Wireshark for Network Security Monitoring and Packet Analysis Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The digital landscape is defined by its constant, complex flow of data, making Deep Packet Inspection (DPI) a non-negotiable skill for all Cybersecurity and NetSecOps professionals. Wireshark for Network Security Monitoring and Packet Analysis Training Course provides a deep-dive into the art and science of Packet Analysis and Network Forensics. Participants will move beyond basic sniffing to master advanced filtering, protocol analysis, and traffic visualization, transforming raw network data into actionable Threat Intelligence. Mastery of Wireshark is critical for modern Threat Hunting and Incident Response, serving as the ultimate diagnostic and security monitoring tool in both physical and Cloud Environments.

In an era of rising Ransomware-as-a-Service (RaaS) and sophisticated Supply Chain Attacks, the ability to analyze network traffic at the packet level is the difference between early detection and catastrophic breach. This course is explicitly structured to empower participants to swiftly identify Zero-Trust violations, trace Malware command-and-control (C2) traffic, and conduct granular Root Cause Analysis. Through extensive hands-on labs and focused real-world case studies, students will develop the essential analytical rigor to defend complex enterprise networks, making them indispensable assets in any modern Security Operations Center (SOC).

Programme Curriculum

Wireshark for Network Security Monitoring and Packet Analysis Training Course

Introduction

The digital landscape is defined by its constant, complex flow of data, making Deep Packet Inspection (DPI) a non-negotiable skill for all Cybersecurity and NetSecOps professionals. Wireshark for Network Security Monitoring and Packet Analysis Training Course provides a deep-dive into the art and science of Packet Analysis and Network Forensics. Participants will move beyond basic sniffing to master advanced filtering,

protocol analysis, and traffic visualization, transforming raw network data into actionable Threat Intelligence. Mastery of Wireshark is critical for modern Threat Hunting and Incident Response, serving as the ultimate diagnostic and security monitoring tool in both physical and Cloud Environments.

In an era of rising Ransomware-as-a-Service (RaaS) and sophisticated Supply Chain Attacks, the ability to analyze network traffic at the packet level is the difference between early detection and catastrophic breach. This course is explicitly structured to empower participants to swiftly identify Zero-Trust violations, trace Malware command-and-control (C2) traffic, and conduct granular Root Cause Analysis. Through extensive hands-on labs and focused real-world case studies, students will develop the essential analytical rigor to defend complex enterprise networks, making them indispensable assets in any modern Security Operations Center (SOC).

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Perform Advanced Packet Capture and apply complex Capture Filters for surgical traffic isolation.
2. Master Deep Packet Inspection (DPI) across critical layers to uncover hidden protocol anomalies.
3. Execute Network Forensics to reconstruct security incidents and trace attack vectors from initial compromise.
4. Apply expert Display Filters to rapidly isolate evidence of Data Exfiltration and C2 communication.
5. Analyze core TCP/IP protocol behavior to identify network Performance Bottlenecks and abnormal traffic flows.
6. Investigate evidence of Malware and Ransomware activity by analyzing encrypted and unencrypted network streams.
7. Utilize Wireshark's Expert System to diagnose common network errors, security flags, and application-layer issues.
8. Perform Real-Time Traffic Analysis for proactive Threat Hunting and anomaly detection within a live environment.
9. Develop custom Coloring Rules and Profiles for efficient, role-based network monitoring and visualization.
10. Extract network artifacts, credentials, and files from Packet Captures (PCAPs) to support Incident Response.
11. Differentiate between normal network Baseline Traffic and suspicious activity like Port Scanning or DDoS precursors.
12. Leverage command-line tools like Tshark for automated and remote network traffic analysis in SecOps.
13. Create comprehensive, evidence-based Incident Reports using statistical data for both technical and non-technical stakeholders.

Target Audience

1. SOC Analysts
2. Incident Responders and Threat Hunters
3. Network Engineers and NetDevOps Professionals
4. Cybersecurity Analysts and Consultants
5. Forensics Investigators
6. Penetration Testers and Ethical Hackers

7. System Administrators and IT Support Specialists
8. Cloud Security Professionals

Course Modules

Module 1: Wireshark Fundamentals and Advanced Capture Techniques

- Installation, interface navigation, and creation of personalized analysis Profiles.
- Understanding the differences between Capture Filters and Display Filters
- Mastering diverse capture methods.
- Saving, manipulating, and merging large-scale PCAP files, including the pcapng format.
- Analyzing capture file statistics.
- Case Study: The Overwhelmed Switch.

Module 2: Deep Dive into TCP/IP and Protocol Analysis

- In-depth dissection of the TCP 3-Way Handshake and its common anomalies for Troubleshooting.
- Identifying and diagnosing common network issues.
- Analyzing UDP and ARP protocol behavior to spot potential man-in-the-middle or host resolution issues.
- Using I/O Graphs and Flow Graphs to visualize bandwidth utilization and identify intermittent drops.
- Decoding common application protocols like HTTP/S, DNS, and DHCP for application-layer insight.
- Case Study: The Slow Application.

Module 3: Security Monitoring with Display Filters and Color Rules

- Building powerful, nested Display Filters using logical operators for targeted evidence hunting.
- Creating dynamic Coloring Rules to instantly highlight packets of security interest.
- Filtering for known indicators of compromise, including suspicious port activity and non-standard protocols.
- Utilizing advanced filter techniques.
- Applying the Expert System and Marking Packets for collaborative Incident Triage.
- Case Study: Identifying Suspicious Activity.

Module 4: Network Forensics and Reconstructing Sessions

- Using the 'Follow Stream' feature to reconstruct and analyze full application-layer conversations.
- Extracting embedded objects and files from captured traffic for malware analysis.
- Analyzing FTP and other clear-text protocol sessions to extract user credentials and sensitive data.
- Techniques for dealing with large PCAP files.
- Understanding and mitigating privacy concerns during packet capture and forensic analysis.
- Case Study: The Exfiltrated File.

Module 5: Detecting Malware and C2 Traffic Analysis

- Identifying signs of Malware infection.
- Analyzing common Command-and-Control communication patterns in network traffic.
- Investigating Encrypted Traffic for suspicious flow characteristics even without decryption keys.
- Spotting precursors to Ransomware deployment, such as SMB enumeration and rapid internal port scanning.
- Using Wireshark statistics to detect low-and-slow Data Exfiltration over common protocols.
- Case Study: The Beaconing Threat.

Module 6: Wireless and Infrastructure Protocol Analysis

- Capturing and analyzing Wireless Traffic with the correct hardware and monitor mode.
- Decoding WPA/WPA2 handshake packets to understand the process
- Analyzing essential infrastructure protocols.
- Investigating IPv6 traffic flows and their security implications in a dual-stack network.
- Deep analysis of VoIP protocols for quality issues or potential eavesdropping.
- Case Study: Unauthorized AP.

Module 7: Threat Hunting and Incident Response with Wireshark

- Integrating Wireshark analysis into the standard Incident Response lifecycle
- Hunting for common attack patterns.
- Correlating Wireshark data with SIEM logs and other security tooling for a holistic view.
- Identifying evidence of zero-day exploitation through unusual packet lengths, fragmented packets, or malformed protocol fields.
- Developing and saving custom, reusable Threat Hunting filters for regular network assessment.
- Case Study: Tracing a Lateral Movement.

Module 8: Advanced Decryption and Reporting

- Configuring Wireshark to decrypt common encrypted protocols
- Analyzing the security implications of unencrypted protocols in a modern network environment.
- Generating professional, audience-specific reports.
- Exporting raw data and critical packet information for use in other forensic tools.
- A comprehensive, time-constrained analysis of a full, multi-stage simulated network breach from capture to final report.
- Case Study: Decrypting a Web Session.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org **or call** +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com