



Wireshark University

Course Information

- WSU01: Wireshark Functionality and Fundamentals**
- WSU02: TCP/IP Network Analysis**
- WSU03: Troubleshooting Network Performance**
- WSU04: Network Forensics and Security**



WSU01

Wireshark Functionality and Fundamentals

Self-Paced Course Format

Self-paced courses are available on DVD through www.wiresharkU.com and include voice-over-video instruction by Laura Chappell, Founder of Wireshark University. Course DVD includes supplement files (PDF format), lab trace files, general trace files and research supplements.

Instructor-Led Course Format

Instructor-led courses are offered through Wireshark University (www.wiresharkU.com) and are taught in a BYOL (Bring Your Own Laptop) style - bring your laptop preloaded with the latest version of Wireshark and you're ready to go!

WSU01 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
- Go To a Specific Packet Number
 - Find Packets Based on Payload
 - Sort Columns
 - Use and Customize Packet Colors
 - Mark Packets
 - Show a Packet in a New Window
 - Test Yourself
- Section 5: Using Time Values and Summaries
- Use the Default Time Column Setting and Precision
 - Use Time Between Packets
 - Set a Time Reference and View Capture Time
 - Troubleshooting with Time
 - Analyze Summary Information
 - Test Yourself
- Section 6: Examining Basic Trace File Statistics
- Examine Protocol Hierarchies
 - View Network Connections
 - View Network Endpoints
 - Evaluate Destinations
 - View IP Address Information
 - Evaluate Packet Lengths
 - Evaluate Port Types
 - Examine Multicast Streams and Settings
 - Test Yourself
- Section 7: Examining Advanced Trace File Statistics
- Create IO Graphs
 - Create TCP Time-Sequence Graphs
 - Analyze Flow Graphs
 - Evaluate Service Response Times
 - Analyze BOOTP/DHCP Statistics
 - View HTTP Statistics
 - Create Round-Trip Time Graphs
- Section 8: Creating Display Filters
- Follow a TCP Stream
 - Create Filters from Conversations and Endpoints
 - Default Display Filters and Filter Syntax
 - Build and Save Filters Based on Packets
 - Filter on Payload Bytes
 - Use Expressions to Build Display Filter
 - Use Boolean Operands and Negatives
 - The 10 Most Useful Filters
 - 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)



WSU02

TCP/IP Network Analysis

Self-Paced Course Format

Self-paced courses are available on DVD through www.wiresharkU.com and include voice-over-video instruction by Laura Chappell, Founder of Wireshark University. Course DVD includes supplement files (PDF format), lab trace files, general trace files and research supplements.

Instructor-Led Course Format

Instructor-led courses are offered through Wireshark University (www.wiresharkU.com) and are taught in a BYOL (Bring Your Own Laptop) style - bring your laptop preloaded with the latest version of Wireshark and you're ready to go!

WSU02 Course Content

This course focuses on both the normal and abnormal communication patterns of the TCP/IP suite and most common applications including DHCP, DNS, FTP, Telnet, HTTP, POP and SMTP.

Course Overview - Introduction

- Section 1: TCP/IP Functionality Overview
 - a) Resources and References for Analysts
 - b) Capture on Hubbed, Switched and Routed Networks
 - c) The TCP/IP Resolution Process
 - d) Packets Going the Wrong Way
 - e) Faults in the Resolution Process
 - f) Test Yourself: What If...

- Section 2: Analyze DNS Traffic
 - a) Understand DNS Packet Structure
 - b) Filter on DNS Traffic
 - c) Analyze Normal DNS Traffic
 - d) Analyze Unusual DNS Traffic

- Section 3: Analyze ARP Traffic
 - a) Understand ARP Packet Structure
 - b) Filter on ARP Traffic
 - c) Analyze Normal ARP Traffic
 - d) Analyze Unusual ARP Traffic

- Section 4: Analyze IPv4 Traffic
 - a) Understand IPv4 Packet Structure
 - b) Filter on IPv4 Traffic
 - c) Analyze Normal IPv4 Traffic
 - d) Analyze Unusual IPv4 Traffic



- Section 5: Analyze ICMP Traffic
 - a) Understand ICMP Packet Structure
 - b) Filter on ICMP Traffic
 - c) Analyze Normal ICMP Traffic
 - d) Analyze Unusual ICMP Traffic

- Section 6: Analyze UDP Traffic
 - a) Understand UDP Packet Structure
 - b) Filter on UDP Traffic
 - c) Analyze Normal UDP Traffic
 - d) Analyze Unusual UDP Traffic

- Section 7: Analyze TCP Traffic
 - a) Understand TCP Packet Structure
 - b) Filter on TCP Traffic
 - c) Analyze Normal TCP Traffic
 - d) Analyze Unusual TCP Traffic

- Section 8: Analyze DHCP Traffic
 - a) Understand DHCP Packet Structure
 - b) Filter on DHCP Traffic
 - c) Analyze Normal DHCP Traffic
 - d) Analyze Unusual DHCP Traffic

- Section 9: Analyze HTTP Traffic
 - a) Understand HTTP Packet Structure
 - b) Filter on HTTP Traffic
 - c) Analyze Normal HTTP Traffic
 - d) Analyze Unusual HTTP Traffic

- Section 10: Analyze Telnet Traffic
 - a) Understand Telnet Packet Structure
 - b) Filter on Telnet Traffic
 - c) Analyze Normal Telnet Traffic
 - d) Analyze Unusual Telnet Traffic

- Section 11: Analyze FTP Traffic
 - a) Understand FTP Packet Structure
 - b) Filter on FTP Traffic
 - c) Analyze Normal FTP Traffic
 - d) Analyze Unusual FTP Traffic



- Section 12: Analyze POP Traffic
- a) Understand POP Packet Structure
 - b) Filter on POP Traffic
 - c) Analyze Normal POP Traffic
 - d) Analyze Unusual POP Traffic

- Section 13: Analyze SMTP Traffic
- a) Understand SMTP Packet Structure
 - b) Filter on SMTP Traffic
 - c) Analyze Normal SMTP Traffic
 - d) Analyze Unusual SMTP Traffic

Recommended Course Prerequisites

This course focuses on both the normal and abnormal communication patterns of the TCP/IP suite and most common applications including DHCP, DNS, FTP, Telnet, HTTP, POP and SMTP.

Recommended prerequisite knowledge:

- Basic network components (hubs, switches, routers)
- IP network address structure
- Wireshark functionality and features (see Wireshark University Course WSU01)
 - Navigation
 - Packet detail tree expansion
 - Capture traffic
 - Display filtering on protocol or field
 - Create basic Wireshark graphs
 - Save packets based on filters, markers or range value



Note:

If you cannot check off at 70% of the items listed in the prerequisite checklist, we recommend you attend WSU01: Wireshark Functionality and Fundamentals.

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



WSU03

Troubleshooting Network Performance

Self-Paced Course Format

Self-paced courses are available on DVD through www.wiresharkU.com and include voice-over-video instruction by Laura Chappell, Founder of Wireshark University. Course DVD includes supplement files (PDF format), lab trace files, general trace files and research supplements.

Instructor-Led Course Format

Instructor-led courses are offered through Wireshark University (www.wiresharkU.com) and are taught in a BYOL (Bring Your Own Laptop) style - bring your laptop preloaded with the latest version of Wireshark and you're ready to go!

WSU03 Course Content

This course focuses on the causes of poor network performance including packet-loss, retransmissions, high latency, low throughput rates, minimal bandwidth, application errors, configuration faults, resolution problems and protocol behavior problems.

- Section 1: Analyzer Placement
 - a) Analyzing Hubbed Networks
 - b) Analyzing Switched Networks
 - c) Analyzing Routed Networks
 - d) Analyzing WAN Links
 - e) Capturing in Stealth Mode

- Section 2: Normal Network Communications
 - a) When Everything Goes Right
 - b) The Multi-Step Resolution Process
 - c) Building the Packet

- Section 3: Causes of Performance Problems
 - a) Where Network Faults Occur
 - b) Time is of the Essence

- Section 4: Wireshark Functions for Troubleshooting
 - a) Using Pre-Defined Coloring Rules
 - b) Basic and Advanced IO Graphs
 - c) Use the Delta Time Value
 - d) Analyze Expert Information
 - e) Look Who's Talking
 - f) Graph Bandwidth Use, Round Trip Time and TCP Performance
 - g) Flow Graphing
 - h) Statistics (Various)



- Section 5: Latency Issues
 - a) The Five Primary Points in Calculating Latency
 - b) Plotting High Latency Times
 - c) Free Latency Calculators
 - d) Using the frame.time_delta Filter

- Section 6: Packet Loss and Retransmissions
 - a) Packet Loss and Recovery – UDP v. TCP
 - b) Previous Segment Lost Events
 - c) Duplicate ACKs
 - d) TCP Retransmissions and Fast Retransmissions
 - e) Out-of-Order Segments

- Section 7: Misconfigurations and Redirections
 - a) Visible Misconfigurations
 - b) Don't Forget the Time

- Section 8: Dealing with Congestion
 - a) Shattered Windows
 - b) Flooded Out

- Section 9: Baseline Network Communications
 - a) Your First Task When You Leave Class

[continued]



Recommended Course Prerequisites

This course focuses on the causes of poor network performance including packet-loss, retransmissions, high latency, low throughput rates, minimal bandwidth, application errors, configuration faults, resolution problems and protocol behavior problems.

Recommended prerequisite knowledge:

- Basic network components (hubs, switches, routers)
- Traffic flows (see Wireshark University Courses WSU01 and WSU02)
- IP network address structure
- Strong knowledge of Wireshark functionality and features (see Wireshark University Course WSU01)
 - Navigation
 - Packet detail tree expansion
 - Capture traffic
 - Display filtering on protocol or field
 - Create basic Wireshark graphs and tables (IO, conversations, endpoints)
 - Save packets based on filters, markers or range value
- Strong knowledge of TCP/IP protocol and application functionality
 - Port usage and resolution
 - Name resolution (network and hardware address)
 - Route resolution
 - ICMP functionality (packet structure, functionality)
 - TCP functionality (handshake, fault tolerance, recovery)
 - DNS functionality (address lookup, errors)
 - IP functionality (addressing, fragmentation)



Note:

If you cannot check off at 70% of the items listed in the prerequisite checklist, we recommend you attend Wireshark University Courses WSU01 (Wireshark Functionality and Fundamentals) and WSU02 (TCP/IP Network Analysis).



WSU04

Network Forensics and Security

Self-Paced Course Format

Self-paced courses are available on DVD through www.wiresharkU.com and include voice-over-video instruction by Laura Chappell, Founder of Wireshark University. Course DVD includes supplement files (PDF format), lab trace files, general trace files and research supplements.

Instructor-Led Course Format

Instructor-led courses are offered through Wireshark University (www.wiresharkU.com) and are taught in a BYOL (Bring Your Own Laptop) style - bring your laptop preloaded with the latest version of Wireshark and you're ready to go!

WSU04 Course Content

This course focuses on network forensics including capture locations, stealth-mode capture, optimal capture and display filters, validating encrypted logins, identifying reconnaissance processes, locating header and payload signatures, catching penetration tests, malware behavior, backdoor communications and virus traffic.

- Section 1: Analyzer Placement
 - a) Analyzing Hubbed Networks
 - b) Analyzing Switched Networks
 - c) Analyzing Routed Networks
 - d) Analyzing WAN Links
 - e) Tapping into Full-Duplex Links
 - f) Capturing in Stealth Mode
 - g) Obtaining Evidence Using a Honeypot

- Section 2: Unusual Network Communications
 - a) Vulnerabilities in the TCP/IP Resolution Process
 - b) Route Resolution
 - c) Spotting Unacceptable Traffic

- Section 3: Reconnaissance Processes
 - a) Port Scans
 - b) Mutant Scans
 - c) IP Scans
 - d) Application Mapping
 - e) OS Fingerprinting

[continued]



- Section 4: Analyzing ICMP Traffic
 - a) ICMP Types and Codes
 - b) ICMP Discovery
 - c) Router Redirection
 - d) Dynamic Router Discovery
 - e) Service Refusal
 - f) OS Fingerprinting

- Section 5: TCP Security
 - a) TCP Segment Splicing
 - b) TCP Fake Resets

- Section 6: Address Spoofing
 - a) MAC Address Spoofing
 - b) IP Address Spoofing

- Section 7: Building Firewall ACL Rules
 - a) Overview of ACL Rule Types

- Section 8: Signatures of Attacks
 - a) Signature Locations
 - b) Header Signatures
 - c) Sequencing Signatures
 - d) Payload Signatures
 - e) Obtaining Signatures
 - f) Attacks and Exploits
 - g) Password Cracks
 - h) Denial of Service Attacks
 - i) Redirections

[continued]



Recommended Course Prerequisites

This course focuses on network forensics including capture locations, stealth-mode capture, optimal capture and display filters, validating encrypted logins, identifying reconnaissance processes, locating header and payload signatures, catching penetration tests, malware behavior, backdoor communications and virus traffic.

Recommended prerequisite knowledge:

- Basic security knowledge (resources, viruses, worms, denial of service)
- Basic and advanced network components (hubs, switches, routers, firewalls, IDS)
- Very strong knowledge of Wireshark functionality and features
 - Navigation
 - Capture filters and methods
 - Packet details (TCP/IP protocols and applications)
 - Display filtering on protocol or field or bit value
 - Search by display filter, hex value or string
 - Basic Wireshark graphs and tables (IO, conversations, endpoints)
 - Advanced Wireshark graphs (CALC, SEQ/ACK, RTT)
 - Save packets based on filters, markers or range value
- Very strong knowledge of TCP/IP protocol and application functionality
 - Port usage and resolution
 - Name resolution (network and hardware address) and route resolution
 - ICMP functionality (packet structure, functionality)
 - TCP functionality (handshake, fault tolerance, recovery)
 - DNS functionality (address lookup, errors)
 - IP functionality (addressing, fragmentation)
 - ARP functionality (structure, functionality)
 - Follow TCP Streams
 - Expert Info/Expert Info Composite interpretation



Note:

If you cannot check off at 70% of the items listed in the prerequisite checklist, we recommend you attend Wireshark University Courses WSU01 (Wireshark Functionality and Fundamentals) and WSU02 (TCP/IP Network Analysis).