Troubleshooting TCP/IP Networks With Wireshark Course Outline

1. Introduction to Network Analysis and Wireshark
    a. TCP/IP Analysis Checklist
    b. Top Causes of Performance Problems
    c. Get the Latest Version of Wireshark
    d. Capturing Traffic
    e. Opening Trace Files
    f. Processing Packets
    g. GTK Interface
    h. The Icon Toolbar
    i. The Changing Status Bar
    j. Right-Click Functionality
    k. General Analyst Resources
    l. Your First Task When You Leave Class
2. Learn Capture Methods and Use Capture Filters

. Checksum Issues at Capture
    a. Analyze Switched Networks
    b. Walk-Through a Sample SPAN Configuration
    c. Analyze Full-Duplex Links with a Network TAP
    d. Analyze Wireless Networks
    e. Initial Analyzing Placement
    f. Remote Capture Techniques
    g. Available Capture Interfaces
    h. Save Directly to Disk
    i. Capture File Configurations
    j. Limit Your Capture with Capture Filters
    k. Examine Key Capture Filters

3. Customize for Efficiency: Configure Your Global Preferences

. First Step: Create a Troubleshooting Profile
    a. Customize the User Interface
    b. Add Custom Columns for the Packet List Pane
    c. Set Your Global Capture Preferences
    d. Define Name Resolution Preferences

  e. Configure Individual Protocol Preferences

4. Navigate Quickly and Focus Faster with Coloring Techniques

. Move Around Quickly: Navigation Techniques

  a. Find a Packet Based on Various Characteristics

  b. Build Permanent Coloring Rules

  c. Identify a Coloring Source

  d. Apply Temporary Coloring

  e. 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)

  a. Set a Time Reference

  b. Compare Timestamp Values

  c. Compare Timestamps of Filtered Traffic

  d. Enable and Use TCP Conversation Timestamps

  e. Compare TCP Conversation Timestamp Values

  f. Troubleshooting Example Using Time

  g. Analyze Delay Types

6. Create and Interpret Basic Trace File Statistics

. Examine Trace File Summary Information

  a. View Active Protocols

  b. Graph Throughput to Spot Performance Problems Quickly

  c. Locate the Most Active Conversations and Endpoints

  d. Other Conversation Options

  e. Graph the Traffic Flows for a More Complete View

  f. Numerous Other Statistics are Available

  g. Quick Overview of VoIP Traffic Analysis Tools

7. Focus on Traffic Using Display Filters

. Display Filters

  a. Filter on Conversations/Endpoints

  b. Build Filters Based on Packets

  c. Display Filter Syntax

  d. Use Comparison Operators and Advanced Filters

  e. Filter on Text Strings

  f. Build Filters Based on Expressions

g. Watch for Common Display Filter Mistakes

h. Manually Edit the dfilters File

8. Effectively Use Command-Line Tools

. TShark and Dumpcap Command-Line Tools

a. Capinfos Command-Line Tool

b. Editcap Command-Line Tool

c. Mergecap Command-Line Tool

d. Text2pcap Command-Line Tool

e. Split and Merge Trace Files

9. TCP/IP Communications and Resolutions Overview

. TCP/IP Functionality

a. When Everything Goes Right

b. The Multi-Step Resolution Process

c. Resolution Helped Build the Packet

d. Where Faults Can Occur

e. Typical Causes of Slow Performance

10. Analyze DNS Traffic

. DNS Overview

a. DNS Packet Structure

b. DNS Queries

c. Filter on DNS Traffic

d. Analyze Normal/Problem DNS Traffic

11. Analyze ARP Traffic

. ARP Overview

a. ARP Packet Structure

b. Filter on ARP Traffic

c. Analyze Normal/Problem ARP Traffic

12. Analyze IPv4 Traffic

. IPv4 Overview

a. IPv4 Packet Structure

b. Analyze Broadcast/Multicast Traffic

c. Filter on IPv4 Traffic

d. IP Protocol Preferences

e. Analyze Normal/Problem IP Traffic

13. Analyze ICMP Traffic

. ICMP Overview

a. ICMP Packet Structure

b. Filter on ICMP Traffic

c. Analyze Normal/Problem ICMP Traffic

14. Analyze UDP Traffic

. UDP Overview

a. Watch for Service Refusals

b. UDP Packet Structure

c. Filter on UDP Traffic

d. Follow UDP Streams to Reassemble Data

e. Analyze Normal/Problem UDP Traffic

15. Analyze TCP Protocol

. TCP Overview

a. The TCP Connection Process

b. TCP Handshake Problem

c. Watch Service Refusals

d. TCP Packet Structure

e. The TCP Sequencing/Acknowledgment Process

f. Packet Loss Detection in Wireshark

g. Fast Recovery/Fast Retransmission Detection in Wireshark

h. Retransmission Detection in Wireshark

i. Out-of-Order Segment Detection in Wireshark

j. Selective Acknowledgement (SACK)

k. Window Scaling

l. Window Size Issue: Receive Buffer Problem

m. Window Size Issue: Unequal Window Size Beliefs

n. TCP Sliding Window Overview

o. Troubleshoot TCP Quickly with Expert Info

p. Filter on TCP Traffic and TCP Problems

q. Properly Set TCP Preferences

r. Follow TCP Streams to Reassemble Data

16. Examine Advanced Trace File Statistics

. Build Advanced IO Graphs

a. Graph Round Trip Times

b. Graph TCP Throughput

c. Find Problems Using TCP Time-Sequence Graphs

17. Analyze HTTP Traffic

. HTTP Overview

a. HTTP Packet Structure

b. Filter on HTTP Traffic

c. Reassembling HTTP Objects

d. HTTP Statistics

e. Analyze Normal/Problem HTTP Traffic

18. Analyze SSL-Encrypted Traffic (HTTPS)

. Examining SSL/HTTPS Traffic

a. Wireshark v1.6.0 Bug Alert #201106

b. Filter on SSL

19. Analyze File Transfer Protocol (FTP) Traffic

. FTP Overview

a. FTP Packet Structure

b. Analyze Active Mode Connections

c. Analyze Passive Mode Connections

d. Filter on FTP Traffic

e. Analyze Normal/Problem FTP Traffic

20. Your 10 Key Troubleshooting Steps

. Baseline "NormalTraffic

a. Use Color

b. Look Who's Talking: Examine Conversations and Endpoints

c. Focus by Filtering

d. Create Basic IO Graphs

e. Examine Delta Time Values

f. Examine the Expert System

g. Follow the Streams

h. Graph Bandwidth Use, Round Trip Time, and TCP Time/Sequence Information

i. Watch Refusals and Redirections

21. LABS

. Capture Traffic to/from Your Hardware Address

a. Create Your Troubleshooting Profile

b. Set Basic Preferences for Your Troubleshooting Profile

c. Find, Mark, Save, and Colorize Packets

d. Detect and Colorize High Latency Indications

e. Find the Top Talkers and Protocols/Applications on a Network

f. Create and Use an IO Graph to Spot Performance Issues

g. Locate a Text String in a Trace File

h. Use Tshark to Capture Traffic to/from Other Hosts on the Network

i. Split a Large Trace File Based on Time-Per-File and Merge Trace Files

j. Create a Coloring Rule to Detect DNS Error Responses and Suspicious DNS Responses

k. Analyze a Network Problem Indicated by ARP

l. Filter on a Range of IPv4 Addresses

m. Detect Suspicious Traffic with a New ICMP Coloring Rule

n. Analyze UDP-Based Multicast Streams and Queuing Delays

o. Alter Coloring of Window Update Packets

p. Use TCP Timestamps and New Coloring Rules to Locate TCP Performance Issues and Questionable Window Sizes

q. Determine Who is at Fault and Work with Multiple Trace Files

r. Determine the Cause of Slow File Downloads

s. Use TCP Graphs to Detect the Cause of Performance Problems

t. Create a Coloring Rule for HTTP Error Responses

u. Export an HTTP Object

v. Decrypt HTTPS Communications

w. Analyze FTP Problems