



Wireshark® Certified Network Analyst™ Official Exam Prep Guide

Exam WCNA-100.x

1st Edition (Version 1.0b)

Laura Chappell

Founder, Chappell University™

Founder, Wireshark University™



This book is intended to provide practice quiz questions based on the thirty-three areas of study defined for the Wireshark Certified Network Analyst Exam. This Official Exam Prep Guide offers a companion to **Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide**.

ISBN10: 1-893939-99-5

ISBN13: 978-1-893939-99-8

Paperback: 800 pages

Website: www.wiresharkbook.com



Wireshark® Certified Network Analyst™ Official Exam Prep Guide

Exam WCNA-100.x

1st Edition (Version 1.0b)

Copyright 2010, Protocol Analysis Institute, Inc., dba “Chappell University”. All rights reserved. No part of this book, or related materials, including interior design, cover design, contents of the accompanying CD or contents of the referenced book website, 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 and email listed on the next page.

Book URL: www.wiresharkbook.com

10-digit ISBN: 1-893939-98-7

13-digit ISBN: 978-1-893939-98-1

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.

Trademarks. All brand names and product names used in this book or mentioned in this book or the accompanying CD are trade names, service marks, trademarks, or registered trademarks of their respective owners. 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 and capture network traffic.

Copy Protection. In all cases, reselling or duplication of this book and related materials used in this Book or the accompanying CD without explicit written authorization is expressly forbidden. We will find you, ya know. So don't steal it or plagiarize this book and don't upload the CD contents to the Internet.

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

Chappell University
5339 Prospect Road, # 343
San Jose, CA 95129 USA
info@chappellU.com
www.chappellU.com

Cover design by Gary Lewis, Kinetic-Creations (www.kinetic-creations.com)

Table of Contents

About This Book	i
How Should You Use this Book?.....	ii
Timed and Untimed Practice Quizzes on the CD.....	iii
What's Online at <i>www.wiresharkbook.com</i> ?.....	iii
Which Version of the Exam Does This Book Match?	iii
Wireshark Certified Network Analyst Exam Objectives	iii
Wireshark Certified Network Analyst™ Program Overview	iv
Why Should I Pursue the Wireshark Certified Network Analyst Certification?.....	iv
How Do I Earn the Wireshark Certified Network Analyst Status?.....	iv
Wireshark University and Wireshark University Training Partners.....	v
Schedule Customized Onsite/Web-Based Training	v
Part 1: Practice Question Set 1-100	7
Part 1 Answer Key	43
Part 1 Answer Explanations	45
Part 2: Practice Question Set 101-206.....	69
Part 2 Answer Key	105
Part 2 Answer Explanations	107
Part 3: Practice Question Set 207-304.....	127
Part 3 Answer Key	159
Part 3 Answer Explanations	161
Appendix A: CD-Based Practice Quizzes	179
Software/Hardware Requirements.....	181
Take a Timed or Untimed Test.....	181
Logging In	182
Welcome Page.....	183
Question Page.....	184
Flag Questions for Review	185
Submit Your Quiz for Scoring	186
Results Page	187
Review Incorrect Answers	188
Appendix B: CD License Agreement.....	189

About This Book



This book is intended to provide practice quiz questions based on the thirty-three areas of study defined for the Wireshark Certified Network Analyst Exam. This Official Exam Prep Guide offers a companion to **Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide**.

ISBN10: 1-893939-99-5

ISBN13: 978-1-893939-99-8

Paperback: 800 pages

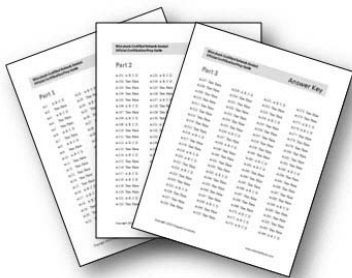
Website: www.wiresharkbook.com

Wireshark Certified Network Analyst™ Official Exam Prep Guide provides you with over 300 practice questions in the book and over 300 practice questions on the accompanying CD. Designed to test you before taking the *Wireshark Certified Network Analyst Exam*, this book offers three separate testing options:

Answer the Questions in the Book—print the Answer Sheets contained on the accompanying CD to note your answers; check your answers against the Answer Key at the end of each part of this book. Review the Answer Explanations (that follow the Answer Key) for any questions you missed.

Take an Interactive Untimed Practice Quiz—the CD contains an untimed test engine that randomly selects different questions each time you run the test. You can flag questions for review and take your time working through a series of 100 questions. There are over 300 questions in the CD test question bank so you will have a chance to take the test multiple times and have a different test experience each time. After submitting your quiz answers for review you can examine your results and see the exact questions that you got correct or incorrect. This enables you to identify topics that you need to study further.

Take an Interactive Timed Practice Quiz—the CD also contains a timed test engine. The questions are randomly selected again, but now you are up against the clock. You have 120 minutes (2 hours) to complete 100 questions.



Answer Sheets—the CD also contains a PDF file with three Answer Sheets—there is one Answer Sheet for each of the three parts of this book.

The Answer Sheets enable you to take the tests in the book multiple times without marking up the book and seeing previous answer selections. Answer Sheets are formatted to match the Answer Keys for fast grading.

How Should You Use this Book?

This book is separated into three parts. The following provides a recommendation of how to use this book to effectively prepare for the Wireshark Certified Network Analyst Exam.



The key icon marks key topics to study in preparation for the Exam.

Step 1: Review the Study Guide

Each chapter in the Study Guide and each part of this Official Exam Prep Guide lists the objectives covered in the Wireshark Certified Network Analyst Exam. Ensure you have the knowledge and skills to master the objectives listed.

Step 2: Print Out the Answer Sheets

As an alternative to writing your answers directly in this book, you can print answer sheets from the CD (in the Supplements folder) or download Answer Sheets from the Download section at www.wiresharkbook.com. This saves you from the headache of flipping pages from the questions to the Answer Key. The Answer Sheets are formatted to match the Answer Key for each part of the book providing for faster self-grading.

Step 3: Answer the Book Practice Questions in Three Parts

The book is divided into three separate sections of approximately 100 questions each. Part 1 covers Sections 1-11 of the Wireshark Certified Network Analyst Exam while Parts 2 and 3 cover Sections 12-22 and Sections 23-33, respectively.

We recommend that you answer Part 1 questions first and grade those answers before moving on to Part 2 and Part 3. Part 1 covers more of the basic concepts and skills of analysis and basic Wireshark functionality.

Step 4: Grade Your Answers

Each chapter ends with an Answer Key and Answer Explanation section. Use the Answer Key to quickly grade your answers. Refer to the Answer Explanation for details on the correct/incorrect answers posed by each question. The Answer Explanation defines the Study Guide chapters that cover the question topic.

Step 5: Take the Interactive Quizzes on the CD

When ready, take the untimed and timed practice quizzes on the accompanying CD. (Refer to Appendix A for information on system requirements and Appendix B for the CD license agreement).

Timed and Untimed Practice Quizzes on the CD

Appendix A details the contents of the accompanying CD, including information on how to access the timed and untimed practice quizzes contained on the CD. It is recommended that you review Appendix A prior to launching the practice quizzes to learn about the following features:

- Logging into the quizzes
- Taking a timed or untimed quiz
- Flagging questions before submitting
- Reviewing results

Appendix B contains the license agreement for the accompanying CD.

What's Online at *www.wiresharkbook.com*?

There are numerous references and resources related to this book and Wireshark Network Analysis: the Official Wireshark Certified Network Analyst Study Guide available at *www.wiresharkbook.com*. These resources include:

- Numerous trace files (.pcap files)
- Chanalyzer recordings (.wsr files)
- MaxMind® GeoIP® database files (.dat files)
- PhoneFactor™ SSL/TLS vulnerabilities documents and trace files
- Wireshark configurations
- Practice Exam Blank Answer Sheets

Which Version of the Exam Does This Book Match?

This book and the practice questions and quizzes herein, match the Wireshark Certified Network Analyst Exam version 100.x.

Wireshark Certified Network Analyst Exam Objectives

Each part in this book provides a list of exam objectives for the Wireshark Certified Network Analyst program. For additional information regarding exam preparation, visit *www.wiresharktraining.com/certification*.

Wireshark Certified Network Analyst™ Program Overview

The Wireshark Certified Network Analyst Exam is a globally-available, proctored exam to meet the secure and widely available delivery requirements desired by candidates.

Visit www.wiresharktraining.com/certification for additional information on the Wireshark Certified Network Analyst program. Questions regarding your Wireshark Certified Network Analyst status may be directed to info@wiresharktraining.com.

Why Should I Pursue the Wireshark Certified Network Analyst Certification?

Successful completion of the Wireshark Certified Network Analyst Exam indicates you have the knowledge required to capture network traffic, analyze the results and identify various anomalies related to performance or security issues.

How Do I Earn the Wireshark Certified Network Analyst Status?

To earn the Wireshark Certified Network Analyst status, you must pass a single exam—the WCNA-100x exam.

Register for the proctored Wireshark Certified Network Analyst Exam online at www.webassessor.com/pai. (PAI represents the Protocol Analysis Institute, the parent company of Wireshark University and Chappell University. For more information on the Exam registration process, visit www.wiresharktraining.com/certification.

Upon completion of the Wireshark Certified Network Analyst Exam, an individual will receive a pass/fail score. Candidates who successfully pass the Wireshark Certified Network Analyst Exam will receive their Wireshark Certified Network Analyst Confirmation within fifteen (15) working days. The Wireshark Certified Network Analyst Exam confirmation contains the candidate's certificate, additional information regarding analysis resources and details on maintaining Wireshark Certified Network Analyst status. For more information on the Wireshark Certified Network Analyst program, visit www.wiresharktraining.com/certification.

Questions regarding Wireshark CNA Certification status may be directed to info@wiresharktraining.com.

Wireshark University and Wireshark University Training Partners

Wireshark University was launched in March 2007.

The goal of Wireshark University is to provide education on how to analyze, troubleshoot, secure and optimize network communications using Wireshark, the world's most popular network analyzer.

Wireshark University is responsible for creating and maintaining the Wireshark Certified Network Analyst Exam, the Wireshark Certified Network Analyst Members Program, Wireshark University Certified Training Partner Program, Wireshark University Certified Instructor Program, and the Wireshark University Certified Training Materials.



Currently, Wireshark University courses are offered throughout the world in instructor-led, self-paced and online formats through Chappell University (www.chappellU.com) and various Wireshark University Training Partners.

For more information on Wireshark University, visit www.wiresharktraining.com or send email to info@wiresharktraining.com.

Schedule Customized Onsite/Web-Based Training

If you are interested in training a team in a fast, effective, hands-on course environment, contact us directly. Customized courses can be developed and delivered by Laura Chappell. Customized courses are based on your network traffic. Course lengths can run from 2 days to 10 days and even include a web-based delivery option to meet the training needs of geographically dispersed students.

Contact us at info@chappellU.com for more information on scheduling customized training for your organization or visit www.chappellU.com. Online recorded courses are available from Chappell Seminars (www.chappellseminars.com).