Wireshark® Network Analysis

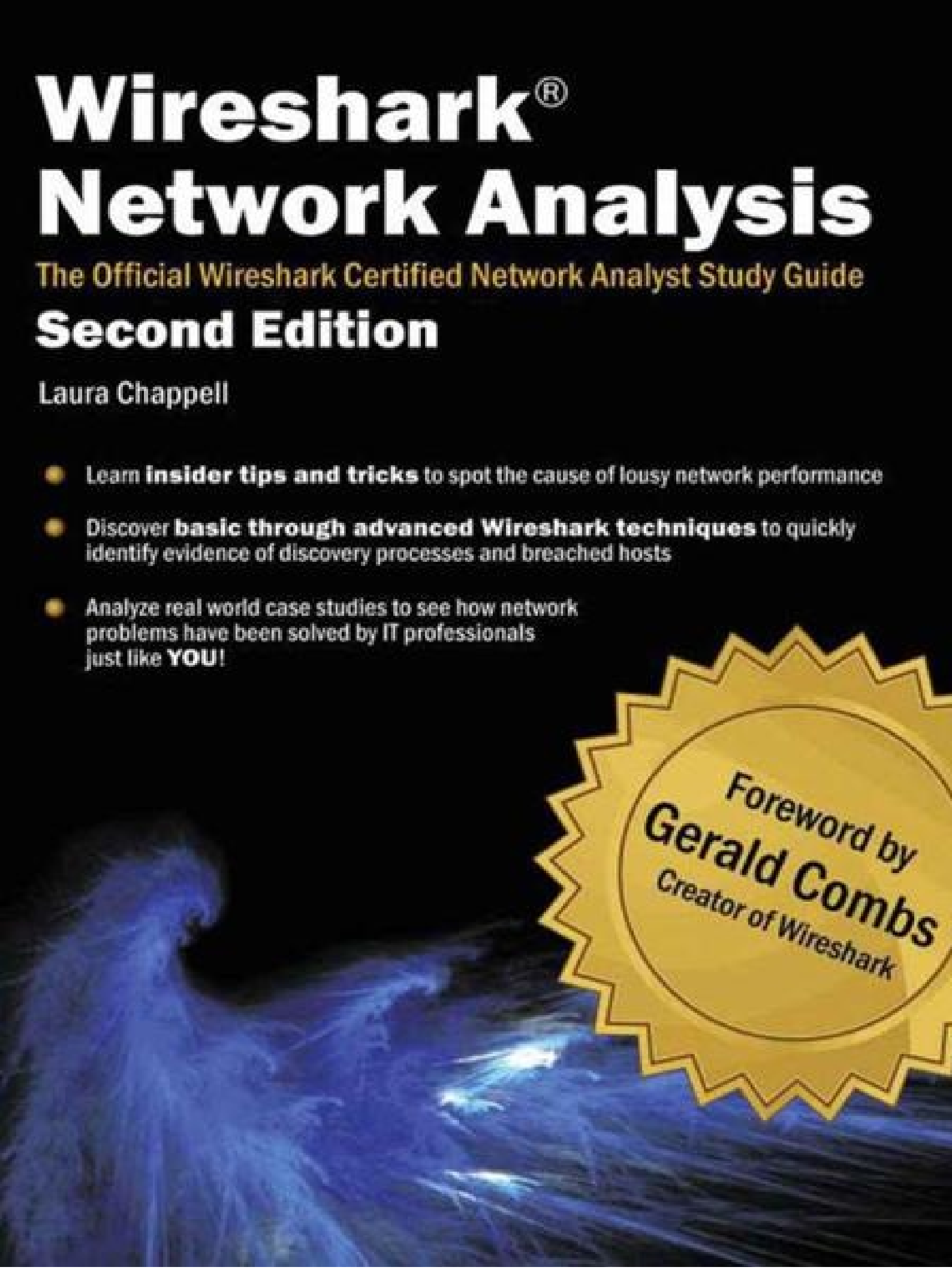
The Official Wireshark Certified Network Analyst Study Guide

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
2nd 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
2nd Edition (Version 2.1b)

Book URL: *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*.

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

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

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

This book and the book website, *www.wiresharkbook.com*, references GeoLite data created by

MaxMind, available from *www.maxmind.com*.

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

This book and the book website, *www.wiresharkbook.com*, references trace files from Mu Dynamics (*www.pcapr.net*).

Protocol Analysis Institute, Inc.
5339 Prospect Road, # 343
San Jose, CA 95129 USA
www.wiresharkbook.com

Also refer to Chappell University at the same address
info@chappellU.com
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* 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.

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 an 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 eac —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 fo 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 feature 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 folk 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*)—thank you both for kindly allowing me to include your *Renegotiating TLS* document and trace files at *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 t 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 a 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 provide 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 Missin 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 fo 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 o 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 you online repository at *www.pcapr.net*. Thank you to **Mu Dynamics** (*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 t 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 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 Gittelson - 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

Table of Contents

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