



Troubleshooting TCP/IP Networks with Wireshark

- 3 Days
- Lecture and Hands-on Labs

Course Overview

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.

Who Should 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.





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
-










Outline

Wireshark Traffic Analysis Labs






-  Lecture + Lab: Installing Wireshark
-  Lecture + Lab: TCP/IP Analysis Checklist
-  Lecture + Lab: Top Causes of Performance Problems
-  Lecture + Lab: Capturing Traffic

-  Lecture + Lab: Opening Trace Files
-  Lecture + Lab: Processing Packets
-  Lecture + Lab: Master the Intelligent Scrollbar
-  Lecture + Lab: Your First Task When You Leave Class

Learn Capture Methods and Use Capture Filters

-  Lecture: Analyze Switched Networks
-  Lecture + Lab: Walk-Through a Sample SPAN Configuration
-  Lecture + Lab: Analyze Full-Duplex Links with a Network TAP
-  Lecture + Lab: USB Capture
-  Lecture: Initial Analyzing Placement
-  Lecture + Lab: Remote Capture Techniques
-  Lecture + Lab: Available Capture Interfaces
-  Lecture + Lab: Save Directly to Disk
-  Lecture + Lab: Examine Key Capture Filters

Customize for Efficiency: Configure Your Global Preferences

-  Lecture + Lab: First Step: Create a Troubleshooting Profile
-  Lecture + Lab: Customize the User Interface
-  Lecture + Lab: Set Your Global Capture Preferences
-  Lecture + Lab: Define Name Resolution Preferences
-  Lecture + Lab: Configure Individual Protocol Preferences










Navigate Quickly and Focus Faster with Coloring Techniques

-  Lecture + Lab: Move Around Quickly: Navigation Techniques
-  Lecture: Build Permanent Coloring Rules






Spot Network and Application Issues with Time Values and Summaries



-  Lecture + Lab: Examine the Delta Time (End-of-Packet to End-of-Packet)
-  Lecture + Lab: Compare Timestamp Values
-  Lecture + Lab: Compare Timestamps of Filtered Traffic
-  Lecture + Lab: Compare TCP Conversation Timestamp Values

Create and Interpret Basic Trace File Statistics








-  Lecture + Lab: Examine Trace File Summary Information
-  Lecture + Lab: View Active Protocols
-  Lecture + Lab: Graph Throughput to Spot Performance Problems
-  Lecture + Lab: Quickly Locate the Most Active Conversations and Endpoints
-  Lecture: Numerous Other Statistics are Available
-  Lecture: Quick Overview of VoIP Traffic Analysis
-  Lecture + Lab: SIP and RTP Analysis Overview
-  Lecture + Lab: SIP Call Setup
-  Lecture + Lab: Session Bandwidth and RTP Port Definition

Focus on Traffic Using Display Filters





-  Lecture + Lab: Filter on Conversations/Endpoints
-  Lecture + Lab: Build Filters Based on Packets
-  Lecture + Lab: Display Filter Syntax
-  Lecture + Lab: Use Comparison Operators and Advanced Filters
-  Lecture + Lab: Filter on Text Strings

-  Lecture: Watch for Common Display Filter Mistakes
-  Lecture + Lab: Share Your Display Filters

TCP/IP Communications and Resolutions Overview

-  Lecture: Ethernet Packet and Frame
-  Lecture + Lab: TCP/IP Functionality
-  Lecture: When Everything Goes Right
-  Lecture: The Multi-Step Resolution Process
-  Lecture + Lab: Resolution Helped Build the Packet
-  Lecture + Lab: Where Faults Can Occur
-  Lecture: Typical Causes of Slow Performance







Analyze DNS Traffic

-  Lecture + Lab: DNS Packet Structure
-  Lecture + Lab: DNS Queries
-  Lecture + Lab: Filter on DNS Traffic
-  Lecture + Lab: Analyze Normal/Problem DNS Traffic

Analyze ARP Traffic

-  Lecture: ARP Overview
- ARP Packet Structure




Analyze IPv4 Traffic

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










Analyze ICMP Traffic






-  Lecture + Lab: ICMP Overview
-  Lecture + Lab: Watch for Service Refusals

Analyze UDP Traffic





-  Lecture: UDP Overview
-  Lecture + Lab: Filter on UDP Traffic
-  Lecture + Lab: Follow UDP Streams to Reassemble Data

Analyze TCP Protocol












-  Lecture: TCP Overview
-  Lecture + Lab: The TCP Connection Process
-  Lecture + Lab: TCP Handshake Problem
-  Lecture + Lab: Watch Service Refusals
-  Lecture + Lab: The TCP Sequencing/Acknowledgment Process
-  Lecture + Lab: Packet Loss Detection in Wireshark
-  Lecture + Lab: Fast Recovery/Fast Retransmission Detection in Wireshark
-  Lecture + Lab: Out-of-Order Segment Detection in Wireshark
-  Lecture + Lab: Selective Acknowledgement (SACK)

-  Lecture + Lab: Window Scaling
-  Lecture + Lab: Window Size Issues: Scaling and Receive Buffer Limitations
-  Lecture + Lab: TCP Sliding Window Overview
-  Lecture + Lab: Troubleshoot TCP Quickly with Expert Info
-  Lecture + Lab: Properly Set TCP Preferences

Graph Traffic Characteristics

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

Analyze HTTP Traffic

-  Lecture + Lab: Display Macros
-  Lecture + Lab: HTTP Overview
-  Lecture + Lab: HTTP Packet Structure
-  Lecture + Lab: Reassembling HTTP Objects
-  Lecture + Lab: HTTP Statistics
-  Lecture + Lab: HTTP Response Time
-  Lecture: Decoding SSL Traffic with Wireshark
-  Lecture + Lab: Overview of HTTP/2
-  Lecture: HTTP/2 Analysis Fundamentals
-  Lecture + Lab: HTTP/2 Frame Format
-  Lecture + Lab: Analyze Normal/Problem HTTP Traffic

Analyze TLS-Encrypted Traffic (HTTPS)

-  Lecture + Lab: Analyze HTTPS Traffic

Quick Start

-  Lecture: Wireshark Cheatsheet