ExperTeach NETWORKING

Wireshark Advanced Troubleshooting

Wireshark Advanced Troubleshooting

Netzwerk- und Anwendungsanalyse für Fortgeschrittene

In modernen IT-Umgebungen sind Performance-Probleme selten eindeutig. Lange Antwortzeiten, Paketverluste oder schwankender Durchsatz sind oft nur Symptome. Die tatsächliche Ursache liegt häufig im Zusammenspiel von TCP-Mechanismen, Netzwerkinfrastruktur, Servern und Anwendungen.

Dieser Wireshark-Expertenkurs richtet sich an erfahrene Anwenderinnen und Anwender, die komplexe Störungen strukturiert untersuchen und belastbare Aussagen treffen möchten. Im Mittelpunkt steht eine methodische Vorgehensweise für die Analyse anspruchsvoller Trace-Dateien – sowohl bei Einzelmessungen als auch bei Mehrpunktanalysen.

Sie vertiefen Ihr Verständnis für das Verhalten von TCP. Außerdem erkennen Sie Paketverluste und Durchsatzprobleme zuverlässig und lernen, Netzwerkursachen klar von server- oder anwendungsbedingten Effekten zu unterscheiden. Die Analyse typischer Anwendungsprotokolle wie TLS, HTTP(S), SMB, DNS und Citrix wird praxisnah behandelt.

Der Kurs ist stark praxisorientiert aufgebaut: Anhand realitätsnaher Fallbeispiele arbeiten Sie mit anonymisierten Trace-Dateien aus produktionsnahen Szenarien. So trainieren Sie nicht nur einzelne Analysefunktionen, sondern entwickeln die Fähigkeit, komplexe Störungen systematisch zu durchdringen und nachvollziehbar zu dokumentieren.

Kursinhalt

- Messtechnik für die Auswertung komplexer Problemstellungen
- Wichtige Vorbereitungen von Messungen vor Ort
- Abgrenzung von Netzwerk- und Anwendungsproblemen
- Analysemethoden – Vorgehen bei der Analyse und beim Erkennen von Problemen
- Erkennen und Ausschließen von Netzwerkproblemen
- Mehrpunktanalysen – Auswerten von Trace-Dateien mehrerer Messpunkte
- Analyse komplexer TCP-Probleme
- Paketverluste erkennen und eingrenzen
- Lange Laufzeiten und Durchsatzprobleme analysieren
- Schlechte Serverperformance und ihre Ursachen
- Analyse der Performance von Datenbankanwendungen
- Anwendungsspezifische Analyse von TLS, HTTP(S), SMB, DNS und Citrix

Zielgruppe

Dieser Kurs wendet sich an erfahrene Anwenderinnen und Anwender von Wireshark, die grundlegende Kenntnisse in der Auswertung von TCP/IP mitbringen und ihre Fähigkeiten in strukturierter Fehlersuche sowie Analyse komplexer Problemstellungen erweitern möchten.

Voraussetzungen

Sie verfügen über gute Kenntnisse der Funktionen von TCP, UDP und IP sowie über solide praktische Erfahrung im Umgang mit Wireshark und der Analyse von TCP/IP. Als Vorbereitung eignet sich insbesondere der Kurs Wireshark Protokollanalyse – Praktischer Einsatz im Netzwerk.

Kursziel

Ziel des Wireshark Workshops ist es, praxisnah Fähigkeiten in der Analyse und Fehlersuche von Netzwerken und TCP/IP-basierten Anwendungen mithilfe von Wireshark zu erlangen und komplexe Fehlerbilder eigenständig analysieren und lösen zu können.

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.at/go/**WIAT**

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Premium Print Paket

Zu diesem Kurs können sie optional das hochwertige Premium Print Paket zum Preis von € 150,- (zzgl. MwSt) erwerben.

Training		Preise zzgl. MwSt.
Termine in Deutschland	**3 Tage**	**€ 2.395,-**
Online Training	**3 Tage**	**€ 2.395,-**

Termin/Kursort		Kurssprache Deutsch	
30.11.-02.12.26	HY Hamburg	19.07.-21.07.27	HY Hamburg
30.11.-02.12.26	HY Online	19.07.-21.07.27	HY Online
15.03.-17.03.27	HY Hamburg	03.11.-05.11.27	HY Hamburg
15.03.-17.03.27	HY Online	03.11.-05.11.27	HY Online

Stand 04.08.2026

ExperTeach

Inhaltsverzeichnis

Wireshark Advanced Troubleshooting – Netzwerk- und Anwendungsanalyse für Fortgeschrittene

1 Wireshark Funktionen und Messtechnik
1.1 Wireshark Displayfilter
1.1.1 Grundlegende Anzeigefilter
1.1.2 Vergleichsoperatoren
1.1.3 Logische Operatoren
1.1.4 Filtern aus einer Liste von Werten
1.2 Mitschnittfilter
1.3 Voreinstellungen und Profile
1.3.1 Benutzerprofile – Configuration Profiles
1.4 Messtechnik mit Wireshark
1.4.1 Port Monitoring – SPAN
1.4.2 Test Access Point – TAP
1.4.3 Wireshark auf dem Endgerät
1.4.4 Messpunkt aus Trace File ermitteln
1.5 Auswerten von Daten mehrerer Standorte
1.5.1 Aufgaben definieren und Messungen starten
1.5.2 Messdateien normalisieren
1.5.3 Auswertung der Trace Files

2 Anwendungen mit Wireshark analysieren
2.1 Anwendungs- und Serverstrukturen
2.1.1 Fat-Client Architektur
2.1.2 Alternativen zum Fat-Client
2.1.3 Terminalserver Lösungen
2.1.4 Virtuelle Desktop-Infrastrukturen
2.2 Anwendungstypen und Performancefaktoren
2.2.1 Durchsatzorientierte Anwendungen
2.2.2 Transaktionsorientierte Anwendungen
2.2.3 Echtzeitanwendungen – Voice und Streaming
2.3 Netzwerkprobleme und Anwendungsprobleme
2.3.1 Typische Netzwerkprobleme
2.3.2 Typische Anwendungsprobleme
2.4 Vorgehen bei der Analyse (Analysetechniken)
2.4.1 Netzwerkprobleme erkennen und ausschließen
2.4.2 Potentielle Probleme an Servern
2.4.3 Der Einfluss von SAN oder NAS
2.4.4 Client-Server-Architektur überprüfen
2.4.5 Probleme in Anwendungen finden

3 Performance-Probleme – Ursachen erkennen und Lösungen finden
3.1 Netzwerkprobleme erkennen und eliminieren
3.2 Hohe Laufzeiten im Netz
3.2.1 Eingrenzung hoher Round-Trip-Zeiten
3.2.2 Elemente der Laufzeit
3.3 Paketverluste in den Griff bekommen
3.3.1 Eingrenzen von Retransmissions
3.3.2 Überlastung im Router oder am WAN
3.3.3 Fehlerhafte Anpassung an WAN-Bandbreite
3.3.4 Probleme mit der Path-MTU-Discovery
3.3.5 Duplex Mismatch im Ethernet
3.3.6 Vertauschte Pakete
3.4 Durchsatzeinbrüche
3.5 Namensauflösung
3.6 Einflüsse von Security-Strukturen
3.6.1 Paketfilter und Firewalls
3.6.2 Probleme mit Web-Proxys erkennen
3.6.3 VPN-Gateway und VPN-Verbindungen

4 TCP-Analyse und Fehlersuche
4.1 Protokollreferenzen TCP
4.1.1 TCP-Verbindungen in Wireshark
4.1.2 TCP-Funktionen in Wireshark
4.1.3 Conversation Completeness
4.2 Paketverluste, Retransmissions und Timing
4.2.1 Selective Acknowledgments (SACK)
4.2.2 Duplicate SACK (D-SACK) nach RFC 2883
4.3 TCP Zero Window
4.3.1 Window Mechanismus und Performance
4.3.2 TCP Window Scaling Option

5 Analyse von Datenbankanwendungen
5.1 Datenbankanwendungen
5.1.1 Strukturen von Datenbankanwendungen
5.2 Monolithische Datenbankanwendungen
5.2.1 Einfache Systeme
5.2.2 Multi Tier - Umgebungen
5.2.3 Traffic Flow – Beispiel für Datenbanksysteme
5.3 Serverarchitekturen, Traffic Flows und Messpunkte
5.4 Auswertung von Datenbankanwendungen
5.4.1 Auswertung der Front-End-Daten
5.4.2 Front-End-Auswertung mit Wireshark
5.4.3 Auswertung der Back-End-Daten
5.4.4 Auswerten der Back End Daten mit Wireshark
5.4.5 Auswertetechnik mit Excel
5.4.6 Performance von Datenbankverbindungen

6 Analyse von Secure Protocols – TLS und SSH
6.1 Sicherheit mit TLS
6.1.1 Der TLS Protokollstapel
6.1.2 Aufgaben von TLS
6.2 Verbindungsaufbau für TLS 1.2
6.3 Verbindungsaufbau für TLS 1.3
6.4 TLS-Fehlersuche
6.5 TLS-Decrypt über RSA-Keys – Beispiel HTTPS
6.6 TLS-Decrypt über TLS Logfiles

7 Analyse von HTTP, HTTP/2, QUIC und HTTP/3
7.1 HTTP und World Wide Web
7.1.1 HTTP-Versionen
7.1.2 Kommunikationsverhalten von HTTP 1.1
7.1.3 Kommunikationsverhalten von HTTP/2
7.1.4 HTTP-Fehler in Wireshark
7.1.5 HTTP-Antwortzeiten
7.2 HTTP 1.1 über Proxys
7.2.1 Explizite Proxys
7.2.2 Authentisierung mit explizitem Proxy
7.3 HTTP Version 2
7.3.1 HTTP/2-Varianten
7.3.2 HTTP over TCP (H2C)
7.3.3 HTTP over TLS (H2)
7.3.4 HTTP/2-Datenaustausch
7.4 Google QUIC und IETF-QUIC
7.4.1 Verbindungsaufbau von Google-QUIC
7.4.2 IETF-QUIC
7.5 HTTP/3 in Wireshark
7.5.1 HTTP/3 Header Kodierung
7.5.2 HTTP/3 Requests und Responses

8 Analyse von Server Message Block – CIFS
8.1 SMB/CIFS - Grundlagen
8.1.1 SMB Versionen – SMB
8.2 Typische SMB-Befehle
8.2.1 SMB2: Negotiate Protocol – 1
8.2.2 Session Setup AndX – Spezielle Logins 2
8.2.3 SMB und SMB2: Tree Connect
8.2.4 SMB2: Create
8.2.5 SMB2: Read
8.2.6 SMB2: Write
8.3 Zugriff auf Verzeichnisse mit SMB2
8.4 SMB2: Zugriff auf Dateien
8.5 Performancefaktoren für SMB/CIFS

9 Analyse von DNS
9.1 DNS-Analyse mit Wireshark
9.1.1 DNS Fehler im Wireshark
9.1.2 DNS-Antwortzeiten in Wireshark
9.1.3 Record Type HTTPS
9.2 DNS-Zonentransfer
9.3 Dynamisches DNS
9.4 DNS over HTTPS (DoH) und andere Varianten
9.4.1 DoH über HTTP/2 in Wireshark
9.4.2 DNS over HTTP/3 in Wireshark

10 Analyse von Citrix und RDP
10.1 Terminal Services
10.1.1 Analyse von TS-Sitzungen
10.2 Analyse von Citrix
10.2.1 ICA-Transportmodelle
10.2.2 Transportprotokolle für EDT
10.2.3 ICA-Protokoll in Wireshark
10.2.4 Gateway Services und Session Reliability
10.3 Remote Desktop Protocol
10.3.1 Verbindungsaufbau von RDP verschlüsselt
10.3.2 RDP über UDP

A Protokollreferenzen
A.1 Protokollreferenzen Ethernet
A.1.1 Ethertypes
A.1.2 Ethernet Unicast, Broadcast und Multicast
A.2 Protokollreferenzen - IPv4
A.2.1 Spezielle IPv4-Adressbereiche
A.2.2 Adressierung und ARP
A.2.3 IP Identification
A.2.4 IP-TTL
A.3 Protokollreferenzen TCP
A.3.1 Die Flags im Code-Feld
A.3.2 TCP-Verbindungen in Wireshark
A.3.3 TCP-Funktionen in Wireshark
A.3.4 Conversation Completeness
A.3.5 TCP-Statistiken
A.4 Protokollreferenzen UDP
A.4.1 Protokollreferenzen ICMPv4
A.4.2 ICMP-Fehlermeldungen
A.5 Protokollreferenzen DNS
A.5.1 DNS in Wireshark
A.5.2 DNS Fehler im Wireshark
A.6 Protokollreferenzen IPv6
A.6.1 IPv6-Adressbereiche
A.6.2 Adressierungskonzept
A.6.3 Struktur von Unicast-Adressen
A.6.4 Neighbor Discovery und Router Discovery
10.3.3 Stateless Autoconfiguration
10.4 Protokollreferenzen ICMPv6
10.4.1 ICMPv6-Fehlermeldungen
A.7 Security Grundlagen
A.7.1 Symmetrische Verschlüsselung
A.7.2 Asymmetrische Verschlüsselung
A.7.3 Hybride Verfahren
10.4.2 Authentisierung
10.4.3 Sichere Applikationen

ExperTeach Training & Consulting GmbH
Handelskai 94-96 · 1200 Wien · Telefon: +43 1 2350 383-0 · Fax: +43 1 2350 383-19 · info@experteach.at · www.experteach.at