



WSU01: Wireshark Functionality and Fundamentals

Learn to use Wireshark efficiently and effectively by placing your analyzer in an ideal location to capture traffic (even on a switched network). Learn to focus on key traffic using capture filters and display filters. Graph traffic, use navigation and colorization techniques and time values to easily spot network problems. Customize your Wireshark system and use the Expert system to identify problem areas. Learn how tshark, editcap, capinfos and other command-line tools work and test yourself by completing lab exercises.

Course Contents

Course Overview – Introduction

Section 1: Introduction to Wireshark

- Module A. History, Authors and License
- Module B. How Wireshark Works
- Module C. Wireshark Folders, Plugins and Help
- Module D. Resources and References for Analysts

Section 2: Capturing Packets

- Module A. Select an Active Interface
- Module B. Capture to a File
- Module C. Capture to a Ring Buffer
- Module D. Open and Work with File Sets
- Module E. Default Capture Filters
- Module F. Create New Capture Filters
- Module G. Avoid Dropped Packets
- Module H. Test Yourself

Section 3: Configuring Global Preferences

- Module A. Customize the User Interface
- Module B. Set Global Capture Preferences
- Module C. Define Name Resolution Preferences
- Module D. Alter Protocol Settings
- Module E. Key Preference Settings

Section 4: Navigation and Colorization Techniques

- Module A. Go to a Specific Packet Number
- Module B. Find Packets Based on Payload Values
- Module C. Sort Columns
- Module D. Use and Customize Packet Colors
- Module E. Mark Packets
- Module F. Show a Packet in a New Window
- Module G. Test Yourself

Section 5: Using Time Values and Summaries

- Module A. Use the Default Time Column Setting and Precision
- Module B. Use Time between Packets
- Module C. Set a Time Reference and View Capture Time
- Module D. Troubleshooting with Time
- Module E. Analyze Summary Information
- Module F. Test Yourself

Section 6: Examining Basic Trace File Statistics

- Module A. Examine Protocol Hierarchies
- Module B. View Network Connections
- Module C. View Network Endpoints
- Module D. Evaluate Destinations
- Module E. View IP Address Information
- Module F. Evaluate Packet Lengths
- Module G. Evaluate Port Types
- Module H. Examine Multicast Streams and Settings
- Module I. Test Yourself

Section 7: Advanced Trace File Statistics

- Module A. Create IO Graphs
- Module B. Create TCP Time-Sequence Graphs
- Module C. Analyze Flow Graphs
- Module D. Evaluate Service Response Times
- Module E. Analyze BOOTP/DHCP Statistics
- Module F. View HTTP Statistics
- Module G. Create Round-Trip Time Graphs

Section 8: Creating Display Filters

- Module A. Follow a TCP Stream
- Module B. Create Filters from Conversations and Endpoints
- Module C. Default Display Filters and Filter Syntax
- Module D. Build and Save Filters Based on Packets
- Module E. Filter on Payload Bytes
- Module F. Use Expressions to Build Display Filters
- Module G. Use Boolean Operands and Negatives
- Module H. The 10 Most Useful Filters
- Module I. Manually Edit the Filter File

Section 9: Save, Export and Print

- Module A. Save Filtered, Marked and Ranges of Packets
- Module B. Chart Conversation/Endpoint/Flow Graph Information
- Module C. Save and Reassemble Data Streams
- Module D. Export Packet Information
- Module E. Print Packets
- Module F. Capture/Edit Screen Shot

Section 10: Expert System and Miscellaneous Tasks

- Module A. Use Expert Information
- Module B. Analyze Firewall ACL Rules
- Module C. Protocol Forcing
- Module D. Merging Files
- Module E. Zoom, Autoscroll and Resizing Columns

Section 11: Using Command-Line Tools

Module A. tshark and dumpcap

Module B. capinfos

Module C. editcap

Module D. mergecap

Module E. text2pcap

Appendix A: Wireshark Lab Exercises

Appendix B: Trace File Catalog

Appendix C: Command-Line Tools Reference

Appendix D: Wireshark University Course List