Systems & Network Training

Wireshark Certified Network Analyst

A 5 day Hands on training course

Save on expenses. This course is also available on your premises.

Description

Wireshark is a free network protocol analyser. This hands-on course provides a comprehensive tour of using Wireshark to troubleshoot networks. The course concentrates on the information needed in order to pass the WCNA exam. Students will gain the most from this course only if they already have a sound knowledge of the TCP/IP protocols.

Key outcomes

By the end of the course delegates will be able to:

- Download and install Wireshark.
- Capture and analyse packets with Wireshark.
- Configure capture and display filters.
- Customise Wireshark.
- Troubleshoot networks using Wireshark.

Training approach

This structured course uses Instructor Led Training to provide the best possible learning experience. Small class sizes ensure students benefit from our engaging and interactive style of teaching with delegates encouraged to ask questions throughout the course. Quizzes follow each major section allowing checking of learning. Hands on sessions are used throughout to allow delegates to consolidate their new skills.

Details

Who will benefit?
Technical staff looking after networks

Prerequisites
TCP/IP foundation for engineers

Duration: 5 days

Customer rating: ★★★★★

Generic training	Small class sizes	Hands On training	Our courseware	Customise your course
Generic training compliments product specific courses covering the complete picture of all relevant devices including the protocols "on the wire".	We limit our maximum class size to 8 delegates; often we have less than this. This ensures optimal interactivity between delegates and instructor.	The majority of our courses use hands on sessions to reinforce the theory.	We write our own courses; courseware does not just consist of slides and our slides are diagrams not bullet point text.	Please contact us if you would like a course to be customised to meet your specific requirements. Have the course your way.
"*Friendly environment with expert teaching that teaches the why before the how.*" G.C. Fasthosts	*"Excellent course. The small class size was a great benefit..."* M.B. IBM	*"Not many courses have practice added to it. Normally just the theoretical stuff is covered."* J.W. Vodafone	*"Comprehensive materials that made the course easy to follow and will be used as a reference point."* V.B. Rockwell Collins	*"I was very impressed by the combination of practical and theory. Very informative. Friendly approachable environment, lots of hands on."* S.R. Qinetiq

Wireshark Certified Network Analyst

Course content

What is Wireshark?
Network analysis, troubleshooting, network traffic flows. Hands on: Download/install Wireshark.

Wireshark introduction
Capturing packets, libpcap, winpcap, airpcap. Dissectors and plugins. The menus. Right click. Hands on: Using Wireshark.

Capturing traffic
Wireshark and switches and routers. Remote traffic capture. Hands on: Capturing packets.

Capture filters
Applying, identifiers, qualifiers, protocols, addresses, byte values. File sets, ring buffers. Hands on: Capture filters.

Preferences
Configuration folders. Global and personal configurations. Capture preferences, name resolution, protocol settings. Colouring traffic. Profiles. Hands on: Customising Wireshark.

Time
Packet time, timestamps, packet arrival times, delays, traffic rates, packets sizes, overall bytes. Hands on: Measuring high latency.

Trace file statistics
Protocols and applications, conversations, packet lengths, destinations, protocol usages, strams, flows. Hands on: Wireshark statistics.

Display filters
Applying, clearing, expressions, right click, conversations, endpoints, protocols, combining filters, specific bytes, regex filters. Hands on: Display traffic.

Streams
Traffic reassembly, UDP and TCP conversations, SSL. Hands on: Recreating streams.

Saving
Filtered, marked and ranges. Hands on: Export.

TCP/IP Analysis
The expert system. DNS, ARP, IPv4, IPv6, ICMP, UDP, TCP. Hands on: Analysing traffic.

IO rates and trends
Basic graphs, Advanced IO graphs. Round Trip Time, throughput rates. Hands on: Graphs.

Application analysis
DHCP, HTTP, FTP, SMTP. Hands on: Analysing application traffic.

WiFi
Signal strength and interference, monitor mode and promiscuous mode. Data, management and control frames. Hands on: WLAN traffic.

VoIP
Call flows, Jitter, packet loss. RTP, SIP. Hands on: Playing back calls.

Performance problems
Baselining. High latency, arrival times, delta times. Hands on: Identifying poor performance.

Network forensics
Host vs network forensics, unusual traffic patterns, detecting scans and sweeps, suspect traffic. Hands on: Signatures.

Command line tools
Tshark, capinfos, editcap, mergecap, text2pcap, dumpcap. Hands on: Command tools.