Using Wireshark to Analyze and Troubleshoot TCP/IP Networks Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Using Wireshark to Analyze and Troubleshoot TCP/IP Networks is a hands-on training program designed for IT professionals who want to strengthen their expertise in **Network Traffic Analysis**, **Packet Analysis**, and advanced network troubleshooting. The course combines theoretical knowledge with practical laboratory exercises to help learners capture, filter, interpret, and investigate network communications using **Wireshark**.

Participants will work through real-world scenarios involving performance bottlenecks, security incidents, protocol behavior, and network anomalies. Through extensive hands-on exercises, learners will gain practical experience analyzing both wired and wireless network traffic and resolving complex connectivity issues.

The course also covers **Network Forensics**, **TCP/IP Analysis**, **Network Security Monitoring**, and advanced troubleshooting methodologies. Its content aligns closely with the objectives of the **Wireshark Certified Analyst (WCA)** certification, making it valuable for both certification candidates and experienced professionals seeking deeper technical knowledge.

Prerequisites

Participants should have:

- Basic **Networking Fundamentals** knowledge
- Understanding of **TCP/IP Protocols**
- Familiarity with network security concepts
- Experience using network analysis tools
- Basic packet analysis and troubleshooting experience (recommended)

Who Should Attend

This course is ideal for:

- **Network Engineers**
- **Network Administrators**
- **System Administrators**
- **Cyber Security Professionals**
- **SOC Analysts**
- Infrastructure specialists
- IT operations teams
- Software developers
- Professionals responsible for network performance and security

Using Wireshark to Analyze and Troubleshoot TCP/IP Networks Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of this course, learners will be able to:

- Explain the objectives of **Network Analysis**.
- Install, configure, and optimize **Wireshark**.
- Capture traffic on wired and wireless networks.
- Apply **Capture Filters** and **Display Filters** effectively.
- Analyze **TCP/IP**, **DNS**, **ARP**, **ICMP**, **IPv4**, **IPv6**, **UDP**, and **TCP** traffic.
- Identify and troubleshoot network performance issues.
- Detect suspicious traffic and security threats.
- Utilize **Network Forensics** methodologies.
- Visualize network performance using graphs and statistics.
- Leverage command-line tools for advanced analysis.

Training Outline

Introduction to Network Analysis and Wireshark

- Fundamentals of **Network Analysis**
- Wireshark architecture and capabilities
- TCP/IP communication analysis
- Common network performance issues
- Installing and updating Wireshark
- Capturing network traffic
- Introduction to **Network Forensics**

Packet Capture and Filtering

- Traffic capture methodologies
- **Capture Filters**
- Switched network analysis
- Using **Network TAPs**
- Wireless network analysis
- Advanced filtering techniques
- Detecting scanning and discovery activities

Customization and Advanced Navigation

- Building **Custom Wireshark Profiles**
- Troubleshooting profile creation
- User interface customization
- Custom column configuration
- Preferences and display optimization
- Coloring rules and visual analysis
- Advanced navigation techniques

Security and Suspicious Traffic Analysis

- Identifying suspicious network activity

BILGINC IT Academy

info@bilginc.com

bilginc.com

- Malicious traffic investigation
- Security event analysis
- Packet content inspection
- Traffic behavior interpretation

Time Analysis and Statistics

- Delta time analysis
- Time references and timestamps
- TCP conversation timing
- Packet timestamp evaluation
- Network statistics and reporting

Command-Line Network Analysis

- Wireshark command-line utilities
- Traffic processing workflows
- Automated analysis techniques
- Advanced network diagnostics

Protocol-Specific Traffic Analysis

- **Display Filters**
- Packet-based filtering
- Endpoint and conversation analysis
- TCP/IP communications
- DNS traffic analysis
- ARP operations
- ICMP troubleshooting
- UDP and TCP traffic analysis

Network Performance Troubleshooting

- **TCP Stream Analysis**
- IO graph creation and interpretation
- TCP trend analysis
- Performance bottleneck identification
- Packet loss investigation
- Latency and connectivity troubleshooting
- Using Wireshark Expert System

Security Monitoring and Network Forensics

- Detecting scanning activities
- Discovery process analysis
- Suspicious payload inspection
- **Network Security Monitoring**
- Security incident investigation
- Network forensic techniques