

Wireshark Protokollanalyse

Praktischer Einsatz im Netzwerk

Wireshark ist ein einzigartiges Tool für die Paketanalyse von Netzwerken und Anwendungen. Als Open Source Anwendung ist es ein mächtiges Werkzeug für alle IT-Profis. Dieser Kurs bietet Ihnen eine solide Basis im Umgang mit Wireshark mit einer systematischen Einführung in die grundlegenden Funktionen sowie Methoden und Techniken zu Analyse und Fehlersuche von Netzwerken, Anwendungen auf Paketebene und die Abgrenzung von Netzwerk- und Applikationsproblemen. Darauf aufbauend erlernen Sie die Analyse und Fehlersuche in TCP/IP mit Wireshark im Detail. Besonders das Transportprotokoll TCP wird dabei genau unter die Lupe genommen. Der Kurs hat einen hohen Praxisanteil und versetzt Sie in die Lage, selbstständig komplexe Analysen mit Wireshark durchzuführen. Kursinhalte und Übungen basieren auf der jeweils aktuellen Wireshark Version. Gleichzeitig bereitet Sie dieser Kurs auf die offizielle Zertifizierung zum Wireshark Certified Analyst (WCA) der Wireshark Foundation vor.

Kursinhalt

- Arbeitsweise und Installation des Wireshark Analyzer
- Live Capture und Live Capture Einstellungen
- Anzeigeoptionen, Profile und Auswertungsmöglichkeiten
- Display-Filter und Capture Filter
- Voreinstellungen, Benutzerprofile und Namensauflösung
- Arbeiten mit Wireshark Command Line Tools
- Wireshark Statistiken
- Methoden und Techniken der Paketanalyse und Fehlersuche
- Auswerten und Eingrenzen typischer Netzwerk- und Anwendungsprobleme
- Protokollanalyse und Fehlersuche des TCP-Protokolls
- Analyse auf der Netzwerkschicht für IPv4 und IPv6

E-Book Das ausführliche deutschsprachige digitale Unterlagenpaket, bestehend aus PDF und E-Book, ist im Kurspreis enthalten.

Zielgruppe

Dieser Workshop eignet sich für alle IT-Fachkräfte, die Wireshark für Analysen und Fehlersuche in Netzwerk und Anwendungen einsetzen möchten und die notwendigen Grundlagen, Kenntnisse und Erfahrungen in der Paketanalyse erwerben möchten. Dieser Kurs bereitet Sie auf die offizielle Zertifizierung der Wireshark Foundation zum Wireshark Certified Analyst vor.

Voraussetzungen

Für eine erfolgreiche Teilnahme sollten Sie sattelfest im Ethernet- und TCP/IP-Umfeld sein. Der vorherige Besuch einer der beiden Kurse TCP/IP oder Enterprise Networks – Protokolle und Technologien in Campus und WAN ist sehr zu empfehlen.

Kursziel

Dieser Kurs bietet Ihnen eine systematische Einführung in die grundlegenden Funktionen und die Bedienung von Wireshark sowie wirksame Methoden und Techniken zu für die Paketanalyse. Darauf aufbauend erlernen Sie die Analyse und Fehlersuche in TCP/IP-basierten Netzwerken und Anwendungen mit Wireshark im Detail. Gleichzeitig bereitet Sie dieser Kurs auf die offizielle Zertifizierung zum Wireshark Certified Analyst (WCA) der Wireshark Foundation vor.

Zertifizierung

Dieser Kurs bereitet auf die offizielle Zertifizierung zum Wireshark Certified Analyst (WCA) der Wireshark Foundation vor.

Dieser Kurs im Web



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

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.

Training	Preise zzgl. MwSt.	
Termine in Deutschland	5 Tage	€ 2.995,-
Termine in Österreich	5 Tage	€ 2.995,-
Termine in der Schweiz	5 Tage	€ 3.790,-
Online Training	5 Tage	€ 2.995,-
Termin/Kursort	Kurs Sprache Deutsch	
09.03.-13.03.26	Frankfurt	24.08.-28.08.26 Online
09.03.-13.03.26	Online	24.08.-28.08.26 Zürich
13.04.-17.04.26	Online	28.09.-02.10.26 Frankfurt
13.04.-17.04.26	Wien	28.09.-02.10.26 Online
18.05.-22.05.26	Düsseldorf	02.11.-06.11.26 Berlin
18.05.-22.05.26	Online	02.11.-06.11.26 Hamburg
15.06.-19.06.26	Hamburg	02.11.-06.11.26 Online
15.06.-19.06.26	Online	02.11.-06.11.26 Online
20.07.-24.07.26	Online	30.11.-04.12.26 Düsseldorf
20.07.-24.07.26	Wien	30.11.-04.12.26 Online
24.08.-28.08.26	München	

Stand 04.03.2026



Inhaltsverzeichnis

Wireshark Protokollanalyse – Praktischer Einsatz im Netzwerk

1 Einführung in die Analyse mit Wireshark	4.2 Protokollhierarchie	6.6.2 TCP-Push
1.1 Was ist Wireshark?	4.3 Statistiken – Endpunkte	6.7 Tipps zur Fehlersuche
1.1.1 Was zeigt Wireshark?	4.4 Statistiken – Verbindungen	
1.1.2 Wireshark Architektur	4.5 Statistiken – I/O-Graph	7 TCP/IP-Analyse der Netzwerkschicht
1.2 Messen in Ethernet Netzwerken	4.6 Statistiken – Plots	7.1 Das Internet Protokoll im Überblick
1.2.1 Ethernet-Daten auswerten	4.7 TCP-Statistiken	7.1.1 Das Netzwerkprotokoll und seine Adressierung
1.3 Erste Schritte mit Wireshark	4.7.1 TCP Stream Graph – Round-Trip-Time	7.1.2 Adressierung und ARP
1.3.1 Aufzeichnungsoptionen – Capture Options	4.7.2 TCP Stream Graph – Durchsatz	7.1.3 ARP-Cache Erneuerung
1.3.2 Display Filter während der Aufzeichnung	4.7.3 TCP Stream Graph – Window Skalierung	7.1.4 Doppelte IP-Adressen
1.3.3 Speichern einer Aufzeichnung	4.7.4 TCP Stream Graph – Time Sequence Graph (Stevens)	7.2 Dynamic Host Configuration Protocol (DHCP)
1.3.4 Einstellung der Sprache	4.7.5 TCP Stream Graph – Time Sequence Graph (tcptrace)	7.2.1 DHCP Standardfunktionen: DORA
	4.8 Grenzen der Wireshark-Statistiken	7.2.2 Weitere DHCP-Funktionen
		7.2.3 DHCP-Relay
2 Mit Wireshark arbeiten	5 Analyse und Fehlersuche	7.3 MTU, PMTU, Fragmentierung
2.1 Anzeigooptionen und Navigation	5.1 Paketanalyse erklärt	7.3.1 MTU
2.1.1 Einstellungen – Preferences	5.1.1 Netzwerkdokumentation	7.3.2 IP-Fragmentierung
2.1.2 Ändern der Ansicht – Layout	5.1.2 Baselineing	7.3.3 PMTU und PMTU-Discovery
2.1.3 Einstellen von Schriftart und Farben	5.2 Fehler systematisch eingrenzen	7.3.4 Anpassung der MSS
2.1.4 Anpassen der Spalten – Columns	5.2.1 Troubleshooting-Methoden	7.4 Internet Control Message Protocol
2.1.5 Zeitoptionen	5.2.2 Bottom Up – Fehlersuche mit dem OSI-Modell	7.4.1 ICMP Echo und ICMP Echo Reply
2.1.6 Speichern der Einstellungen	5.3 Fehlersuche im Netz ohne Wireshark	7.4.2 ICMP-Fehlermeldungen
2.1.7 Paket finden – Find Packet	5.3.1 Duplex Mismatch im Ethernet	7.4.3 ICMP – Destination Unreachable
2.2 Voreinstellungen und Profile	5.3.2 Überlastung im Router oder am WAN	7.4.4 ICMP Time Exceeded
2.2.1 Benutzerprofile – Configuration Profiles	5.3.3 Paketfilter und Firewalls	7.5 Analyse von DNS
2.3 Anzeigefilter – Display Filter	5.4 Messtechnik mit Wireshark	7.5.1 Funktionsweise und Abfragen
2.3.1 Eingabe und Syntax	5.4.1 Messpunkte wählen	7.5.2 DNS in Wireshark
2.3.2 Das Filterergebnis	5.4.2 Port Monitoring – SPAN	7.5.3 Wichtige DNS-Typen
2.3.3 Grundlegende Anzeigefilter	5.4.3 Test Access Point – TAP	7.5.4 DNS Fehler in Wireshark
2.3.4 Vergleichsoperatoren	5.4.4 Wireshark auf dem Endergerät	7.5.5 DNS-Antwortzeiten in Wireshark
2.3.5 Layer Operator – mehrfache Felder	5.4.5 Messpunkt aus Trace File ermitteln	7.5.6 Typische DNS Probleme und Hintergründe
2.3.6 Filtern aus einer Liste von Werten	5.5 Netzwerkperformance mit Wireshark	7.6 IPv6 – Protokoll und Adressierung
2.3.7 Text filtern mit contains and matches	5.5.1 Round Trip Time – Initial RTT	7.6.1 IPv6-Protokollheader
2.3.8 Logische Operatoren	5.5.2 Round Trip Time – während einer Verbindung	7.6.2 Adressierungskonzept
2.3.9 Speichern von Anzeigefiltern	5.5.3 Service Response Time – SRT	7.6.3 IPv6-Adressformat und Schreibweise
2.3.10 „This“-Filter	5.5.4 Durchsatz und Overhead	7.6.4 Struktur von IPv6-Adressen
2.3.11 Kontext-Filter – Als Filter anwenden	5.6 Auswerten von Laufzeitproblemen	7.6.5 Bilden der Interface ID
2.3.12 Kontext-Filter – Verbindungsfilter	5.6.1 Hohe Round-Trip-Zeiten	7.6.6 Besondere Adressen
2.3.13 Filter aus Statistiken – Endpunkte	5.6.2 Hohe Service-Response-Zeiten	7.6.7 Struktur von Unicast-Adressen
2.3.14 Filter aus Statistiken – Verbindungen	5.7 Netzwerkprobleme und Anwendungsprobleme	7.6.8 Multicast Adressen
2.3.15 Follow TCP Stream	5.8 Applikationstypen und Performancefaktoren	7.7 Neighbor Discovery und Router Discovery
2.3.16 Anzeigefilter – Tipps aus der Praxis	5.8.1 Durchsatzorientierte Anwendungen	7.7.1 Neighbor Discovery
2.4 Mitschnittoptionen und Mitschnittfilter	5.8.2 Transaktionsorientierte Anwendungen	7.7.2 Duplicate Address Detection
2.4.1 Voreinstellungen für den Mitschnitt	5.8.3 Echtzeitanwendungen – Voice und Streaming	7.7.3 Router Discovery
2.4.2 Optionen der Aufzeichnung – Eingabe		7.8 Adressvergabe bei IPv6
2.4.3 Optionen der Aufzeichnung – Ausgabe		7.8.1 Statische Konfiguration
2.4.4 Optionen der Aufzeichnung – Optionen	6 TCP/IP-Analyse der Transportschicht	7.8.2 Stateless Autoconfiguration
2.4.5 Mitschnittfilter – Capture Filter	6.1 Transport über UDP und TCP	7.8.3 DHCPv6
2.4.6 Aufzeichnen von Dateisätzen – File Sets	6.1.1 Adressierung einer Applikation	7.8.4 Stateless DHCPv6
2.4.7 Mehrere Interfaces	6.1.2 UDP – Einfach und ungesichert	7.8.5 Stateful DHCPv6
2.5 Ein- und Ausgabe	6.1.3 TCP – Verbindungsorientiert und gesichert	
2.5.1 Ein- und Ausgabe – Speichern	6.2 TCP-Funktionen in Wireshark	A Referenzen
2.5.2 Speichern von gefilterten Paketen	6.2.1 TCP-Verbindungsaufbau	A.1 Protokollfelder, Referenzen und Filter
2.5.3 Ein- und Ausgabe – Exportieren	6.2.2 Sequenzierung von Daten	A.1.1 Ethernets
	6.2.3 Verbindungsabbau	A.1.2 Ethernet Unicast, Broadcast und Multicast
	6.2.4 TCP-Reset	A.1.3 Spezielle IPv4-Adressbereiche
3 Erweiterte Funktionen des Wireshark Analyzers	6.2.5 Sequenzierung in Wireshark	A.1.4 IPv6-Adressbereiche
3.1 Namensauflösung – Name Resolution	6.2.6 Conversation Completeness	A.2 Sniffing in VMware
3.1.1 Namensauflösung – Physikalische Adressen	6.3 TCP-Window und Performance	A.2.1 Promiscuous Mode für Standard vSwitch
3.1.2 Namensauflösung – Transportadressen	6.3.1 Sliding Window Mechanismus	A.2.2 Port Mirroring auf Distributed vSwitch
3.1.3 Namensauflösung – Netzwerkadressen	6.3.2 Window Size in Wireshark	A.2.3 ESXi CLI
3.2 Was ist Protocol Reassembly?	6.3.3 Window Mechanismus und Performance	A.3 Aufzeichnen mit dem Windows pktmon
3.2.1 Packet Reassembly am Beispiel von TCP	6.3.4 TCP Window Scaling Option	A.4 Messtechnik – VLAN-Tags
3.2.2 Packet Reassembly im Detail	6.3.5 Bytes in flight und Window Size	A.5 Messen in Wireless LAN Netzwerken
3.3 Farben in der Paketliste	6.4 Paketverluste, Retransmissions und Timing	A.5.1 Capture ohne Monitor Mode
3.3.1 Einfärbungsregeln – Coloring Rules	6.4.1 Wiederholung bei Paketverlust	A.5.2 Capture in Monitor Mode – Linux
3.3.2 Verbindung einfärben – Colorize Conversation	6.4.2 Retransmissions in Wireshark	A.6 Spezialfilter für den Mitschnitt
3.3.3 Mit Filter einfärben – Colorize with Filter	6.4.3 Eingrenzen von Retransmissions	A.7 Weitergehende Anzeigefilter
3.4 Kommandozeile – Command Line Tools	6.4.4 Selective Acknowledgments (SACK)	A.7.1 Filtern auf Bitebene
3.4.1 Command Line – capinfos	6.4.5 Retransmission – Timing	A.7.2 Reguläre Ausdrücke – Regex
3.4.2 Command Line – tshark	6.5 TCP-Probleme mit Wireshark auswerten	A.7.3 Beispiele für Display Filter
3.4.3 Command Line – mergcap	6.5.1 RTT und RTO in Wireshark	A.8 Windows Registry Einstellungen für TCP/IP
3.4.4 Command Line – editcap	6.5.2 Experteninformationen für TCP	A.9 Links zu Tools und Zusatzinfos
4 Wireshark Statistiken	6.6 Weitere TCP-Funktionen	
4.1 Statistiken -> Eigenschaften der Mitschnittdatei	6.6.1 Delayed Acknowledgments	

