Packet Analysis Power Workshop (Wireshark)

Learn via: **Classroom**

Duration: **5 Day**

https://bilginc.com/en/training/packet-analysis-power-workshop-wireshark-4403-training/

Overview

During this 5 day instructor led training course, delegates will receive a comprehensive introduction into the features, functions and the usage of the Wireshark Analyser and will learn methods and techniques about monitoring, analysis and troubleshooting of their networks from the packet level. This course will also focus on the detailed analysis and troubleshooting of typical network protocols and applications with specific focus on switched Ethernet, TCP/IP networks and TCP/IP based applications.

Prerequisites

Delegates are required to attend the following course or have equivalent knowledge:

- Networking & TCP/IP Fundamentals (NWF)

Outline

Features, functions and basic operation of Wireshark Analyzer

- Introduction and operation of Wireshark
- Live Capture and Live Capture settings
- Display options and basic interpretation
- Working with Display Filters and Capture Filters
- File Input and Output

Advanced features of Wireshark Analyzer

- Preferences and user profiles
- Name resolution
- Reconstructing user data – Protocol reassembly
- Packet colorization

Methodology and techniques of network analysis

- What is packet analysis?
- Steps and techniques for analyzing traffic
- Analysing Switched Ethernet - Tapping into the network
- Capturing wireless network traffic
- Measuring network delay and response time
- Measuring network throughput and overhead

Statistics and Baselining

- Baselining of networks and applications
- Wireshark statistics

Analysing networks and applications

- Typical network related problems
- Application types and typical application related problems
- 'Is it the network or the application?' – Fault isolation
- Analysing and reconstructing voice traffic

Switched Ethernet analysis

- Spanning Tree operation and Spanning Tree analysis
- Analysing VLANs, VLAN-Tagging

TCP/IP analysis of the network layer

- IP addressing
- Typical IP scenarios
- IP options
- ICMP, ARP and DHCP

TCP/IP analysis of the transport layer

- TCP functions
- Session Setup, Data Transfer and Session Teardown
- Window Mechanism and Window optimization
- TCP options (SACK, Window Scaling) and TCP timers
- UDP functions

Analysing TCP/IP with Wireshark

- Wireshark preferences for advanced TCP/IP analysis
- Typical TCP/IP related problems
- Wireshark Expert Info messages and their meanings

TCP/IP applications

- HTTP
- FTP
- DNS
- SSL