



WCNA

CertificationTM

Program

Information Package

Protocol Analysis Institute, Inc.

Chappell University

[Revision 0619c]



Welcome to the WCNA Certification Program

Welcome to the WCNA Certification program (formerly known as the “Wireshark Certified Network Analyst” program¹).

The WCNA Certification Exam (hereinafter referred to as “the Exam”) was designed to confirm individual competencies in network/protocol analysis for the purpose of troubleshooting communications, network optimization, network forensics (security), and confirm in-depth knowledge of TCP/IP.

The Exam is based on the thirty-three areas of study defined in the ***Exam Focus and Content*** section of this document.

Learn more about the WCNA Certification program and the Exam at <https://www.wcnacertification.com>.

Locate a testing center near you at <https://www.kryteriononline.com/Locate-Test-Center>.

Register for the WCNA Certification Exam at <https://www.webassessor.com/pai>.

¹ In April 2019, Riverbed began the process of “monetizing Wireshark’s assets.” As part of this questionable “sponsor” activity, Riverbed’s legal department demanded that we stop using “Wireshark University” and “Wireshark Certified Network Analyst” although we founded both programs with Gerald Combs, the creator of Wireshark. The certification program was therefore renamed to “WCNA Certification.” Our WCNAs may add the line “Wireshark Specialist” to their certification designation, if they wish.

Contents

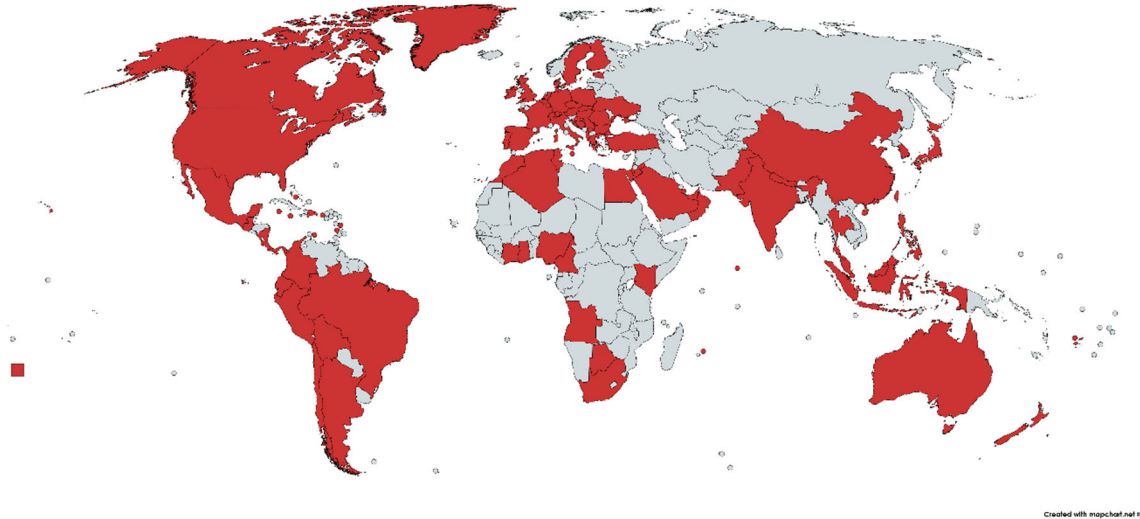
WCNA Overview -----	1
Exam Overview	1
Exam Registration	1
Online Proctored Exam Version	2
Exam Time Limit and Question Count.....	2
Exam Pricing	2
Pass/Fail Grading.....	2
Question Formats	2
Test Retake Procedure	2
Taking Your Proctored Exam -----	3
Acceptable Forms of Identification	3
Closed Book Policy.....	4
Cancellation/Rescheduling Details.....	4
Cancellation/Rescheduling within 72 Hours of Your Exam Appointment	4
Certification Maintenance and Expiration.....	4
In Case of Test Problems or Questions.....	4
Frequently Asked Questions (FAQ) -----	5
Can I keep my belongings with me during the test session?	5
May I bring food or drinks into the testing room?.....	5
Can I take the Exam at the same time I register?.....	5
How long does the Exam take?	5
Is the Exam in English only?	5
Where can I take the Exam?.....	5
What do I get when I pass my Exam?.....	5
How long is my certification valid?	6
How do I take the Practice Exam?	6
How do I prepare for the WCNA Certification Exam?	6
Who created this certification?	6
What's the WCNA Certification Exam passing score?.....	7
I didn't receive my new WCNA Certification credentials yet. Who should I contact?	7

Exam Preparation	8
Online Self-Paced Training	8
All Access Pass Membership	8
Books	8
Wireshark Network Analysis: The Official Wireshark Certified Network Analyst (WCNA) Study Guide, Second Edition	8
Wireshark Certified Network Analyst: Official Exam Prep Guide, Second Edition	8
WCNA Certification Exam Objectives	9
Section 1: Network Analysis Overview	9
Section 2: Introduction to Wireshark	9
Section 3: Capture Traffic	10
Section 4: Create and Apply Capture Filters	10
Section 5: Define Global and Personal Preferences	10
Section 6: Colorize Traffic	11
Section 7: Define Time Values and Interpret Summaries	11
Section 8: Interpret Basic Trace File Statistics	11
Section 9: Create and Apply Display Filters	12
Section 10: Follow Streams and Reassemble Data	12
Section 11: Customize Wireshark Profiles	12
Section 12: Annotate, Save, Export and Print Packets	12
Section 13: Use Wireshark's Expert System	13
Section 14: TCP/IP Analysis Overview	13
Section 15: Analyze Domain Name System (DNS) Traffic	13
Section 16: Analyze Address Resolution Protocol (ARP) Traffic	13
Section 17: Analyze Internet Protocol (IPv4/IPv6) Traffic	13
Section 18: Analyze Internet Control Message Protocol (ICMPv4/ICMPv6) Traffic	14
Section 19: Analyze User Datagram Protocol (UDP) Traffic	14
Section 20: Analyze Transmission Control Protocol (TCP) Traffic	14
Section 21: Graph IO Rates and TCP Trends	14
Section 22: Analyze Dynamic Host Configuration Protocol (DHCPv4/DHCPv6) Traffic	15
Section 23: Analyze Hypertext Transfer Protocol (HTTP) Traffic	15
Section 24: Analyze File Transfer Protocol (FTP) Traffic	15
Section 25: Analyze Email Traffic	15
Section 26: Introduction to 802.11 (WLAN) Analysis	16
Section 27: Voice over IP (VoIP) Analysis Fundamentals	16
Section 28: Baseline "Normal" Traffic Patterns	16
Section 29: Find the Top Causes of Performance Problems	17
Section 30: Network Forensics Overview	17
Section 31: Detect Scanning and Discovery Processes	17
Section 32: Analyze Suspect Traffic	18
Section 33: Effective Use of Command-Line Tools	18

WCNA Overview

The WCNA Certification program has become one of the top industry certifications with over 90 countries represented worldwide.

The certification program focuses on analyzing packets, protocols and traffic for the purpose of network troubleshooting, optimization and security.



Exam Overview

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

To earn the WCNA Certification status, you must pass a single Exam—the WCNA Certification Exam.

The WCNA Certification Exam is available at hundreds of testing centers around the world. You can take your Exam at a KRYTERION High-stake Online Secure Testing (HOST) location.

Register for the proctored WCNA Certification Exam online at <https://www.webassessor.com/pai>.

Exam Registration

Register for the proctored WCNA Certification Exam online at <https://www.webassessor.com/pai>.

Online Proctored Exam Version

The Exam is also available in an Online Proctored Exam format that allows you to schedule to take the test at your home or office. Biometric authentication steps are required (photo and keyboard analytics) in order to register for an Online Proctored Exam.

Online Proctored Exams are proctored via an external webcam following the requirements defined by Kryterion, Inc. To view the requirements for the Online Proctored Exam option, register for a free test taker account at <https://www.webassessor.com/pai> and login to your *Home* page. Under the *Online Proctored* heading you will find links for the requirements documentation, Sentinel software installation, and the biometrics enrollment link.

Visit <https://www.kryteriononline.com/kryterion-support> for more information on Online Proctored Exam technology.

Exam Time Limit and Question Count

The WCNA Certification Exam is a closed-book Exam consisting of 100 questions. The Exam time limit is 2 hours (120 minutes).

Exam Pricing

The WCNA Certification Exam cost is USD 299 for a single Exam sitting. The WCNA Practice Exam (online) cost is USD 29 for a single WCNA Practice Exam session. Additional Exam sittings and WCNA Practice Exam sessions must be paid for separately at the full price. If you require more than one Practice Exam session, we recommend you purchase the *WCNA Certification Official Exam Prep Guide* (see *Wireshark Certified Network Analyst: Official Exam Prep Guide* on page 8).

In addition, the Chappell University All Access Pass online training subscription offers a set of *WCNA Exam Prep Guide* courses. For more information on these courses, visit <https://chappell.talentlms.com>.

Pass/Fail Grading

The WCNA Certification Exam is graded on a pass/fail basis. Passing scores are set by using statistical analysis. At the completion of the Exam, candidates receive a score report.

Question Formats

There are two forms of questions in the WCNA Certification Exam — true/false and multiple choice. Only one answer is correct for each multiple-choice question. Questions may also include images.

Test Retake Procedure

If you fail the Exam, you must wait five (5) business days before retaking the Exam. You must purchase another *Test Taker Authorization Code* at <https://www.webassessor.com/pai>. Only three (3) Exams with the same Exam identification number may be taken per calendar year.

You must purchase another Exam sitting at the full price if you require a retake.

Taking Your Proctored Exam

Once your registration and scheduling are complete, you will receive an email confirmation which includes the details of your registration including your *Test Taker Authorization Code*. The email also includes the HOST location address and the date and time of your Exam session. If you require a customized receipt for your employer, click on the *Generate Receipt* button on the Home page of your Webassessor account.



You are required to bring two forms of identification with you to the HOST location, which your proctor verifies and records. In addition, you must bring your Test Taker Authorization Code which you received in your registration confirmation email.

The proctor will hand you a document to read in the waiting room while they load your Exam in the testing area. The testing center document prepares you for your Exam session.

Once your Exam has loaded, your proctor will show you where the restrooms are, store your personal belongings in a secure compartment, and answer any Exam session questions you may have. You may then begin your Exam.

The Exam engine provides you with detailed instructions on how to take the Exam and guides you through each step of the Exam process.

You have two hours (120 minutes) to complete the WCNA Certification Exam. You may review your answers before submitting your Exam. Unanswered questions are graded as incorrect.

When finished, you are prompted to notify your proctor that you have completed the Exam. The proctor will then close your Exam session. You will receive your pass/fail notification upon completion of the Exam.

Acceptable Forms of Identification

Acceptable forms of photo ID include a government-issued driver's license or ID card, passport, military identification, an employee identification card, or a student picture ID from an accredited college or university.

The following forms of non-photo ID are acceptable: credit card, check cashing card or a bank debit card. A social security card is not an acceptable form of identification.

The Online Proctored Exam requires a photo ID as well as keyboard analytic process to verify the identity of the test taker and match the registrant with the test taker. For more information regarding the Online Proctored Exam process and security, visit <https://www.kryteriononline.com/test-taker/online-proctoring-support>.

Closed Book Policy

The WCNA Certification Exam is closed-book format. No Internet access or open computer (other than the Exam system) is allowed during the Exam. Candidates may not access any printed materials or electronic devices such as extra computers, USB flash drives, or cell phones.

Cancellation/Rescheduling Details

If you need to reschedule your Exam appointment, you may do so **earlier than 72 hours** of your Exam appointment. Log into your KRYTERION account at <https://www.webassessor.com/pai> and click on **View Schedule Details** and the **Reschedule** button.

IMPORTANT: Read the next section regarding cancellation and rescheduling within 72 hours of your Exam appointment.

Cancellation/Rescheduling within 72 Hours of Your Exam Appointment

If you wish to cancel or reschedule your Exam within 72 hours of your appointment, please call the Protocol Analysis Institute, Inc., (PAI) Customer Support line at +1 775-360-5162. Office hours are 10am to 6pm Pacific Time. Do not attempt to contact Kryterion or the testing center directly. *You will forfeit \$175 of your Exam registration fee if you reschedule or cancel your Exam appointment within 72 hours of your Exam appointment or do not show for your Exam appointment.*

Certification Maintenance and Expiration

Your WCNA Certification status is valid for three (3) years from the date of successful Exam completion. At the end of 3 years, you will need to take the Recertification Exam to maintain your certification status. While we do not require Continuing Professional Education (CPE) or Continuing Education Unit (CEU) credits, we do recommend that you continue expanding your knowledge and skills.

In Case of Test Problems or Questions

Please first review the FAQ section of this document on page 5. If you have additional questions regarding the certification process, your certification status, or the Kryterion testing engine, contact Protocol Analysis Institute, Inc., at info@WCNAcertification.com or call the Protocol Analysis Institute, Inc., (PAI) Customer Support line at +1 775-360-5162. Office hours are 10am to 6pm Pacific Time.

Frequently Asked Questions (FAQ)

Can I keep my belongings with me during the test session?

Your personal items may not be accessed during the test session. Personal items include bags, wallets, purses, briefcases, watches, books, beepers, cell phones, electronic organizers and calculators. You should, however, always keep your identification with you.

May I bring food or drinks into the testing room?

No, tobacco products, food, drink, and chewing gum are not allowed in the testing area.

Can I take the Exam at the same time I register?

Not the proctored Exam—the earliest you can schedule your Exam is 72 hours before your desired Exam date/time. Registrants can take the WCNA Practice Exam immediately following registration.

How long does the Exam take?

Candidates are provided two hours (120 minutes) to complete the Exam. An Exam timer indicates the remaining Exam time. A question counter indicates the number of questions answered and total number of questions in the Exam.

A Review Test option allows you to mark questions for review and revisit all questions and answers in the Exam. You may skip questions during the Exam, but it is recommended you complete each question before submitting your Exam for grading. Unanswered questions are marked incorrect. The Practice Exam also includes a two-hour (120 minutes) time limit.

Is the Exam in English only?

Currently the Exam and Practice Exam are only available in English.

Where can I take the Exam?

The WCNA Certification Exam is delivered by Kryterion, Inc. Kryterion has hundreds of testing centers around the world. Visit <https://www.kryteriononline.com/Locate-Test-Center> to locate a Kryterion High-stake Online Secure Testing (HOST) location near you.

What do I get when I pass my Exam?

Within fifteen (15) business days of successful completion of the Exam, Protocol Analysis Institute, Inc., will deliver your *WCNA Certification Welcome Kit* to the email address provided during your Exam registration.

The Welcome Kit includes:

- your WCNA Certification Certificate,
- your WCNA Certification ID Number,
- your valid certification date details,
- “WCNA Certified” logo files, and
- additional information regarding usage of the “WCNA Certified” logo.

How long is my certification valid?

Your WCNA Certification status is valid for three (3) years from the date of successful Exam completion. After that three (3) year period, you must take the WCNA Recertification Exam.

How do I take the Practice Exam?

Register for the Practice Exam just as you register for the final Exam. The Practice Exam is available for you to take as soon as you have completed the registration process at <https://www.webassessor.com/pai>.



Locate the **Launch** button for your Exam on your Webassessor home page. If you need to stop your Practice Exam for some reason, you may do so simply by closing the Practice Exam window. Any questions you have already answered have been saved for you. If the Practice Exam was interrupted due to technical issues, you may re-launch the Practice Exam by logging into your Webassessor home page and clicking the **Launch** button. The Practice Exam will resume at the first unanswered question.

You have two hours (120 minutes) of active time to complete the Practice Exam. Please note that the online Practice exam contains the same question bank included in the *Wireshark Certified Network Analyst Exam Prep Guide* available at Amazon and in the *Exam Prep Guide (WCNA) Courses* in the Chappell University **All Access Pass**. Visit <https://www.chappell-university.com> for more information.

How do I prepare for the WCNA Certification Exam?

You can prepare for the WCNA Certification Exam using self-paced learning, instructor-led training or on-the-job study. Refer to *Exam Preparation* on page 8 for more details.

We recommend the *Wireshark Certified Network Analyst Exam Prep Guide* (see page 8) which contains over 300 practice questions. The *Wireshark Certified Network Analyst Exam Prep Guide* is available through Amazon in both paperback and Kindle format.

In addition, the Chappell University All Access Pass online training subscription offers a set of *WCNA Exam Prep Guide* courses. For more information on these courses, visit <https://chappell.talentlms.com>.

Who created this certification?

Laura Chappell, world-renown network analyst and founder of Chappell University and the Protocol Analysis Institute, Inc., created the WCNA Certification program in 2007². You can learn more about Laura Chappell at <https://www.chappell-university.com>.

² The WCNA Certification program was formerly called the “Wireshark Certified Network Analyst” program.

What's the WCNA Certification Exam passing score?

The WCNA Certification Exam is a Pass/Fail exam. You are provided with topics of the questions answered incorrectly on each Exam upon completion of the Exam. The passing score for each examination is calculated by equating the scoring values associated with each question.

I didn't receive my new WCNA Certification credentials yet. Who should I contact?

Send an email to info@WCNAcertification.com with your contact details. We will follow up and respond as soon as possible.

Exam Preparation

The WCNA Certification Exam focuses on TCP/IP communications analysis, troubleshooting, optimization, and network forensics.

Consider the following options for Exam preparation.

Online Self-Paced Training

All Access Pass Membership

The All Access Pass (AAP) subscription provides access to numerous courses on Wireshark and TCP/IP network analysis, troubleshooting, and security.

For example, you can find the following courses in the AAP:

- Network Forensics with Wireshark
- Wireshark 101: Essential Skills for Network Analysis
- Troubleshooting with Wireshark
- WCNA Exam Prep Guide

Visit <https://www.chappell-university.com> to view the complete contents of the All Access Pass.



Books

Wireshark Network Analysis: The Official Wireshark Certified Network Analyst (WCNA) Study Guide, Second Edition

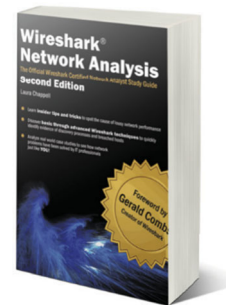
This comprehensive book covers all thirty-three areas of study for the WCNA Certification Exam while providing numerous case studies, tips and tricks for using Wireshark efficiently to troubleshoot and secure networks.

ISBN10: 1-893939-94-4

ISBN13: 978-1-893939-94-3

Paperback: 986 pages

Book URL: <https://www.chappell-university.com/books>



Wireshark Certified Network Analyst: Official Exam Prep Guide, Second Edition

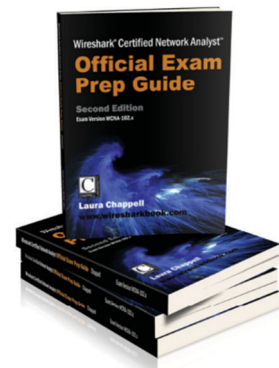
This book provides 300+ practice quiz questions based on the thirty-three areas of study defined for the WCNA Certification Exam. This Official Exam Prep Guide offers a companion to *Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide (Second Edition)*.

10-digit ISBN: 1-893939-90-1

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

Paperback: 186 pages

Book URL: <https://www.chappell-university.com/books>





WCNA Certification Exam Objectives


The WCNA Certification Exam is based on thirty-three areas of concentration.

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




Section 1: Network Analysis Overview

- Define the Purpose of Network Analysis 
- List Troubleshooting Tasks for the Network Analyst 
- List Security Tasks for the Network Analyst
- List Optimization Tasks for the Network Analyst
- List Application Analysis Tasks for the Network Analyst
- Define Legal Issues of Listening to Network Traffic
- Overcome the "Needle in the Haystack " Issue
- Understand General Network Traffic Flows
- Review a Checklist of Analysis Tasks





Section 2: Introduction to Wireshark

- Describe Wireshark's Purpose
- Know How to Obtain the Latest Version of Wireshark
- Compare Wireshark Release and Development Versions
- Report a Wireshark Bug or Submit an Enhancement
- Capture Packets on Wired or Wireless Networks 
- Open Various Trace File Types
- Describe How Wireshark Processes Packets
- Define the Elements of 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
- Access Options through Right-Click Functionality
- Define the Functions of the Menus and Toolbars


Section 3: Capture Traffic

- Know Where to Tap into the Network 
- Know When to Run Wireshark Locally
- Capture Traffic on Switched Networks
- Define how Test Access Ports (TAPs) are used 
- Define When to Set up Port Spanning/Port Mirroring on a Switch
- Analyze Routed Networks
- Analyze Wireless Networks
- Define Options for Capturing at Two Locations Simultaneously (Dual Captures)
- Identify the Most Appropriate Capture Interface
- Capture on Multiple Adapters Simultaneously
- Capture Traffic Remotely
- Automatically Save Packets to One or More Files 
- Optimize Wireshark to Avoid Dropping Packets
- Conserve Memory with Command-Line Capture

Section 4: Create and Apply Capture Filters

- Describe the Purpose of Capture Filters
- Build and Apply a Capture Filter to an Interface
- Filter by a Protocol 
- 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
- Share Capture Filters with Others

Section 5: Define Global and Personal Preferences

- Find Your Configuration Folders
- Set Global and Personal Configurations
- Customize Your User Interface Settings
- Define Your Capture Preferences
- Define How Wireshark Automatically Resolves 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 Right-Click

Section 6: Colorize Traffic

- Use Colors to Differentiate Traffic
- Disable One or More Coloring Rules
- Share and Manage Coloring Rules
- Identify Why a Packet is a Certain Color
- Color Conversations to Distinguish Them
- Temporarily Mark Packets of Interest



Section 7: Define Time Values and Interpret Summaries

- Use Time to Identify Network Problems
- Understand How Wireshark Measures Packet Time
- Choose the Ideal Time Display Format
- Identify Delays with Time Values
- Create Additional Time Columns
- Measure Packet Arrival Times with a Time Reference
- Identify Client, Server and Path Delays
- Calculate End-to-End Path Delays
- Locate Slow Server Responses
- Spot Overloaded Clients
- View a Summary of Traffic Rates, Packet Sizes and Overall Bytes Transferred

Section 8: Interpret Basic Trace File Statistics

- Launch Wireshark Statistics
- Identify Network Protocols and Applications
- 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

Section 9: Create and Apply Display Filters

- Understand the Purpose of Display Filters 
- Create Display Filters Using Auto-Complete
- Apply Saved Display Filters
- Make Display Filters Quickly Using Right-Click Filtering
- Filter on Conversations and Endpoints
- 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
- Use Display Filter Macros for Complex Filtering
- Avoid Common Display Filter Mistakes
- Manually Edit the *dfilters* File


Section 10: Follow Streams and Reassemble Data

- Follow and Reassemble UDP Conversations
- Follow and Reassemble TCP Conversations
- Follow and Reassemble SSL Conversations
- Identify Common File Types


Section 11: Customize Wireshark Profiles

- Customize Wireshark with Profiles
- Create a New Profile
- Share Profiles
- Create a Troubleshooting Profile
- Create a Corporate Profile
- Create a WLAN Profile
- Create a VoIP Profile
- Create a Security Profile









Section 12: Annotate, Save, Export and Print Packets

- Annotate a Packet or an Entire Trace File
- Save Filtered, Marked and Ranges of Packets
- Export Packet Contents for Use in Other Programs
- Export SSL Keys 
- Save Conversations, Endpoints, I/O Graphs and Flow Graph Information
- Export Packet Bytes





Section 13: Use Wireshark's Expert System

- Launch Expert Info Quickly
- Colorize Expert Info Elements
- Filter on TCP Expert Information Elements
- Define TCP Expert Information 






Section 14: TCP/IP Analysis Overview

- Define Basic TCP/IP Functionality 
- Follow 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 






Section 15: Analyze Domain Name System (DNS) Traffic

- Define the Purpose of DNS 
- Analyze Normal DNS Queries/Responses 
- Analyze DNS Problems 
- Dissect the DNS Packet Structure 
- Filter on the DNS/MDNS Traffic





Section 16: Analyze Address Resolution Protocol (ARP) Traffic

- Define the Purpose of ARP Traffic 
- Analyze Normal ARP Requests/Responses 
- Analyze Gratuitous ARP 
- Analyze ARP Problems 
- Dissect the ARP Packet Structure 
- Filter on ARP Traffic





Section 17: Analyze Internet Protocol (IPv4/IPv6) Traffic

- Define the Purpose of IP 
- Analyze Normal IPv4 Traffic 
- Analyze IPv4 Problems 
- Dissect the IPv4 Packet Structure 
- Filter on IPv4/IPv6 Traffic 
- Sanitize IPv4 Addresses in a Trace File
- Set Your IP Protocol Preferences












Section 18: Analyze Internet Control Message Protocol (ICMPv4/ICMPv6) Traffic

- Define the Purpose of ICMP 
- Analyze Normal ICMP Traffic 
- Analyze ICMP P Problems 
- Dissect the ICMP Packet Structure 
- Filter on ICMP and ICMPv6 Traffic




Section 19: Analyze User Datagram Protocol (UDP) Traffic

- Define the Purpose of UDP 
- Analyze Normal UDP Traffic 
- Analyze UDP Problems 
- Dissect the UDP Packet Structure 
- Filter on UDP Traffic





Section 20: Analyze Transmission Control Protocol (TCP) Traffic

- Define the Purpose of TCP 
- Analyze Normal TCP Communications 
- Define the Establishment of TCP Connections 
- Define How TCP-based Services Are Refused 
- Define How TCP Connections are Terminated 
- Track TCP Packet Sequencing 
- Define How TCP Recovers from Packet Loss 
- Improve Packet Loss Recovery with Selective Acknowledgments 
- Define TCP Flow Control 
- Analyze TCP Problems 
- Dissect the TCP Packet Structure 
- Filter on TCP Traffic
- Set TCP Protocol Parameters








Section 21: Graph I/O Rates and TCP Trends

- Use Graphs to View Trends
- Generate Basic I/O Graphs
- Filter I/O Graphs
- Generate Advanced I/O Graphs
- Compare Traffic Trends in I/O Graphs 
- Graph Round Trip Time
- Graph Throughput Rates
- Graph TCP Sequence Numbers over Time
- Interpret TCP Window Size Issues 
- Interpret Packet Loss, Duplicate ACKs and Retransmissions 







Section 22: Analyze Dynamic Host Configuration Protocol (DHCPv4/DHCPv6) Traffic

- Define the Purpose of DHCP 
- Analyze Normal DHCP Traffic 
- Analyze DHCP Problems 
- Dissect the DHCP Packet Structure 
- Filter on DHCPv4/DHCPv6 Traffic
- Display BOOTP-DHCP Statistics



Section 23: Analyze Hypertext Transfer Protocol (HTTP) Traffic

- Define the Purpose of HTTP 
- Analyze Normal HTTP Communications 
- Analyze HTTP Problems 
- Dissect HTTP Packet Structures 
- Filter on HTTP or HTTPS Traffic
- Export HTTP Objects
- Display HTTP Statistics
- Graph HTTP Traffic Flows
- Analyze HTTPS Communications 
- Analyze SSL/TLS Handshake 
- Analyze TLS Encrypted Alerts 
- Decrypt HTTPS Traffic
- Export SSL Keys

Section 24: Analyze File Transfer Protocol (FTP) Traffic

- Define the Purpose of FTP 
- Analyze Normal FTP Communications 
- Analyze Passive Mode Connections 
- Analyze Active Mode Connections 
- Analyze FTP Problems 
- Dissect the FTP Packet Structure 
- Filter on FTP Traffic
- Reassemble FTP Traffic

Section 25: Analyze Email Traffic

- Analyze Normal POP Communications
- Analyze POP Problems
- Dissect the POP Packet Structure
- Filter on POP Traffic
- Analyze Normal SMTP Communications 
- Analyze SMTP Problems 
- Dissect the SMTP Packet Structure
- Filter on SMTP Traffic

Section 26: Introduction to 802.11 (WLAN) Analysis

- 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
- Analyze Normal 802.11 Communications
- Dissect Basic 802.11 Frame Elements
- Filter on WLAN Traffic
- Analyze Frame Control Types and Subtypes
- Customize Wireshark for WLAN Analysis











Section 27: Voice over IP (VoIP) Analysis Fundamentals

- Define VoIP Traffic Flows
- Analyze Session Bandwidth and RTP Port Definition
- Analyze VoIP Problems
- Analyze SIP Traffic and RTP
- Play Back VoIP Conversations
- Decipher RTP Payloads
- Create a VoIP Profile
- Filter on VoIP Traffic




Section 28: Baseline “Normal” Traffic Patterns

- Define the Importance of Baseline
- Baseline Broadcast and Multicast Types and Rates
- Baseline Protocols and Applications
- Baseline Boot up Sequences
- Baseline Login/Logout Sequences
- Baseline Traffic during Idle Time
- Baseline Application Launch Sequences and Key Tasks
- Baseline Web Browsing Sessions
- Baseline Name Resolution Sessions
- Baseline Throughput Tests
- Baseline Wireless Connectivity
- Baseline VoIP Communications











Section 29: Find the Top Causes of Performance Problems

- Troubleshoot Performance Problems 
- Identify High Latency Times 
- Point to Slow Processing Times 
- Find the Location of Packet Loss 
- Watch Signs of Misconfigurations 
- Analyze Traffic Redirections 
- Watch for Small Payload Sizes 
- Locate Problems Caused by Congestion 
- Identify Application Faults 
- Note Any Name Resolution Faults 

Section 30: Network Forensics Overview

- Compare Host to Network Forensics 
- Gather Evidence
- Avoid Detection
- Handle Evidence Properly 
- Recognize Unusual Traffic Patterns 
- Color Unusual Traffic Patterns

Section 31: Detect Scanning and Discovery Processes

- Define the Purpose of Discovery and Reconnaissance 
- 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

Section 32: Analyze Suspect Traffic

- Identify Vulnerabilities in the TCP/IP Resolution Processes
- Find Maliciously Modified 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
- Locate Route Redirection Using ICM
- Catch ARP Poisoning
- Catch IP Fragmentation and Overwriting
- Spot TCP Splicing
- Watch Other Unusual TCP Traffic
- Identify Password Cracking Attempts
- Build Filters and Coloring Rules from IDS Rules

Section 33: Effective Use of Command-Line Tools

- Define the Purpose of Command-Line Tools
- Use Wireshark.exe (Command-Line Launch)
- Capture Traffic with Tshark
- List Trace File Details with Capinfos
- Edit Trace Files with Editcap
- Merge Trace Files with Mergecap
- Convert Text with Text2pcap
- Capture Traffic with Dumpcap