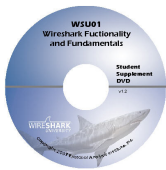




WSU01 [Self-Paced Course]

Wireshark Functionality and Fundamentals



Course Format

This course is available only in self-paced format (voice-over-video) taught by **Laura Chappell**. The course DVD includes videos, supplemental files (in PDF format) and reference/resource materials for the network analyst.

Course Content

Learn how to use Wireshark efficiently and effectively by placing Wireshark in the ideal location to capture traffic (even on a switched network). Learn to focus on key traffic using filters and display your results with Wireshark's graphs.

Course Overview - Introduction

- Section 1: Introduction to Wireshark
- a) History, Authors and License
 - b) How Wireshark Works
 - c) Wireshark Folders, Plugins and Help
 - d) Resources and References for Analysts
 - e) CACE Technologies - AirPcap
 - f) Capture on Hubbed, Switched and Routed Networks
- Section 2: Capturing Packets
- a) Select an Active Interface
 - b) Capture to a File
 - c) Capture to a Ring Buffer
 - d) Open and Work with File Sets
 - e) Default Capture Filters
 - f) Create New Capture Filters
 - g) Avoid Dropped Packets
 - h) Test Yourself
- Section 3: Configuring Global Preferences
- a) Customize the User Interface
 - b) Set Global Capture Preferences
 - c) Define Name Resolution Preferences
 - d) Alter Protocol Settings
 - e) My Favorite Preferences



- Section 4: Navigation and Colorization Techniques
- a) Go To a Specific Packet Number
 - b) Find Packets Based on Payload
 - c) Sort Columns
 - d) Use and Customize Packet Colors
 - e) Mark Packets
 - f) Show a Packet in a New Window
 - g) Test Yourself
- Section 5: Using Time Values and Summaries
- a) Use the Default Time Column Setting and Precision
 - b) Use Time Between Packets
 - c) Set a Time Reference and View Capture Time
 - d) Troubleshooting with Time
 - e) Analyze Summary Information
 - f) Test Yourself
- Section 6: Examining Basic Trace File Statistics
- a) Examine Protocol Hierarchies
 - b) View Network Connections
 - c) View Network Endpoints
 - d) Evaluate Destinations
 - e) View IP Address Information
 - f) Evaluate Packet Lengths
 - g) Evaluate Port Types
 - h) Examine Multicast Streams and Settings
 - i) Test Yourself
- Section 7: Examining Advanced Trace File Statistics
- a) Create IO Graphs
 - b) Create TCP Time-Sequence Graphs
 - c) Analyze Flow Graphs
 - d) Evaluate Service Response Times
 - e) Analyze BOOTP/DHCP Statistics
 - f) View HTTP Statistics
 - g) Create Round-Trip Time Graphs
- Section 8: Creating Display Filters
- a) Follow a TCP Stream
 - b) Create Filters from Conversations and Endpoints
 - c) Default Display Filters and Filter Syntax
 - d) Build and Save Filters Based on Packets
 - e) Filter on Payload Bytes
 - f) Use Expressions to Build Display Filter
 - g) Use Boolean Operands and Negatives
 - h) The 10 Most Useful Filters
 - i) Manually Edit the Filter File



- Section 9: Save, Export and Print
- a) Save Filtered, Marked and Ranges of Packets
 - b) Chart Conversation/Endpoint/Flow Graph Information
 - c) Save and Reassemble Data Streams
 - d) Export Packet Information
 - e) Print Packets
 - f) Capture/Edit Screen Shots for Reports
- Section 10: Expert System and Miscellaneous Tasks
- a) Use Expert and Expert Info Composite Information
 - b) Analyze ACL Firewall Rules
 - c) Protocol Forcing
 - d) Merging Files
 - e) Zoom, Autoscroll and Resizing Columns
- Section 11: Using Command-Line Tools
- a) tshark and dumpcap
 - b) capinfos
 - c) editcap
 - d) mergecap
 - e) text2pcap

Recommended Course Prerequisites

Learn how to use Wireshark efficiently and effectively by placing Wireshark in the ideal location to capture traffic (even on a switched network). Learn to focus on key traffic using filters and display your results with Wireshark's graphs.

This is an introductory class. Minimal prerequisites apply.

Recommended prerequisite knowledge:

- Basic networking components (hubs, switches, routers)
- IP network address structure
- General TCP/IP protocol and applications

Note: This course is a recommended prerequisite course for Wireshark University Courses WSU03 (Troubleshooting Network Performance) and WSU04 (Network Forensics and Security)