Introduction to Troubleshooting TCP/IP Networks with Wireshark

Course WIRE-1B 5 Days Instructor-led, Hands-on

Introduction

In this hands-on, instructor-led, five-day course, you will receive in-depth training on Wireshark and TCP/IP communications analysis. You will learn to use Wireshark to identify the most common causes of performance problems in TCP/IP communications. You will develop a thorough understanding of how to use Wireshark efficiently to spot the primary sources of network performance problems.

At Course Completion

After completing this course, students will 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

Prerequisites

Before attending this course, students must have attended:

- CompTIA Network+

Course Materials

The student kit includes a comprehensive workbook and other required materials for this class.

Course Outline

Module 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
- GTK Interface
- The Icon Toolbar
- Mastering the Intelligent Scrollbar
- The Changing Status Bar
- Right-Click Functionality
- General Analyst Resources
- Your First Task When You Leave Class

Module 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

Module 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

Contact ISInc for more information at 916.920.1700 or by visiting our website at http://www.isinc.com

- Configure Individual Protocol Preferences

Module 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
- Apply Temporary Coloring
- Mark Packets of Interest

Module 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
- Troubleshooting Example Using Time
- Analyze Delay Types

Module 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
- Bust Statistics
- Numerous Other Statistics are Available
- Quick Overview of VoIP Traffic Analysis Tools
- SIP and RTP Analysis Overview
- SIP Call Setup
- Analyzing Call Setup with SIP
- Session Bandwidth and RTP Port Definition

Module 7: Focus on Traffic Using Display Filters

- Display Filters
- Filter on Conversations/Endpoints
- Build Filters Based on Packets
- Display Filter Syntax

Contact ISInc for more information at 916.920.1700 or by visiting our website at http://www.isinc.com

- 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

Module 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

Module 9: Analyze DNS Traffic

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

Module 10: Analyze ARP Traffic

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

Module 11: Analyze Ipv4 Traffic

- IP4 Overview
- Ipv4 Packet Structure
- Analyze Broadcast/Multicast Traffic
- Filter o Ipv4 Traffic
- IP Protocol Preferences
- Analyze Normal/Problem IP Traffic

Module 12: Analyze ICMP Traffic

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

Module 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

Module 14: Analyze TCP Protocol

- TCP Overview
- Watch for Service Refusals
- UDP Packet Structure
- Filter on UDP Traffic
- Follow UDP Streams to Reassemble Data
- Analyze Normal/Problem UDP Traffic

Module 15: Analyze TCP Protocol

- TCP Overview
- The TCP Connection Process
- TCP Handshake Problem
- Watch Service Refusals
- TCP Packet Structure
- The TCP Sequencing/Acknowledgement 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 Acknowledgment (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

Contact ISInc for more information at 916.920.1700 or by visiting our website at http://www.isinc.com

Module 16: Graph Traffic Characteristics

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

Module 17: 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

Module 18: Analyze TLS-Encrypted Traffic (HTTPS)

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

Module 19: Review Your Key Troubleshooting Steps

- Baseline “Normal Traffic
- 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