WCNA certification for Wireshark Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Wireshark is a free network protocol analyzer used to inspect and understand network traffic in detail. This hands-on course provides a comprehensive introduction to using Wireshark for network troubleshooting and protocol analysis. The content is also focused on the knowledge and skills needed to prepare for the WCNA exam.

The program is an **intensive, advanced TCP/IP course** that examines protocol behavior in detail according to the relevant RFCs. Particular attention is given to TCP and network performance. For this reason, the course is intended for participants who already understand TCP/IP fundamentals rather than those who are completely new to the subject.

Participants are expected to be comfortable with addressing and general TCP/IP configuration concepts. Hands-on sessions use Wireshark for practical protocol analysis across a wide range of network scenarios.

Prerequisites

There are no formal prerequisite courses. However, participants should already have a good understanding of how IP networking works.

A TCP/IP foundation-level course may be useful for learners who want to strengthen their background before attending.

What You Will Learn

By the end of the course, participants should be able to:

- Analyze packets and protocols in detail.
- Troubleshoot network issues using Wireshark.
- Identify performance problems through Wireshark analysis.
- Perform network forensics using captured traffic.

Training Outline

What Is Wireshark?

- Network analysis
- Troubleshooting
- Network traffic flows

Hands-on

- Downloading and installing Wireshark

WCNA certification for Wireshark Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Wireshark Introduction

- Capturing packets
- libpcap, winpcap, and airpcap
- Dissectors and plugins
- Menus
- Right-click functionality

Hands-on

- Working with Wireshark

Capturing Traffic

- Using Wireshark with switches and routers
- Remote traffic capture

Hands-on

- Capturing packets

Capture Filters

- Applying capture filters
- Identifiers and qualifiers
- Protocol, address, and byte-value filtering
- File sets and ring buffers

Hands-on

- Building and applying capture filters

Preferences

- Configuration folders
- Global and personal configurations
- Capture preferences
- Name resolution
- Protocol settings
- Traffic colouring
- Profiles

Hands-on

- Customizing Wireshark

Time Analysis

- Packet time
- Timestamps
- Packet arrival times
- Delays
- Traffic rates
- Packet sizes

BILGINÇ IT Academy

info@bilginc.com

bilginc.com

- Overall byte counts

Hands-on

- Measuring high latency

Trace File Statistics

- Protocols and applications
- Conversations
- Packet lengths
- Destinations
- Protocol usage
- Streams
- Flows

Hands-on

- Working with Wireshark statistics

Display Filters

- Applying and clearing filters
- Filter expressions
- Right-click filtering
- Conversations and endpoints
- Protocol filters
- Combining filters
- Filtering specific bytes
- Regular expression filters

Hands-on

- Filtering displayed traffic

Streams

- Traffic reassembly
- UDP and TCP conversations
- SSL traffic

Hands-on

- Reconstructing streams

Saving and Exporting

- Filtered packets
- Marked packets
- Packet ranges

Hands-on

- Exporting captured data

WCNA certification for Wireshark Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

TCP/IP Analysis

- Wireshark Expert System
- DNS
- ARP
- IPv4
- IPv6
- ICMP
- UDP
- TCP

Hands-on

- Analyzing network traffic

IO Rates and Trends

- Basic graphs
- Advanced IO graphs
- Round Trip Time
- Throughput rates

Hands-on

- Using graphs for traffic and performance analysis

Application Analysis

- DHCP
- HTTP
- FTP
- SMTP

Hands-on

- Analyzing application traffic

WiFi Analysis

- Signal strength and interference
- Monitor mode and promiscuous mode
- Data frames
- Management frames
- Control frames

Hands-on

- Analyzing WLAN traffic

VoIP Analysis

- Call flows
- Jitter
- Packet loss

BILGINÇ IT Academy

info@bilginc.com

bilginc.com

- RTP
- SIP

Hands-on

- Reviewing and playing back calls

Performance Problems

- Baselining
- High latency
- Arrival times
- Delta times

Hands-on

- Identifying poor network performance

Network Forensics

- Host forensics versus network forensics
- Unusual traffic patterns
- Detecting scans and sweeps
- Suspicious traffic

Hands-on

- Identifying traffic signatures

Command-Line Tools

- Tshark
- capinfos
- editcap
- mergecap
- text2pcap
- dumpcap

Hands-on

- Using Wireshark command-line utilities