# TROUBLESHOOTING TCP/IP NETWORKS WITH WIRESHARK

Course Code: 9879

## Learn to use Wireshark to identify and fix your TCP/IP network performance problems.

Optimize TCP/IP networks with Wireshark®. This hands-on, in-depth course provides the skills to isolate and fix network performance issues. Learn how Wireshark can solve your TCP/IP network problems by improving your ability to analyze network traffic.

## What You'll Learn

- Top 10 reasons for network performance complaints
- Place the analyzer properly for traffic capture on a variety of network types
- Capture packets on wired and wireless networks
- Configure Wireshark for best performance and non-intrusive analysis
- Navigate through, split, and work with large traffic files
- Use time values to identify network performance problems
- Create statistical charts and graphs to pinpoint performance issues
- Filter out traffic for more efficient troubleshooting and analysis
- Customize Wireshark coloring to focus on network problems faster
- Use Wireshark's Expert System to understand various traffic problems
- Use the TCP/IP Resolution Flowchart to identify possible communication faults
- Analyze normal/abnormal Domain Name System (DNS) traffic
- Analyze normal/abnormal Address Resolution Protocol (ARP) traffic
- Analyze normal/abnormal Internet Protocol v4 (IPv4) traffic
- Analyze normal/abnormal Internet Control Messaging Protocol (ICMP) traffic
- Analyze normal/abnormal User Datagram Protocol (UDP) traffic
- Analyze normal/abnormal Transmission Control Protocol (TCP) traffic
- Analyze normal/abnormal Hypertext Transport Protocol (HTTP/HTTPS) traffic

## Who Needs to Attend

Anyone interested in learning to troubleshoot and optimize TCP/IP networks and analyze network traffic with Wireshark, especially network engineers, information technology specialists, security analysts, and those preparing for the Wireshark

Certified Network Analyst exam.

## Prerequisites

Recommended:

skillsoft global knowledge™

# TROUBLESHOOTING TCP/IP NETWORKS WITH WIRESHARK

Course Code: 9879

| | | |
|---|---|---|
| CLASSROOM LIVE | $5,063 CAD | 5 Day |

# TROUBLESHOOTING TCP/IP NETWORKS WITH WIRESHARK

Course Code: 9879

| | | |
|---|---|---|
| VIRTUAL CLASSROOM LIVE | $5,063 CAD | 5 Day |

## Virtual Classroom Live Outline

### 1. Introduction to Network Analysis and Wireshark

- TCP/IP Analysis Checklist
- Top Causes of Performance Problems
- Get the Latest Version of Wireshark
- Capturing Traffic
- Opening Trace Files
- Processing Packets
- The Qt Interface Overview
- Using Linked Panes
- The Icon Toolbar
- Master the Intelligent Scrollbar
- The Changing Status Bar
- Right-Click Functionality
- General Analyst Resources
- Your First Task When You Leave Class

### 2. Learn Capture Methods and Use Capture Filters

- Analyze Switched Networks
- Walk-Through a Sample SPAN Configuration
- Analyze Full-Duplex Links with a Network TAP
- Analyze Wireless Networks
- USB Capture
- Initial Analyzing Placement
- Remote Capture Techniques
- Available Capture Interfaces
- Save Directly to Disk
- Capture File Configurations

- Limit Your Capture with Capture Filters
- Examine Key Capture Filters

**3. Customize for Efficiency: Configure Your Global Preferences**

- First Step: Create a Troubleshooting Profile
- Customize the User Interface
- Add Custom Columns for the Packet List Pane
- Set Your Global Capture Preferences
- Define Name Resolution Preferences
- Configure Individual Protocol Preferences

**4. Navigate Quickly and Focus Faster with Coloring Techniques**

- Move Around Quickly: Navigation Techniques
- Find a Packet Based on Various Characteristics
- Build Permanent Coloring Rules
- Identify a Coloring Source
- Use the Intelligent Scrollbar with Custom Coloring Rules
- Apply Temporary Coloring
- Mark Packets of Interest

**5. Spot Network and Application Issues with Time Values and Summaries**

- Examine the Delta Time (End-of-Packet to End-of-Packet)
- Set a Time Reference
- Compare Timestamp Values
- Compare Timestamps of Filtered Traffic
- Enable and Use TCP Conversation Timestamps
- Compare TCP Conversation Timestamp Values
- Determine the Initial Round Trip Time (iRTT)
- Troubleshooting Example Using Time
- Analyze Delay Types

**6. Create and Interpret Basic Trace File Statistics**

- Examine Trace File Summary Information
- View Active Protocols
- Graph Throughput to Spot Performance Problems Quickly
- Locate the Most Active Conversations and Endpoints
- Other Conversation Options
- Graph the Traffic Flows for a More Complete View
- Burst Statistics
- Numerous Other Statistics are Available
- Quick Overview of VoIP Traffic Analysis
- SIP and RTP Analysis Overview
- SIP Call Setup
- Analyzing Call Setup with SIP
- Session Bandwidth and RTP Port Definition

**7. Focus on Traffic Using Display Filters**

- Display Filters

- Filter on Conversations/Endpoints
- Build Filters Based on Packets
- Display Filter Syntax
- Use Comparison Operators and Advanced Filters
- Filter on Text Strings
- Build Filters Based on Expressions
- Watch for Common Display Filter Mistakes
- Share Your Display Filters

**8. TCP/IP Communications and Resolutions Overview**

- TCP/IP Functionality
- When Everything Goes Right
- The Multi-Step Resolution Process
- Resolution Helped Build the Packet
- Where Faults Can Occur
- Typical Causes of Slow Performance

**9. Analyze DNS Traffic**

- DNS Overview
- DNS Packet Structure
- DNS Queries
- Filter on DNS Traffic
- Analyze Normal/Problem DNS Traffic

**10. Analyze ARP Traffic**

- ARP Overview
- ARP Packet Structure
- Filter on ARP Traffic
- Analyze Normal/Problem ARP Traffic

**11. Analyze IPv4 Traffic**

- IPv4 Overview
- IPv4 Packet Structure
- Analyze Broadcast/Multicast Traffic
- Filter on IPv4 Traffic
- IP Protocol Preferences
- Analyze Normal/Problem IP Traffic

**12. Analyze ICMP Traffic**

- ICMP Overview
- ICMP Packet Structure
- Filter on ICMP Traffic
- Analyze Normal/Problem ICMP Traffic

**13. Analyze UDP Traffic**

- UDP Overview
- Watch for Service Refusals
- UDP Packet Structure

- Filter on UDP Traffic
- Follow UDP Streams to Reassemble Data
- Analyze Normal/Problem UDP Traffic

**14. Analyze TCP Protocol**

- TCP Overview
- The TCP Connection Process
- TCP Handshake Problem
- Watch Service Refusals
- TCP Packet Structure
- The TCP Sequencing/Acknowledgment Process
- Packet Loss Detection in Wireshark
- Fast Recovery/Fast Retransmission Detection in Wireshark
- Retransmission Detection in Wireshark
- Out-of-Order Segment Detection in Wireshark
- Selective Acknowledgement (SACK)
- Window Scaling
- Window Size Issue: Receive Buffer Problem
- Window Size Issue: Unequal Window Size Beliefs
- TCP Sliding Window Overview
- Troubleshoot TCP Quickly with Expert Info
- Filter on TCP Traffic and TCP Problems
- Properly Set TCP Preferences
- Follow TCP Streams to Reassemble Data 16. Examine Advanced Trace File Statistics
- Build Advanced IO Graphs
- Graph Round Trip Times
- Graph TCP Throughput
- Find Problems Using TCP Time-Sequence Graphs

**15. Graph Traffic Characteristics**

- Advanced I/O Graphing
- Graph Round Trip Times
- Graph TCP Throughput
- Find Problems Using TCP Time Sequence Graphs

**16. Analyze HTTP Traffic**

- HTTP Overview
- HTTP Packet Structure
- Filter on HTTP Traffic
- Reassembling HTTP Objects
- HTTP Statistics
- HTTP Response Time
- Overview of HTTP/2
- HTTP/2 Analysis Fundamentals
- HTTP /2 Frame Format
- Analyze Normal/Problem HTTP Traffic

**17. Analyze TLS-Encrypted Traffic (HTTPS)**

- Analyze HTTPS Traffic
- Encrypted Alerts
- Decryption Steps
- Filter on SSL

**18. Review Your 10 Key Troubleshooting Steps**

- Baseline "NormalTraffic
- Use Color
- Look Who's Talking: Examine Conversations and Endpoints
- Focus by Filtering
- Create Basic IO Graphs
- Examine Delta Time Values
- Examine the Expert System
- Follow the Streams
- Graph Bandwidth Use, Round Trip Time, and TCP Time/Sequence Information
- Watch Refusals and Redirections

## Virtual Classroom Live Labs

Lab 1: Capture Traffic to/from Your Hardware Address

Lab 2: Create Your Troubleshooting Profile

Lab 3: Set Basic Preferences for Your Troubleshooting Profile

Lab 4: Find, Mark, Save, and Colorize Packets

Lab 5: Detect and Colorize High Latency Indications

Lab 6: Find the Top Talkers and Protocols/Applications on a Network

Lab 7: Create and Use an IO Graph to Spot Performance Issues

Lab 8: Locate a Text String in a Trace File

Lab 9: Create a Coloring Rule to Detect DNS Error Responses and Suspicious DNS Responses

Lab 10: Analyze a Network Problem Indicated by ARP

Lab 11: Filter on a Range of IPv4 Addresses

Lab 12: Detect Suspicious Traffic with a New ICMP Coloring Rule

Lab 13: Analyze UDP-Based Multicast Streams and Queuing Delays

Lab 14: Use an IO Graph to Locate TCP Performance Issues

Lab 15: Determine Who is at Fault and Work with Multiple Trace Files

Lab 16: Determine the Cause of Slow File Downloads

Lab 17: Use TCP Graphs to Detect the Cause of Performance Problems

Lab 18: Create a Filter Expression Button to Detect HTTP Error Responses

Lab 19: Export an HTTP Object

Lab 20: Decrypt HTTPS Communications

skillsoft global knowledge™

# TROUBLESHOOTING TCP/IP NETWORKS WITH WIRESHARK

Course Code: 9879

| | | |
|---|---|---|
| VIRTUAL CLASSROOM LIVE | $5,063 CAD | 5 Day |

Jul 21 - 25, 2025 | 8:30 AM - 4:30 PM EDT

# TROUBLESHOOTING TCP/IP NETWORKS WITH WIRESHARK

Course Code: 9879

| | |
|---|---|
| PRIVATE GROUP TRAINING | 5 Day |

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 4/17/2025 10:48:58 AM