Wireshark

Course 5442 – 24 Hours

Overview

In this hands-on 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, and you will prepare for the latest Wireshark certification exam.

Who Should Attend

מתאים לאנשי תמיכה טכנית, טכנאי שטח, אנשי מכירות, מנהלי תיקי לקוחות (Account managers), מנהלי צוותי מכירות בתחום התקשורת, מנהלי שיווק בתחום התקשורת והייטק, מנהלי פיתוח עסקי , מנהלי רכש והדרכה.

Prerequisites

- הקורס אינו דורש ידע מוקדם

Course Contents

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 Icon Toolbar
- The Changing Status Bar
- General Analyst Resources

2. Learn Capture Methods and Use Capture Filters

- Checksum Issues at Capture
- Analyze Switched Networks
- Walk-Through a Sample SPAN Configuration
- 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. 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

4. 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

5. 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
- Numerous Other Statistics are Available
- Quick Overview of VoIP Traffic Analysis Tools

6. 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
- Manually Edit the dfilters File

7. 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

8. Analyze DNS Traffic

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

9. Analyze ARP Traffic

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

10. Analyze IPv4 Traffic

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

11. Analyze ICMP Traffic

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

12. 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

13. 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
- 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
- Filter on TCP Traffic and TCP Problems
- Properly Set TCP Preferences
- Follow TCP Streams to Reassemble Data

14. Examine Advanced Trace File Statistics

- Build Advanced IO Graphs
- Graph Round Trip Times
- Graph TCP Throughput
- Find Problems Using TCP Time-Sequence Graphs

15. Analyze HTTP Traffic

- HTTP Overview
- HTTP Packet Structure
- Filter on HTTP Traffic
- Reassembling HTTP Objects
- HTTP Statistics
- Analyze Normal/Problem HTTP Traffic

16. Analyze SSL-Encrypted Traffic (HTTPS)

- Examining SSL/HTTPS Traffic
- Filter on SSL

17. Analyze File Transfer Protocol (FTP) Traffic

- FTP Overview
- FTP Packet Structure
- Analyze Active Mode Connections
- Analyze Passive Mode Connections
- Filter on FTP Traffic
- Analyze Normal/Problem FTP Traffic