Systems & Network Training

Wireshark 101 for engineers

A 2 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 starting point for troubleshooting networks using Wireshark. The course concentrates on the Wireshark product and students will gain from 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.

Duration: 2 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 101 for engineers

Course content

What is Wireshark?

Protocol analysers, Wireshark features, versions, troubleshooting techniques with Wireshark.

Installing Wireshark

Downloading Wireshark, UNIX issues, Microsoft issues, the role of winpcap, promiscuous mode, installing Wireshark. Wireshark documentation and help.
Hands on: Downloading and installing Wireshark.

Capturing traffic

Starting and stopping basic packet captures, the packet list pane, packet details pane, packet bytes pane, interfaces, using Wireshark in a switched architecture.
Hands on: Capturing packets with Wireshark.

Troubleshooting networks with Wireshark

Common packet flows.
Hands on: Analysing a variety of problems with Wireshark.

Capture filters

Capture filter expressions, capture filter examples (host, port, network, protocol, worm), primitives, combining primitives, payload matching.
Hands on: Configuring capture filters.

Display filters

Applying and clearing filters. Protocol, fields, addresses, frames containing strings. Filter comparisons. Combining filters. Finding packets, marking packets.
Hands on: Configuring display filters.

Working with captured packets

Live packet capture, saving to a file, capture file formats, reading capture files from other analysers, merging capture files.
Hands on: Saving captured data.

Analysis and statistics with Wireshark

Following TCP streams, protocol statistics, conversation lists, endpoint lists, I/O graphs, protocol specific statistics.
Hands on: Using the analysis and statistics menus.

Command line tools

Tshark, tethereal, capinfos, editcap, mergecap, text2pcap, idl2eth.
Hands on: Using tshark.

Advanced issues

802.11 issues, management frames, monitor mode, packet reassembling, name resolution, customising Wireshark.
Hands on: Customising name resolution.