CONCEPT

Network Packet Analysis with Wireshark: Capture, TCP Latency and Troubleshooting

10 – 14 May 2027
London - Central London four-star



Network Packet Analysis with Wireshark: Capture, TCP Latency and Troubleshooting

Ref: 629_18164 **Date:** 10 – 14 May 2027 **Location:** London - Central London four-star **Fees:** 25300 SAR

Introduction:

Network packet analysis settles the argument that follows every slow-application complaint: is the delay in the network, the server or the client? Without trace evidence, teams swap blame, reboot devices and close tickets that reopen a week later. This Core Concept course trains engineers to place capture points correctly, filter large trace files with the open-source analyser Wireshark, and read Ethernet, IP, TCP, DNS, DHCP, HTTP and TLS exchanges to locate the true source of delay. Participants finish with a Packet-Level Troubleshooting Report for a slow-application incident.

Course Objectives:

- Select a capture point and method, using port mirroring, a network tap or a host capture, that records the traffic a fault investigation needs without dropped frames
- Build capture and display filters, colouring rules and custom columns that reduce a large trace file to the conversations relevant to a ticket
- Interpret TCP handshakes, receive windows, retransmissions and round-trip times to separate network delay from server and client delay
- Analyse DNS, DHCP, HTTP and TLS handshake exchanges to pinpoint name resolution, addressing, request-response and session set-up faults
- Establish traffic baselines with I/O graphs and conversation statistics so abnormal behaviour can be recognised quickly
- Write a packet-level troubleshooting report that states the root cause, the trace evidence and the corrective action for a slow-application incident

Target Audience:

- Network operations engineers who investigate connectivity loss, packet loss and link congestion across campus and data centre networks
- Systems and server engineers who must prove or rule out host-side delay when applications respond slowly
- Service desk and support escalation engineers who handle performance tickets that other teams cannot resolve
- Application support engineers who trace client-server exchanges during releases and incidents
- Network monitoring staff who maintain traffic baselines and investigate alerts from performance tools

Course Outline:

Day 1: Capture Strategy, Capture Points and Trace Handling

- Packet Analyser Architecture: Capture Library, Dissectors and the Command-Line Capture Utility
- Capture Point Selection: Client Side, Server Side and Midpoint Placement
- Port Mirroring SPAN and Remote SPAN Versus Passive Full-Duplex Network Taps
- Promiscuous Mode, Ring Buffers, Snap Length and Dropped-Packet Checks
- Trace File Handling: Merging, Slicing, Time References and Sanitising for Sharing

Day 2: Filters, Dissection of Ethernet, IP and TCP, and the Analyser Workspace

- Capture Filter Syntax Versus Display Filter Syntax with Field-Based Expressions
- Colouring Rules, Custom Columns and Analyst Configuration Profiles
- Ethernet II Frame and 802.1Q Tag Dissection with ARP Request-Reply Checks
- IPv4 Header Inspection: TTL, Fragmentation Flags and DSCP Markings
- TCP Header Fields, Three-Way Handshake and Window Scale Option Under RFC 7323

Day 3: TCP Performance, Retransmissions and Latency Analysis Lab

- Round-Trip Time Measurement and Retransmission Timeout Behaviour Under RFC 6298
- Expert Information Panel: Duplicate ACKs, Fast Retransmissions and Out-of-Order Segments
- RACK Loss Detection and Congestion Control Phases Under RFC 5681 and RFC 8985
- Zero Window, Window Full and Bytes-in-Flight Analysis with TCP Stream Graphs
- Delta Time Columns for Separating Network Transit, Server Think Time and Client Delay

Day 4: Application Protocols, TLS Handshake Reading and Slow-Application Diagnosis

- DNS Query-Response Timing, Failed Lookups and Resolver Retry Patterns
- DHCP Discover-Offer-Request-Acknowledge Sequence and Lease Failure Traces
- HTTP Request-Response Timing, Status Codes and Object Download Waterfalls
- TLS Handshake Reading: Client Hello, Server Hello, Certificate Exchange and Alert Messages
- Wireless Capture Overview: Monitor Mode, Channel Selection and 802.11 Retry Frames

Day 5: Lab: Baselining and the Packet-Level Troubleshooting Report

- I/O Graph Baseline Build: Throughput, Packet Rate and Response-Time Plots
- Conversation, Endpoint and Protocol Hierarchy Statistics for Anomaly Spotting
- Case Lab: Multi-Point Capture of a Slow Business Application Incident
- Root Cause Evidence Chain: Annotated Packets, Graphs and Timing Tables
- Packet-Level Troubleshooting Report Presentation and Peer Challenge

Skills You Will Gain:

- Capture Point Planning
- Display Filter Construction
- TCP Stream Diagnostics
- Latency Attribution
- Protocol Exchange Interpretation
- Traffic Baselining
- Trace Evidence Documentation
- Wireless Frame Inspection

Why Attend This Course:

- Return with a Packet-Level Troubleshooting Report built from a multi-point capture of a slow-application case
- End blame between network, server and application teams by presenting timing evidence taken from the wire
- Work through trace files in the lab each day instead of watching slide demonstrations
- Exchange capture techniques with engineers who run networks in offices, hospitals, plants and hosting centres

Conclusion:

Slow applications and intermittent failures are resolved faster when engineers can show exactly where time is lost in a conversation. The course moves from capture points and trace handling, through filters and Ethernet, IP and TCP dissection, to retransmission and latency analysis, then DNS, DHCP, HTTP, TLS handshake reading and wireless capture. The final day builds traffic baselines with I/O graphs and applies them to a multi-point case lab, producing a Packet-Level Troubleshooting Report ready to share with application owners.