# Wireshark Certified Analyst (WCA-101)

Master the core skills of packet analysis that set you apart as a Wireshark Certified Analyst. This Wireshark tutorial shows you how to use the world's most popular packet capture tool to inspect traffic in motion, identify key protocol headers, and pinpoint issues with dynamic filters. Study with unlimited virtual labs built by IT pros, and build the hands-on experience you need to pass the WCA-101 exam. Earn your Wireshark Certified Analyst credential as you capture real traffic and troubleshoot Ethernet, IP, TCP, and application-layer problems.

CBT Nuggets course material →

STUDY PLAN

**WEEK 1**

## Managing Wireshark Files

Wireshark Overview

TCP/IP Protocol Suite

The Encapsulation/Decapsulation of Data

Open, Save, and Close Files, and Export Specified Packets

Describe the Difference Between Different Capture File Formats, Especially PCAP an

Hands-on Lab

## Exporting Objects and Finding Packets

Introduction

Export Objects From Packet Captures

Use "Find Packet" to Locate Packets of Interest

Use the Packet and File Comments Feature

Set/Unset Time Reference

Apply Different Time Formats in a Capture

Hands-on Lab

## Core Wireshark Features for Packet Analysis

Introduction

Describe How Wireshark Applies Different Name Resolution Options

Configure Name Resolution

Use "Decode As" Feature

Use "Capture File Properties" to Identify Key Information About the Capture

Use "Protocol Hierarchy" to Identify Key Protocols in a Capture

Hands-on Lab

## Additional Wireshark Features for Packet Analysis

Introduction

Use "Conversations" to Identify Key Communications in a Capture

Use "Endpoints" to Analyze Host Traffic in a Capture

Create and Interpret an I/O Graph That Shows Packets/s or Bits/s for a Given Display Filter

Distinguish Between Actual Bytes Captured and Fields Generated by the Wireshark Dissectors (Shown in [ ])

Use "Follow TCP/UDP Stream"

Hands-on Lab

## Wireshark Capture Techniques and Management

Introduction

Legal Considerations of Using Wireshark

Compare and Contrast the Benefits of Different Methods Used for Traffic Capture

Select the Appropriate Interface to Capture Traffic in Wireshark

Start/Stop/Restart Capture in Wireshark

Limit Capture by File Size, Packets, or Duration

Implement a Ring Buffer

Hands-on Lab

## Command-Line and File Operations in Wireshark

Introduction

Save a Capture

Export Specified Packets to a New File

Capture Traffic Using Command-Line Tools

Capture Traffic Using "dumpcap.exe"

Capture Traffic Using tshark.exe

Use "editcap.exe" to Modify a Capture File

Use "mergecap.exe" to Merge Multiple Capture Files

Describe the Purpose of Using Promiscuous or Monitor Mode During a Capture

Hands-on Lab

## Using Capture and Display Filters

Introduction

Compare and Contrast Display Filters and Capture Filters

Display Filters and Capture Filters Demo

Implement a Capture Filter to Capture Only Traffic From a Single Protocol, IP Addre

Use Multiple Methods to Create a Display Filter to Isolate Traffic for a Single Protoco

Hands-on Lab

## Membership Filters and Operators

Introduction

Use Membership Filters (tcp.port in {80,443})

Use Logical Operators to Connect Multiple Filters Together

Comparison Operators

Create a Button for Easy Access to a Display Filter

Hands-on Lab

## Mastering Display Filters in Wireshark

Introduction

Identify Situations Where a Display Filter Will Show Incomplete or Excess Results

Parentheses in Display Filters

Identify the Behavior of Using ! (Not) in Different Parts of Filter Logic by Explaining th

Apply Filters From Statistics > Conversations and Statistics > Endpoints

Create a Filter Using Generated Fields in Wireshark

Hands-on Lab

## Wireshark Interface and Profiles

Introduction

Identify Key Components of the GUI (Packet List, Hex View, Packet Details, etc.)

Modify Panes With a Different Layout/Features

Describe the Value of Using Profiles

Create/Modify/Copy a Profile

Wireshark Profile Files

Hands-on Lab

### Custom Views and Highlighting for Packet Analysis

Introduction

Describe the Importance of Columns in Troubleshooting

Use Multiple Methods to Add a Column

Use Coloring Rules to Highlight Packets

Use the Minimap (Colored Sidebar) to Quickly Locate Packets of Interest

Use the "Colorize Conversation" Feature

Understand the Importance of Protocol Preferences in Your Analysis

Use the Mark/Unmark Packet Feature

Hands-on Lab

### Analyze Ethernet Frames

Intro to Analyzing Ethernet Frames

Protocol Stacks Overview

Layer 2 Ethernet Overview

EtherTypes and MAC Addresses

EtherType for ARP

EtherType for 802.1Q Tagging

EtherType for LACP and LLDP

802.3 +LLC/SNAP Frames

EtherType for MPLS

Validation for Layer 2 EtherTypes

### Analyze ARP in Action

Introduction to Analyze ARP in Action

ARP Protocol Purpose and Operation

**WEEK 2**

ARP Request and Reply Analysis

ARP Probe

Gratuitous ARP

Working with ARP Caches

Validation for ARP

### Analyzing Attacks at L2 with Wireshark

Introduction to Analyzing Attacks at L2

MAC Flooding

Local Ping Sweep Scan

Remote Ping Sweep Scan

On-Path MITM ARP Poisoning

Validation of L2 Attacks

### IPv4 Header Fundamentals

Intro to IPv4 Header Fundamentals

IPv4 Header Overview

Core IPv4 Header Fields

IPv4 Address Ranges

IPv4 NAT Fundamentals

**WEEK 3**

Predicting NAT Behavior

Capture and Analyze NAT Traffic

Validation – IPv4 Header Fundamentals

### IPv4 Fragmentation - Reassembly

Introduction – IPv4 Fragmentation & Reassembly

Overview – IPv4 Fragmentation & Reassembly

IPv4 Fragmentation and Reassembly Process

IPv4 Fragmentation, TCP MSS, and Path MTU Discovery

IPv4 Fragmentation Issues

Validation – IPv4 Fragmentation & Reassembly

### Using IPv4 TTL and Protocol Fields

Introduction – Using IPv4 TTL and Protocol Fields

Overview - IPv4 TTL and Protocol Fields

IPv4 TTL Behavior and Path Analysis

IPv4 Routing Loops and TTL

IPv4 Encapsulation and Protocols

Validation – Using IPv4 TTL and Protocol Fields

## WEEK 4

### IPv4 Troubleshooting With Wireshark

Introduction – IPv4 Troubleshooting

Overview – IPv4 Troubleshooting

Troubleshooting Scenario 1

Troubleshooting Scenario 2

Troubleshooting Scenario 3

Validation – IPv4 Troubleshooting

### ICMPv4 Packet Analysis

Introduction – ICMPv4 Packet Analysis

Overview – ICMPv4

Echo Request and Response

ICMPv4 Unreachable Type 3

ICMPv4 Time Exceeded Type 11

Validation – ICMPv4 Analysis

### Analyzing IPv6 in Wireshark

Introduction – Analyzing IPv6

Overview – IPv6

IPv6 Addressing and Types

IPv6 Header Fundamentals

IPv6 Neighbor Discovery Protocol (NDP) Overview

## WEEK 5

IPv6 Neighbor Discovery Protocol (NDP) Analysis

IPv6 Extension Headers

Validation – Analyzing IPv6

### UDP Packet Analysis

Introduction – UDP Packet Analysis

Overview – UDP Packet Analysis

UDP Header Fundamentals

UDP Communication Examples

UDP Issues and Analysis

Validation – UDP Packet Analysis

### DHCPv4 Packet Analysis

Introduction – DHCPv4 Packet Analysis

Overview – DHCPv4

DORA in Action

Option Types and Their Values

Filters for DHCP

DHCPv4 Relay Operation and Analysis

When 169.254.x.x Appears

Validation – DHCPv4 Packet Analysis

### DNS Packet Analysis

Intro to Analyzing DNS Traffic

Overview - Analyzing DNS Traffic

## WEEK 6

Identifying DNS Requests and Replies in Captures

Understanding and Filtering DNS Record Types

Correlating DNS Data to Broader Network Activity

Validation - Analyzing DNS Traffic

### TCP and the 3-Way Handshake

Introduction to TCP and the 3-Way Handshake

Overview of TCP and the 3-Way Handshake

Analyzing the Three-Way Handshake

Using Display Filters for TCP Connection Setup

Troubleshooting Incomplete or Failed Handshakes

Validation - TCP and the 3-Way Handshake

### TCP SEQ & ACK Numbers

Introduction to TCP Sequence and Acknowledgement Numbers

Overview of TCP Sequence and Acknowledgement Numbers

Understanding TCP SEQ Numbers and ACKs

Using Wireshark to Confirm TCP SEQ Numbers and ACKs

Tools and Filtering for TCP SEQ Numbers and ACKs

Validation TCP SEQ Numbers and ACKs

## WEEK 7

### TCP Session Teardown and Reset

Introduction to TCP Session Teardown and Reset

Review of TCP Connection Setup

Session Termination Overview

Graceful TCP Teardown

Port Scans

Observing TCP Setup and Teardown

Validation

### TCP Selective Acknowledgements

Intro to TCP SACK Options

SACK Options Overview

Looking at Selective ACKs (SACKs) in Wireshark

Another Look into SACKs

FAST Retransmissions

Validation for TCP SACK

### Analyzing TCP MSS

Introduction to TCP MSS

Overview of MSS Negotiation and Path MTU

Preparing the Wireshark Profile

Observing MSS in Wireshark

IPv6 and MSS

## WEEK 8

Tunnels and MSS

MSS Asymmetry

MSS Clamping by Intermediate Devices

Validation – Analyzing MSS in Action

### TCP Window Scaling and Timing

Introduction to TCP Window Scaling and Timing

Overview of TCP Window Scaling and Timing

Who is Sending What, and When?

Confirming Whether TCP Window Scaling Is Enabled

Confirming the Actual Receiver Window Size

Comparing Sessions With and Without Window Scaling

Analyzing iRTT and TCP Timers in Wireshark

Validation – Applying Window Scaling and RTT Analysis

### Visualizing Traffic with I/O Graphs

Introduction to I/O Graphs

Overview of I/O Graphs

Using Basic I/O Graph Features

Using the Custom Profiles

Comparing and Filtering Traffic

Using Min, Max, and Average in I/O Graphs

## WEEK 9

Validation I/O graphs

### Using Wireshark Flow Graphs

Introduction to Flow Graphs

Overview of Flow Graphs

Conversation and Direction Basics

Building Flow Graphs

Analyzing Request and Response Sequences

Identifying Problems and Issues by Using the Flow Graph

Validation Flow Graphs

### Using TCP Stream Graphs

Introduction  to TCP Stream Graphs

Overview of TCP Stream Graphs

Time-Sequence Graph & Contiguous SACK Blocks

Non-Contiguous SACK Blocks

Time-Sequence Graph (Stevens)

ACK RTT Graph

Throughput Graph

Window Scaling Graph

Validation for TCP Stream Graphs

### Wireshark Used for Troubleshooting

Intro to Troubleshooting

Troubleshooting Overview

Troubleshooting Scenario 1

## WEEK 10

Troubleshooting Scenario 2

Troubleshooting Scenario 3

Troubleshooting Scenario 4

Troubleshooting Scenario 5