eogogicsinc
Knowledge That Powers Organizations!

Course ID
WSHARK5D
Course Title
Wireshark Training: Advanced Network Analysis and Troubleshooting
Course Duration
5 days

Aimed At

Wireless and Wired Telecom and IT networking professionals who perform network assessment, traffic analysis, and enterprise-wide network troubleshooting.

Prerequisites

Understanding of the complete TCP/IP protocol stack and IP routing along with experience in deploying, managing, and operating enterprise-level networks. Prior experience with Wireshark, used for lab work in this course, is not required.

Course in a Nutshell

Wireshark is the go-to tool for gaining an in-depth understanding of network protocols, performing detailed network examination, determining traffic patterns, planning capacity and expansion, and conducting network security reviews. Due to its power and complexity, its mastery requires advanced training.

In this hands-on, vendor-agnostic workshop, you will learn how to use Wireshark with a live network to view, capture, analyze, and troubleshoot network traffic. The workshop covers protocol analysis and troubleshooting across all equipment vendors and network infrastructure types. It is taught by an engineer with extensive experience in packet-level network analysis.

Customize It!

We can customize the course to your organization's network analysis requirements.

Learn How To

- Describe the key network protocols deployed in today's wired and wireless enterprise networks. Analyzed protocols include:
  - HTTP, TCP, UDP, IP, DHCP, DNS, ICMP, Ethernet, IEEE 802.11, Bluetooth, ZigBee, and ZigBee IP.
- View and analyze network traffic.
- Capture and filter network traffic.
- Analyze previously captured network traffic.
- Develop reusable profiles for analyzing and troubleshooting network traffic.
- Interpret the Wireshark graphs and statistical reports.
- Identify and troubleshoot common network problems, including:
  - Latency.
  - Packet errors.
  - Bandwidth performance issues.

Course Outline

Wireshark Training Part 1: Wireshark Basics

- Introduction to Wireshark
- When to use Wireshark
- Where to physically connect
- Wireshark Graphical User Interface
- Capturing network traffic

Labs:

- Install Wireshark
- Explore Wireshark installation
- Capture and save network traffic
- Understanding the packet details pane

Wireshark Training Part 2: Viewing Network Protocols with Wireshark

- Capture filters
- Display filters
- Preferences
- Time stamps
- Mark and ignore packets
- Import and export packet captures

Labs:

- Capture filters
- Display filters

Wireshark Training Part 3: Analysis Tools and Troubleshooting Techniques

- Troubleshooting methodology
- Configuration profiles
- Preferences
- Creating coloring rules
- Establishing a baseline
    - Leveraging Wireshark statistical reports and graphs

Labs:

- Custom profile
- Coloring rules
- Traffic baselines

Wireshark Training Part 4: Analyzing and Troubleshooting Layer 2 Protocols

- Ethernet frames
- MAC addresses
- ARP request/response procedure
- STP
    - BPDU format
    - Bridge selection
    - Port states
- VLANs
    - 802.1Q frame encapsulation

Labs:

- Ethernet
- ARP
- STP
- 802.1Q

Wireshark Training Part 5: Analyzing and Troubleshooting Wireless Protocols

- How to sniff wireless networks
- 802.11 WLAN traffic
  - Radiotap information
  - Beacons and network capabilities
- Bluetooth 4.0 traffic
- Sensor networks
  - 802.15.4
  - ZigBee and ZigBee Pro

Labs:

- RadioTap
- IEEE 802.11
- Bluetooth (optional)
- 802.15.4 and ZigBee (optional)

Wireshark Training Part 6: Analyzing and Troubleshooting IP

- IPv4 header
- IPv4 address
- IP packet fragmentation
- ICMP messaging
- RPL and 6LoWPAN to support the IoT

Labs:

- IP
- ICMP
- RPL / 6LoWPAN (optional)

Wireshark Training Part 7: Analyzing and Troubleshooting TCP

- Establishing a TCP connection
- TCP header
- Port numbers and sockets
- Selective acknowledgements
- Sliding window
- Contention and advertised receiving windows
- Congestion control

Labs:

- TCP 3-Way Handshake
- TCP fields
- TCP traffic

Wireshark Training Part 8: Analyzing and Troubleshooting UDP, and Higher Level Protocols

- Compare and contrast TCP and UDP
- UDP header
- DHCP communications
- DNS process
- HTTP/HTTPS

Labs:

- UDP, DNS and DHCP (optional)
- HTTP (optional)

Wireshark Training Part 9: Analyzing IoT Sensor Network Protocols (Optional)

- IEEE 802.15.4 Low Data Rate Wireless PAN
- ZigBee PRO
- ZigBee IP

Labs:

- 802.15.4 and ZigBee PRO
- RPL and 6LoWPAN

Wireshark Training Part 10: Best Practices and Course Wrap-up

- Checklists
- Managing trace files
- Course recap and conclusion

Labs:

- Analyze a real-life capture

- I/O graph

Website: www.eogogics.com or www.gogics.com
E-mail: info@eogogics.com
Tel. +1 (703) 345-4375
USA 1 (888) 364-6442