



Wireshark Network Traffic Investigation Training Course

Wireshark Network Traffic Investigation Training Course

Overview

Wireshark Network Traffic Investigation Training Course is a five-day intermediate course for network analysts, SOC investigators, incident responders, infrastructure engineers, and cybersecurity operations teams who leave with a Network Traffic Investigation Workbook. Participants practice packet capture planning, Wireshark filter analysis, TCP conversation analysis, protocol metadata review, suspicious traffic triage, and network incident timeline reconstruction. The course separates packet evidence from broad network security and penetration testing. Agile Leaders Training Center develops practical network traffic investigation capability.

Who Should Attend

- Network analysis functions responsible for interpreting packet behavior and service performance
- Security operations functions responsible for triaging suspicious network activity
- Incident response functions responsible for reconstructing network evidence
- Infrastructure engineering functions responsible for diagnosing protocol and connectivity symptoms
- Cybersecurity operations functions responsible for documenting traffic findings

The course assumes participants can interpret TCP/IP addressing, ports, common protocols, and network diagrams, and leaves out offensive exploitation, malware reverse engineering, wireless intrusion, and broad security architecture.

Departments and Industries

The course supports departments and industries that operate, monitor, or investigate networked services.

- Banking network and security operations
- Telecommunications service assurance
- Energy and utility infrastructure monitoring
- Healthcare technology operations
- Managed network and security services

Learning Objectives

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



- Apply evidence-led packet capture planning
- Use capture and display filters accurately
- Analyze protocols, conversations, and TCP behavior
- Diagnose performance symptoms from packet evidence
- Prioritize suspicious traffic and reconstruct timelines
- Build a Network Traffic Investigation Workbook

Course Agenda

Day 1: Plan and Preserve Packet Evidence

- Network Observation Point Selection Map
- Packet Capture Scope and Evidence Plan
- Wireshark Capture Interface Configuration
- Capture Filter Design and Validation Method
- PCAP Integrity and Case Notes Record

Day 2: Navigate and Filter Traffic

- Wireshark Packet List, Details, and Bytes Workflow
- Display Filter Field and Operator Builder
- Endpoint and Conversation Statistics Matrix
- Protocol Hierarchy and Traffic Distribution Review
- Time Reference and Capture Alignment Method

Day 3: Analyze Protocol Behavior

- TCP Handshake and Session State Diagram
- TCP Retransmission and Loss Evidence Table
- DNS Query and Response Analysis Worksheet
- HTTP Transaction and Object Metadata Map
- TLS Handshake and Certificate Metadata Review

Day 4: Investigate Anomalies and Incidents

- Wireshark Expert Information Triage Method
- Follow Stream Conversation Reconstruction
- Suspicious Connection Pattern Matrix
- Network Incident Timeline Worksheet
- Finding Confidence and Alternative Explanation Log

Day 5: Practice the Traffic Investigation

- Exercise: Validate a Packet Capture Scope
- Exercise: Build Filters for a Network Question
- Exercise: Diagnose TCP and Protocol Symptoms
- Exercise: Reconstruct Suspicious Traffic Activity
- Capstone: Network Traffic Investigation Workbook

Practical Exercises

The course uses suggested activities based on banking, telecommunications, energy, healthcare, and managed-service networks.

- Suggested activity: select observation points, define capture scope, and preserve a PCAP evidence record.
- Suggested activity: build capture and display filters that answer specific operational questions.
- Suggested activity: connect TCP, DNS, HTTP, and TLS metadata to a performance or security hypothesis.
- Suggested activity: assemble conversations, timelines, confidence judgments, and findings into an investigation workbook.

FAQs

Who suits Wireshark network traffic investigation training, and what does it assume?

Network, security operations, incident response, infrastructure, and cybersecurity teams suit the training; it assumes familiarity with TCP/IP, ports, common protocols, and network diagrams.

How does Wireshark network traffic investigation differ from general network security training?

Wireshark traffic investigation concentrates on packet evidence, conversations, protocol behavior, timelines, and findings, while general network security training covers broader architecture, controls, administration, and policy.

What is the difference between Wireshark capture filters and display filters?

Capture filters limit which packets are collected, while display filters select which packets are shown from an existing capture without removing the other captured packets.

How does Wireshark help diagnose TCP performance symptoms?

Wireshark helps analysts examine handshakes, sequence behavior, acknowledgments, retransmissions, loss indicators, timing, window behavior, and conversation statistics alongside the network context.



How should analysts document suspicious network traffic findings?

Analysts should record capture scope, timestamps, filters, endpoints, conversations, protocol evidence, alternative explanations, confidence, limitations, and the actions needed to confirm or escalate each finding.

Conclusion

Participants take back a Network Traffic Investigation Workbook linking capture decisions, filters, protocol evidence, conversations, timelines, performance symptoms, suspicious activity, and supported findings. It changes isolated packets into a traceable investigation workflow. The workbook supports coordinated analysis across network, infrastructure, security operations, and incident response functions.



Training Course Categories

Agile PM and Project Management Training Courses

Agribusiness & Food Security Training Courses

Certified Courses By International Bodies

Communication and Public Relations Training Courses

Crisis Management and Business Continuity Training Courses

Data Analytics Training and Data Science Courses

Digital Government & Public Service Training Courses

Education and Learning Development Training Courses

Environment & Sustainability Training Courses

Facilities and Real Estate Training Courses

Finance and Accounting Training Courses

Governance, Risk and Compliance Training Courses

Healthcare Management Training Courses

Heritage Conservation and Museum Management Training Courses

Hospitality and Tourism Training Courses

Human Resources Training and Development Courses

IT Security Training & IT Training Courses

Leadership and Management Training Courses

Legal Training, Procurement and Contracting Courses

Maintenance Training and Engineering Training Courses

Marketing, Customer Relations, and Sales Courses

NGO, Humanitarian and Development Management Training Courses

Occupational Health, Safety and Security Training Courses

Oil & Gas Training and Other Technical Courses

Personal & Self-Development Training Courses

Quality and Operations Management Training Courses



Training Course Categories

Secretarial and Administration Training Courses

Shipping, Maritime and Ports Training Courses



Training Cities

Abu Dhabi UAE	Accra Ghana	Amman Jordan
Amsterdam Netherlands	Athens Greece	Baku Azerbaijan
Bali Indonesia	Bangkok Thailand	Barcelona Spain
Berlin Germany	Cairo Egypt	Cape town South Africa
Casablanca Morocco	Chicago USA	Doha Qatar
Dubai UAE	Frankfurt Germany	Geneva Switzerland
Istanbul Turkey	Jakarta Indonesia	Johannesburg South Africa
Kuala Lumpur Malaysia	Kuwait Kuwait	Langkawi Malaysia
Lisbon Portugal	London UK	Madrid Spain
Manama Bahrain	Marbella Spain	Milan Italy
Montreux Switzerland	Munich Germany	Muscat Oman
Nairobi Kenya	New York USA	Nice France

Training Cities

Paris

France

Phuket

Thailand

Port Louis

Mauritius

Porto

Portugal

Prague

Czech Republic

Rome

Italy

San Diego

USA

Seoul

South Korea

Sharm El-Sheikh

Egypt

Singapore

Singapore

Tashkent

Uzbekistan

Tbilisi

Georgia

Tokyo

Japan

Toronto

Canada

Trabzon

Turkey

Vienna

Austria

Zanzibar

Tanzania

Zoom

Online Training

Zurich

Switzerland