

3-Day On-Site Essential Wireshark Training

Enhance your Wireshark skills and become fully confident in analyzing network and application performance and reliability issues for your company



Wireshark is the IT industry-standard tool for packet-level analysis of network and application protocols... but to use Wireshark effectively, you have to have the right skills, knowledge, and experience and that doesn't come from casual use or watching videos and webinars.

Mastering Wireshark requires focused, structured training that includes hands-on application to real-world packet capture scenarios.

PacketIQ provides **on-site*** - **hands-on** training with **real-world packet trace files** that thoroughly cover *all* of Wireshark's features and functionality including: (* up to 12 students per class)

- How to customize Wireshark and apply essential options and filters
- Analysis techniques to quickly isolate network and application problems and performance issues
- Analysis of a wide range of modern network and upper layer protocols

The Essential Wireshark course is conducted by a **Wireshark Certified Network Analyst (WCNA)** and **author of "Wireshark Essentials"** with over 25 years of experience – this training is **GUARANTEED** to vastly improve your skills and knowledge to make you much more effective at packet-level analysis. ***These are essential skills for network, application, server, database, and security professionals alike.***



Includes a unique set of **Wireshark Quick Reference Guides** on each topic for improved retention and usage and advanced **Wireshark Profiles** to enhance your analysis.



WIRESHARK 101: Features & Functions

Day 1: learn all of the essential features and functions of Wireshark, increase your proficiency, and learn fundamental analysis techniques.

The topics covered in Wireshark 101 include:

- How Wireshark works
- Frames vs Packets vs Segments
- Menus, toolbars, right-click options
- Customizing personal profiles
- Custom columns
- Capturing packets – where and how
- Capture filters – hosts, ports, offsets
- Remote captures
- Display filters
- Filter expression buttons
- Working with timestamps (absolute, relative, delta time)
- Conversations & data streams
- Expert info & statistics
- Configuring and using IO graphs
- Stream analysis – TCP, SIP, RTP
- Wireless adapters & captures
- Coloring rules
- Command line utilities
- Wireshark Tips



WIRESHARK 201: Performance Analysis

Day 2: Learn how to save your company money by improving user productivity and reducing costs of troubleshooting poorly performing applications and **significantly improve your value as an IT professional.**

The topics covered in Wireshark 201 include:

- **Top 5 Reasons for Poor Application Performance**
- **Performance Analysis Methodology**
- Defining the problem
- Collecting system–app–path info
- Preparing tools and approach
- Performing & verifying packet captures
- Identifying / isolating traffic of interest
- Initial error analysis
- Detecting and prioritizing delays
- Server processing time events
- App turns and app turn delays
- Analyzing network throughput
- Miscellaneous traffic issues
- TCP & UDP connections & issues
- TCP throughput analysis
- Application issues & errors
- Reporting performance metrics
- Other tools and techniques



WIRESHARK 301: Packets & Protocols

Day 3: Gain *essential knowledge* for troubleshooting complex network and application issues by analyzing real-world packet trace. Attain familiarity with packet structures, network and application services protocols, Upper Layer Protocols, and typical data flows for each.

The topics and protocols covered in Wireshark 301 include:

- Ethernet – IPv4/v6 – UDP – TCP packet formats and fields
- ARP – DNS – DHCP – ICMP including **IPv6** implementations of these services
- HTTP – Web 2.0, AJAX, SOAP, REST, XML, JSON, SSL/TLS, HTTP analysis
- CIFS/SMB & FTP protocols, commands, flows
- SQL – databases & query structure
- VoIP – call control, transport, SIP, RTP, RTCP, codecs
- Citrix – overview, protocols

*Wireshark training courses require customer-provided training facilities and that each attendee possess a workstation or laptop that can support Wireshark software and training-related packet trace file installations.

Pricing does not include travel expenses for trainer. 50% deposit required when training is scheduled.

Contact PacketIQ to schedule your training today!

Call our main number at +1 **321-888-2288** or toll-free +1 **888-382-8860**, Email info@packetiq.com, or use the **Contact Us** form on www.packetiq.com.

© PacketIQ Inc. 2014. All rights reserved

Wireshark and the “fin” logo are registered trademarks of the Wireshark Foundation