

# Wireshark<sup>®</sup> Network Analysis

The Official Wireshark Certified Network Analyst Study Guide

## Second Edition

Laura Chappell

- Learn **insider tips and tricks** to spot the cause of lousy network performance
- Discover **basic through advanced Wireshark techniques** to quickly identify evidence of discovery processes and breached hosts
- Analyze real world case studies to see how network problems have been solved by IT professionals just like **YOU!**



Foreword by  
**Gerald Combs**  
Creator of Wireshark



**Wireshark® Network Analysis**  
**The Official Wireshark Certified Network Analyst™ Study Guide**  
**2<sup>nd</sup> Edition (Version 2.1b)**

Laura Chappell  
Founder, Chappell University™  
Founder, Wireshark University™



Readers interested in this book may also be interested in the associated **Wireshark Certified Network Analyst Official Exam Prep Guide – Second Edition.**

**10-digit ISBN:** 1-893939-90-1  
**13-digit ISBN:** 978-1-893939-90-5



**Wireshark® Network Analysis**  
**The Official Wireshark Certified Network Analyst™ Study Guide**  
**2<sup>nd</sup> Edition (Version 2.1b)**

Copyright 2012, Protocol Analysis Institute, Inc, dba Chappell University. All rights reserved. No pa

of this ebook, or related materials, including interior design, cover design and contents of the referenced book website, [www.wiresharkbook.com](http://www.wiresharkbook.com), 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 at the address listed on the next page.

**Book URL:** [www.wiresharkbook.com](http://www.wiresharkbook.com)

**Paperback Book 13-digit ISBN:** 978-1-893939-94-3

**Paperback Book 10-digit ISBN:** 1-893939-94-4

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 the 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 email to [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. Wireshark and the "fin" logo are registered trademarks of the Wireshark Foundation. Protocol Analysis Institute, Inc is the exclusive developer for Chappell University.

**Limit of Liability/Disclaimer of Warranty.** The author and publisher have used their best efforts in preparing this book and the related materials used in this book. 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 book or related materials used in this book. 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.

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

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

This book and the book website, [www.wiresharkbook.com](http://www.wiresharkbook.com), references Chanalyzer Pro software created by MetaGeek ([www.metageek.net/wiresharkbook](http://www.metageek.net/wiresharkbook)).

This book and the book website, [www.wiresharkbook.com](http://www.wiresharkbook.com), references GeoLite data created by

MaxMind, available from [www.maxmind.com](http://www.maxmind.com).

PhoneFactor™ SSL/TLS vulnerabilities documents and trace files referenced on the book website, [www.wiresharkbook.com](http://www.wiresharkbook.com), were created by Steve Dispensa and Ray Marsh ([www.phonefactor.com](http://www.phonefactor.com)).

This book and the book website, [www.wiresharkbook.com](http://www.wiresharkbook.com), references trace files from Mu Dynamics ([www.pcapr.net](http://www.pcapr.net)).

This book references rules released by Emerging Threats Copyright © 2003-2012, Emerging Threats. All rights reserved. For more information, visit [emergingthreats.net](http://emergingthreats.net).

Protocol Analysis Institute, Inc.

5339 Prospect Road, # 343

San Jose, CA 95129 USA

[www.wiresharkbook.com](http://www.wiresharkbook.com)

Also refer to Chappell University at the same address

[info@chappellU.com](mailto:info@chappellU.com)

[www.chappellU.com](http://www.chappellU.com)

Cover: Fractal image, *Waves Envisioned during Late Nights at Work*, by Scott Spicer

Created with Apophysis 2.09

## Dedication

This Second Edition is dedicated to Gerald Combs, creator of Wireshark (formerly Ethereal) and a good friend.

Twelve years ago, I sent Gerald a note—just out of the blue—"may I include Ethereal on my CD? I want to give it away at conferences." Expecting some pushback—after all, he didn't know who the heck I was—I was amazed and thrilled to receive his response stating "sure, go ahead—that would be great!"

Gerald is more than the creator of Wireshark. Gerald is one of us. He struggled with a problem. He formulated a solution. Then he did something extraordinary—he shared his solution with the world. In his typical unselfish mode, Gerald opened up his project for the contribution and participation of others.

Ethereal morphed into Wireshark, and Wireshark continued to mature. Wireshark has surpassed every other network analyzer product in the industry to become the de facto standard for network traffic analysis.

In 2011 Wireshark was voted the #1 Security Tool on the [SecTools.org](http://SecTools.org) Top 125 Network Security Tools survey (conducted by Gordon Lyons, creator of Nmap). This is a much deserved recognition that Wireshark and packet analysis is a must-have skill for IT security professionals.

Throughout Wireshark's rise in popularity, Gerald has remained one of the most honest, humble, dedicated professionals in our field.

Callan

---

Thank you Gerald.

p.s. Again I want to express very special thanks to Gerald's wife, Karen, and their absolutely cute-beyond-belief, I-have-my-Daddy-wrapped-around-my-little-finger, smarty-pants-who-melts-your-heart daughter! Gerald always beams when he talks about you two very special ladies and it is a treat spending time with you both <girl power!>. I am grateful for the love, support and inspiration you have provided Gerald. Your tremendous humor and joie de vivre inspires me!

# ACKs

---

There are many people who were directly and indirectly involved in creating the First and Second Editions of this book.

First and foremost, I would like to thank my children, **Scott and Ginny**, for your patience, support and humor during the many hours I was huddled over my computer to complete this book. Your words of encouragement really helped me balance work and life during some long days and nights of deadline. It will be a treat to write that "Cooking Badly" book with you someday!

**Mom, Dad, Steve and Joe**—ahh... yes, the "fam." You guys have given me so much humorous material for my presentations! Can't wait for "take your daughter to work day," Mom!

Special thanks to **Brenda Cardinal and Jill Poulsen** who have worked with me for over 10 years each—you masochists! I am fortunate to have both of you around to brighten my days and put life in perspective.

To **Colton Cardinal**, who provided humorous distractions, smiles and, giggles—thanks for all the time staring at the clocks during the past year and a half. I feel very fortunate to have the chance to watch you grow up!

**Joy DeManty**—I'm sure you're sick of reading this book over and over and over again! I appreciate your keen eye in reviewing this second edition. Let's agree on this - no more 1,000 page books!

**Lanell Allen**—again you really pulled through for us on this project! Your tireless hours of work put into finding my typos, half-sentences and dangling prepositions (he he) was invaluable. Thank you for taking on this project.

**Gerald Combs**—what can I say? You have selflessly shared with us a tremendous tool and I am so very grateful for your devotion to Wireshark. The first and second editions of this book are dedicated to you.

**The Wireshark developers**—what a group! It has been a pleasure meeting so many of you in person at the Sharkfest conferences. Your continued efforts to improve and enhance Wireshark have helped so many IT professionals find the root of network issues. Thank you for the many hours you have dedicated to making Wireshark the world's most popular network analyzer solution! You can find the developer list at **Help | About Wireshark | Authors**. I hope this book accurately explains the features you have spent so many hours implementing. If I missed anything you'd like included in future editions of this book, please let me know.

**Gordon "Fyodor" Lyon**—the creation of the First Edition of this book was triggered when you released "Nmap Network Scanning"—an excellent book that every networking person should own. I appreciate your time and effort looking over the network scanning section. I look forward to working with you on some future projects—there are so many possibilities!

**Ryan Woodings and Mark Jensen of MetaGeek**—it has been a pleasure collaborating with you folks on ideas and microwave popping methods (g)! It has been a blast showing Wi-Spy/Chanalyzer Pro at conferences and sharing these hot products with the IT community. I look forward to more brainstorming sessions. Special thanks to **Trent Cutler** for reviewing the WLAN chapter and sending on some great feedback.

**Steve Dispensa and Marsh Ray of PhoneFactor** ([www.phonefactor.com](http://www.phonefactor.com))—thank you both for kindly allowing me to include your *Renegotiating TLS* document and trace files at [www.wiresharkbook.com](http://www.wiresharkbook.com). You two did a great job documenting this security issue and your work benefits us all.

**Stig Bjørlykke, Wireshark Core Developer**—you came up with so many great additions to the First Edition of this book and recent versions of Wireshark! Your understanding of the inner workings of Wireshark as well as the areas that often perplex people helped make this book much more valuable to the readers. We all appreciate your development efforts to make Wireshark such a valuable tool!

**Sean Walberg**—Thanks for being such a great resource on the VoIP chapter. You really have such a wonderful talent explaining the inner workings of VoIP communications. I loved your presentation at Sharkfest—funny and geeky at the same time! I appreciate your efforts to clarify the VoIP chapter in this book.

**Martin Mathieson, Wireshark Core Developer**—I am so grateful for the fixes and tips you provided for the VoIP chapter and the time you took to explain the duplicate IP address detection feature you added to Wireshark. I appreciate you providing the RFC references to be included and understanding that the readers may be new to VoIP analysis. The time and energy you have put into enhancing Wireshark are a benefit to us all!

**Jim Aragon**—Thanks so much for your tremendous feedback on the First Edition of this book and providing the tip on capturing traffic. It's always great to read your ideas and suggestions and you've given me loads of ideas for future tips and training.

**Sake Blok, Wireshark Core Developer**—Don't you ever sleep? <g> Thanks for your feedback and corrections on the First Edition of this book. It's great having your case study, *The Tale of the Missing ARP* (in *Chapter 16: Analyze Address Resolution Protocol (ARP) Traffic*). I really appreciate the changes you made to Wireshark regarding the "field not in use, but existent" issue. Yippie!

**Ron Nutter**—Hey, buddy! Hard to believe we've known each other for a zillion years, eh? Thanks for adding the Cisco spanning instructions in this Second Edition. I know the readers will appreciate that you shared your tips for setting up an efficient capture with Cisco equipment.

**Jeff Carrell**—You jumped right in to clean up my messy draft of IPv6 introductory materials. You did a great job refocusing me to 'show them the packets.' No wonder people love your IPv6 classes! Thank so much for helping out over the holidays. I know you were working away on the "Guide to TCP/IP" book and your time is precious these days.

**Betty DuBois**—Thanks for all your review time and talent—not only on this book project, but also on the Wireshark University Instructor-Led courses and the WCNA Exam. It's always great to talk/work with a fellow packet-geekess!

**Keith Parsons**—Thanks for clarifying the concepts in the WLAN chapter and adding the awesome "To DS/From DS" graphic and table! You always have great ideas and teaching methods—and you're truly the "geek toy king" as well!

**Anders Broman, Wireshark Core Developer**—Thanks for taking the time to look through the VoIP chapter and ensure the information was accurate and presented clearly. Thank you so much for all your efforts as a Wireshark core developer and making so many of the changes I've whined about.

**The pcapr Team**—I appreciate you allowing me to provide readers with several trace files from your online repository at [www.pcapr.net](http://www.pcapr.net). Thank you to **Mu Dynamics** ([www.mudynamics.com](http://www.mudynamics.com)) for supporting the *pcapr.net* project.

**David Teng**—Thanks for your thorough read through of the first edition and the numerous edits and suggestions you provided. It is difficult to imagine the effort you put into translating this huge book from Chinese, but I do hope to see it in print someday.

**My Students**—Sincere thanks to the **hundreds of thousands of students** who have taken my online training courses, instructor-led courses and self-paced courses over 20 years of teaching. I've gotten to know so many of you as friends. Your honest and direct feedback has always helped me hone my training materials (and my jokes).

**Gary Lewis**—you wild guy, you! If anyone out there needs graphic design services, Gary is the "go to" guy with a great (and somewhat twisted) sense of humor. Thanks for a great cover design on the First Edition—and a lovely rework of the Second Edition!

**Case Study/Tip Submitters**—Case studies were submitted from all around the world. Thanks to all you who overloaded my email with your Wireshark success stories. The following individuals provided case studies that were included in this book to offer a glimpse into how folks use Wireshark to save time and money.

LabNuke99 - P.C. - Jim Aragon - Roy B. - Martin B. - Bill Back - Sake Blok - Jeff Carrell - Coleen D  
- Todd DeBoard and Team - Mitch Dickey - Thanassis Diogos - Steve Dispensa - Todd Dokey - Vik  
Evans - Russ F. - Allen Gittelsohn - Richard Hicks - Rob Hulsebos - Mark Jensen - Jennifer Keels -  
Christian Kreide - Todd Lerdal - Robert M. - Jim McMahon - Ron Nutter - Karl R. - Mark R. - Guy  
Talbot - Delfino L. Tiongco - Sean Walberg - Christy Z.

**And of course**—Finally, I'd like to thank those folks who create lousy applications, cruddy TCP/IP stacks, scummy operating systems, pathetic interconnecting devices and sad default configurations and the users who bring their muck onto the network—you make life so interesting!

If I've missed anyone in this ACK section, I apologize and plead brain-drain at this point!



# Contents at a Glance

---

[Chapter 1: The World of Network Analysis](#)

[Chapter 2: Introduction to Wireshark](#)

[Chapter 3: Capture Traffic](#)

[Chapter 4: Create and Apply Capture Filters](#)

[Chapter 5: Define Global and Personal Preferences](#)

[Chapter 6: Colorize Traffic](#)

[Chapter 7: Define Time Values and Interpret Summaries](#)

[Chapter 8: Interpret Basic Trace File Statistics](#)

[Chapter 9: Create and Apply Display Filters](#)

[Chapter 10: Follow Streams and Reassemble Data](#)

[Chapter 11: Customize Wireshark Profiles](#)

[Chapter 12: Annotate, Save, Export and Print Packets](#)

[Chapter 13: Use Wireshark's Expert System](#)

[Chapter 14: TCP/IP Analysis Overview](#)

[Chapter 15: Analyze Domain Name System \(DNS\) Traffic](#)

[Chapter 16: Analyze Address Resolution Protocol \(ARP\) Traffic](#)

[Chapter 17: Analyze Internet Protocol \(IPv4/IPv6\) Traffic](#)

[Chapter 18: Analyze Internet Control Message Protocol \(ICMPv4/ICMPV6\) Traffic](#)

[Chapter 19: Analyze User Datagram Protocol \(UDP\) Traffic](#)

[Chapter 20: Analyze Transmission Control Protocol \(TCP\) Traffic](#)

[Chapter 21: Graph IO Rates and TCP Trends](#)

[Chapter 22: Analyze Dynamic Host Configuration Protocol \(DHCPv4/DHCPv6\) Traffic](#)

[Chapter 23: Analyze Hypertext Transfer Protocol \(HTTP\) Traffic](#)

[Chapter 24: Analyze File Transfer Protocol \(FTP\) Traffic](#)

[Chapter 25: Analyze Email Traffic](#)

[Chapter 26: Introduction to 802.11 \(WLAN\) Analysis](#)

[Chapter 27: Introduction to Voice over IP \(VoIP\) Analysis](#)

[Chapter 28: Baseline "Normal" Traffic Patterns](#)

[Chapter 29: Find the Top Causes of Performance Problems](#)

[Chapter 30: Network Forensics Overview](#)

[Chapter 31: Detect Network Scanning and Discovery Processes](#)

[Chapter 32: Analyze Suspect Traffic](#)

[Chapter 33: Effective Use of Command Line Tools](#)

[Appendix A: Resources on the Book Website](#)

[All Access Pass Training Offer](#)

# Table of Contents

---

[Contents at a Glance](#)

[List of Tips](#)

[Wireshark Certified Network Analyst Exam Topics](#)

[\\$100 Off All Access Pass \(AAP\) Online Training](#)

[Dedication](#)

[ACKs](#)

[Foreword by Gerald Combs](#)

[Preface](#)

[About This Book](#)

[Wireshark Certified Network Analyst™ Program Overview](#)

[Wireshark University™ and Wireshark University™ Training Partners](#)

[Schedule Customized Onsite/Web-Based Training](#)

# **Chapter 1: The World of Network Analysis**

---

[Define Network Analysis](#)

[Follow an Analysis Example](#)

[Walk-Through of a Troubleshooting Session](#)

[Walk-Through of a Typical Security Scenario \(aka Network Forensics\)](#)

[Understand Security Issues Related to Network Analysis](#)

[Overcome the "Needle in the Haystack Issue](#)

[Review a Checklist of Analysis Tasks](#)

[Understand Network Traffic Flows](#)

[Launch an Analysis Session](#)

[Case Study: Pruning the "Puke"](#)

[Case Study: The "Securely Invisible" Network](#)

[Summary](#)

[Practice What You've Learned](#)

[Review Questions](#)

[Answers to Review Questions](#)

## **Chapter 2: Introduction to Wireshark**

---

[Wireshark Creation and Maintenance](#)

[Capture Packets on Wired or Wireless Networks](#)

[Open Various Trace File Types](#)

[Understand How Wireshark Processes Packets](#)

[Use the Start Page](#)

[Identify the Nine GUI Elements](#)

[Navigate Wireshark's Main Menu](#)

[Use the Main Toolbar for Efficiency](#)

[Focus Faster with the Filter Toolbar](#)

[Make the Wireless Toolbar Visible](#)

[Work Faster Using RightClick Functionality](#)

[Sign Up for the Wireshark Mailing Lists](#)

[Join ask.wireshark.org!](#)

[Know Your Key Resources](#)

[Get Some Trace Files](#)

[Case Study: Detecting Database Death](#)

[Summary](#)

[Practice What You've Learned](#)

[Review Questions](#)

[Answers to Review Questions](#)

## **Chapter 3: Capture Traffic**

---

[Know Where to Tap Into the Network](#)

[Run Wireshark Locally](#)

[Capture Traffic on Switched Networks](#)

[Analyze Routed Networks](#)

[Analyze Wireless Networks](#)

[Capture at Two Locations \(Dual Captures\)](#)

[Select the Right Capture Interface](#)

[Capture on Multiple Adapters Simultaneously](#)

[Interface Details \(Windows Only\)](#)

[Capture Traffic Remotely](#)

[Automatically Save Packets to One or More Files](#)

[Optimize Wireshark to Avoid Dropping Packets](#)

[Conserve Memory with Command-Line Capture](#)

[Case Study: Dual Capture Points the Finger](#)

[Case Study: Capturing Traffic at Home](#)

[Summary](#)

[Practice What You've Learned](#)

[Review Questions](#)

[Answers to Review Questions](#)

# **Chapter 4: Create and Apply Capture Filters**

---

[The Purpose of Capture Filters](#)

[Apply a Capture Filter to an Interface](#)

[Build Your Own Set of Capture Filters](#)

[Filter by a Protocol](#)

[Filter Incoming Connection Attempts](#)

[Create MAC/IP Address or Host Name Capture Filters](#)

[Capture One Application's Traffic Only](#)

[Use Operators to Combine Capture Filters](#)

[Create Capture Filters to Look for Byte Values](#)

[Manually Edit the Capture Filters File](#)

[Share Capture Filters with Others](#)

[Case Study: Kerberos UDP to TCP Issue](#)

[Summary](#)

[Practice What You've Learned](#)

[Review Questions](#)

[Answers to Review Questions](#)

# **Chapter 5: Define Global and Personal Preferences**

---

[Find Your Configuration Folders](#)

[Set Global and Personal Configurations](#)

[Customize Your User Interface Settings](#)

[Define Your Capture Preferences](#)

[Automatically Resolve IP and MAC Names](#)

[Plot IP Addresses on a World Map with GeoIP](#)

[Resolve Port Numbers \(Transport Name Resolution\)](#)

[Resolve SNMP Information](#)

[Configure Filter Expressions](#)

[Configure Statistics Settings](#)

[Define ARP, TCP, HTTP/HTTPS and Other Protocol Settings](#)

[Configure Protocol Settings with RightClick](#)

[Case Study: NonStandard Web Server Setup](#)

[Summary](#)

[Practice What You've Learned](#)

[Review Questions](#)

[Answers to Review Questions](#)

## **Chapter 6: Colorize Traffic**

---

[Use Colors to Differentiate Traffic Types](#)

[Disable One or More Coloring Rules](#)

[Share and Manage Coloring Rules](#)

[Identify Why a Packet is a Certain Color](#)

[Create a "Butt Ugly" Coloring Rule for HTTP Errors](#)

[Color Conversations to Distinguish Them](#)

[Temporarily Mark Packets of Interest](#)

[Alter Stream Reassembly Coloring](#)

[Case Study: Colorizing SharePoint Connections During Login](#)

[Summary](#)

[Practice What You've Learned](#)

[Review Questions](#)

[Answers to Review Questions](#)



## **Chapter 7: Define Time Values and Interpret Summaries**

---

[Use Time to Identify Network Problems](#)

[Send Trace Files Across Time Zones](#)

[Identify Delays with Time Values](#)

[Identify Client, Server and Path Delays](#)

[View a Summary of Traffic Rates, Packet Sizes and Overall Bytes Transferred](#)

[Case Study: Time Column Spots Delayed ACKs](#)

[Summary](#)

[Practice What You've Learned](#)

[Review Questions](#)

[Answers to Review Questions](#)

# **Chapter 8: Interpret Basic Trace File Statistics**

---

[Launch Wireshark Statistics](#)

[Identify Network Protocols and Applications](#)

[Protocol Settings Can Affect Your Results](#)

[Identify the Most Active Conversations](#)

[List Endpoints and Map Them on the Earth](#)

[Spot Suspicious Targets with GeoIP](#)

[List Conversations or Endpoints for Specific Traffic Types](#)

[Evaluate Packet Lengths](#)

[List All IPv4/IPv6 Addresses in the Traffic](#)

[List All Destinations in the Traffic](#)

[List UDP and TCP Usage](#)

[Analyze UDP Multicast Streams](#)

[Graph the Flow of Traffic](#)

[Gather Your HTTP Statistics](#)

[Examine All WLAN Statistics](#)

[Case Study: Application Analysis: Aptimize Website Accelerator™](#)

[Case Study: Finding VoIP Quality Issues](#)

[Summary](#)

[Practice What You've Learned](#)

[Review Questions](#)

[Answers to Review Questions](#)

# **Chapter 9: Create and Apply Display Filters**

---

[Understand the Purpose of Display Filters](#)

[Create Display Filters Using Auto-Complete](#)

[Apply Saved Display Filters](#)

[Use Expressions for Filter Assistance](#)

[Make Display Filters Quickly Using RightClick Filtering](#)

[Filter on Conversations and Endpoints](#)

[Filter on the Protocol Hierarchy Window](#)

[Understand Display Filter Syntax](#)

[Combine Display Filters with Comparison Operators](#)

[Alter Display Filter Meaning with Parentheses](#)

[Filter on the Existence of a Field](#)

[Filter on Specific Bytes in a Packet](#)

[Find Key Words in Upper or Lower Case](#)

[More Interesting Regex Filters](#)

[Let Wireshark Catch Display Filter Mistakes](#)

[Use Display Filter Macros for Complex Filtering](#)

[Avoid Common Display Filter Mistakes](#)

[Manually Edit the \*dfilters\* File](#)

[Case Study: Using Filters and Graphs to Solve Database Issues](#)

[Case Study: The Chatty Browser](#)

[Case Study: Catching Viruses and Worms](#)

[Summary](#)

[Practice What You've Learned](#)

[Review Questions](#)

[Answers to Review Questions](#)

# **Chapter 10: Follow Streams and Reassemble Data**

---

[The Basics of Traffic Reassembly](#)

[Follow and Reassemble UDP Conversations](#)

[Follow and Reassemble TCP Conversations](#)

[Follow and Reassemble SSL Conversations](#)

[Reassemble an SMB Transfer](#)

[Case Study: Unknown Hosts Identified](#)

[Summary](#)

[Practice What You've Learned](#)

[Review Questions](#)

[Answers to Review Questions](#)

# **Chapter 11: Customize Wireshark Profiles**

---

[Customize Wireshark with Profiles](#)

[Case Study: Customizing Wireshark for the Customer](#)

[Summary](#)

[Practice What You've Learned](#)

[Review Questions](#)

[Answers to Review Questions](#)

# **Chapter 12: Annotate, Save, Export and Print Packets**

---

[Annotate a Packet or an Entire Trace File](#)

[Save Filtered, Marked and Ranges of Packets](#)

[Export Packet Content for Use in Other Programs](#)

[Export SSL Keys](#)

[Save Conversations, Endpoints, IO Graphs and Flow Graph Information](#)

[Export Packet Bytes](#)

[Case Study: Saving Subsets of Traffic to Isolate Problems](#)

[Summary](#)

[Practice What You've Learned](#)

[Review Questions](#)

[Answers to Review Questions](#)

# **Chapter 13: Use Wireshark's Expert System**

---

[Let Wireshark's Expert Information Guide You](#)

[Understand TCP Expert Information](#)

[Case Study: Expert Info Catches Remote Access Headaches](#)

[Summary](#)

[Practice What You've Learned](#)

[Review Questions](#)

[Answers to Review Questions](#)

# **Chapter 14: TCP/IP Analysis Overview**

---

[TCP/IP Functionality Overview](#)

[Build the Packet](#)

[Case Study: Absolving the Network from Blame](#)

[Summary](#)

[Practice What You've Learned](#)

[Review Questions](#)

[Answers to Review Questions](#)



---

sample content of Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide

- [download online Twilight of the Dead \(Fiends of the Eastern Front, Book 3\) pdf, azw \(kindle\), epub](#)
- [read Happily Ever After: Six Secrets to a Successful Marriage \(Chapman Guides\) here](#)
- [read Llewellyn's Complete Book of Predictive Astrology: The Easy Way to Predict Your Future online](#)
- [download online The Shadow of a Great Rock: A Literary Appreciation of the King James Bible online](#)
- [read \*Yellow Elephant: Improve Your Memory and Learn More, Faster, Better\*](#)
- [Knives at Dawn for free](#)
  
- <http://bestarthritiscare.com/library/The-Ultimate-Dividend-Playbook--Income--Insight-and-Independence-for-Today-s-Investor.pdf>
- <http://dadhoc.com/lib/Happily-Ever-After--Six-Secrets-to-a-Successful-Marriage--Chapman-Guides-.pdf>
- <http://ramazotti.ru/library/Llewellyn-s-Complete-Book-of-Predictive-Astrology--The-Easy-Way-to-Predict-Your-Future.pdf>
- <http://berttrotman.com/library/The-Titanic-Sinks-.pdf>
- <http://academialanguagebar.com/?ebooks/The-Wizard-of-Oz---2nd-Edition---BFI-Film-Classics-.pdf>
- <http://fortune-touko.com/library/Faces-of-Compassion--Classic-Bodhisattva-Archetypes-and-Their-Modern-Expression---An-Introduction-to-Mahayana-B>