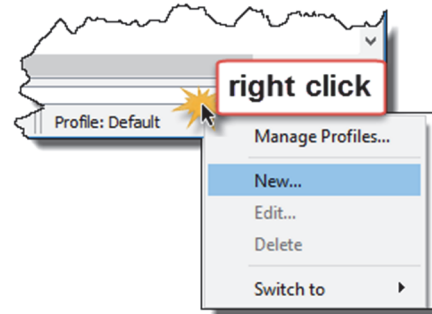
Step 2: Create your Wireshark Workbook 001 profile

In Wireshark, profiles enable you to customize Wireshark columns, dissector preference settings, display filter buttons, and more.

Right-click on the *Profile* column on the Status Bar and select *New*.

Name your new profile *Wireshark Workbook 001* and click *OK*.

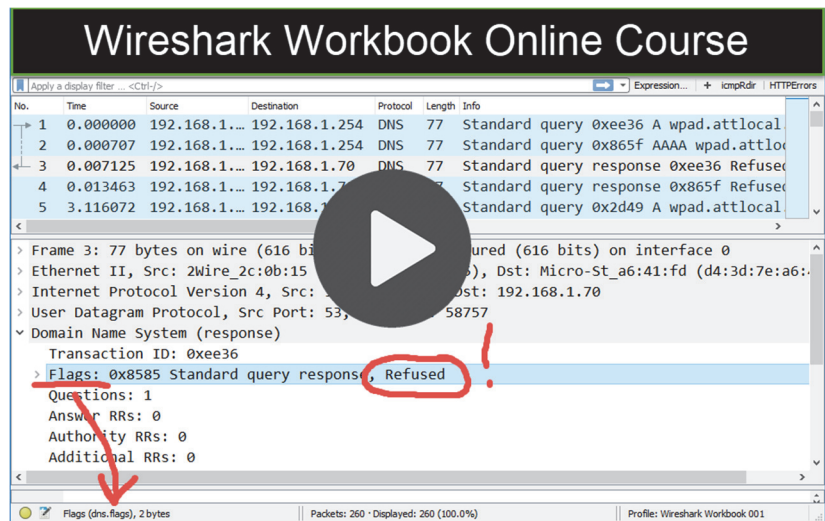
That's it! Now you have created a new profile that can be used as you work through the labs in this book.



Step 3: Check out the online Wireshark Workbook 1 course

If you are already a **Wireshark Training All Access Pass** member, you can take the **Wireshark Workbook 1** course set to watch how the labs are solved. You can skip around to different lab solutions as desired.

Visit chappell-university.com for more information on online and onsite training courses.



Ok! Once you have the trace files, *Answer Sheet*, and your *Wireshark Workbook 001* profile, you are ready to go! Fire up Wireshark and let's get started!