

Wireshark Protokollanalyse

Praktischer Einsatz im Netzwerk

Die aus dem Ethereal-Projekt hervorgegangene Analysesoftware Wireshark ist ein mächtiges Werkzeug für Netzwerk- und Systemadministratoren. Dieser Kurs bildet eine solide Basis mit einer systematischen Einführung in die grundlegenden Funktionen und die Bedienung von Wireshark sowie Methoden und Techniken zu Monitoring, Analyse und Fehlersuche von Netzwerken auf Paketebene und die Abgrenzung von Netzwerk- und Applikationsproblemen. Darauf aufbauend erlernen die Teilnehmer die Analyse und Fehlersuche typischer Netzwerktechnologien wie Switched Ethernet und TCP/IP mit dem Wireshark im Detail. Besonders das Transportprotokoll TCP wird dabei genau unter die Lupe genommen. Der Kurs hat einen hohen Praxisanteil und versetzt die Teilnehmer in die Lage, selbstständig komplexe Analysen mit Wireshark durchzuführen. Kursinhalte und Übungen basieren auf der jeweils aktuellen Wireshark Version.

Kursinhalt

- Arbeitsweise des Wireshark Analyzer
- Live Capture und Live Capture Einstellungen
- Anzeigeeoptionen und Auswertungsmöglichkeiten
- Display-Filter und Capture Filter
- Erweiterte Funktionen: Voreinstellungen, Benutzerprofile und Namensauflösung
- Methoden und Techniken der Paketanalyse
- Wireshark Statistiken und Baselineing
- Fehlersuche: Eingrenzung von Netzwerk- und Anwendungsproblemen
- Analyse von Switched Ethernet: Duplex und Speed, Spanning Tree und VLAN-Analyse
- TCP/IP-Analyse der Netzwerkschicht für IPv4 und IPv6
- TCP/IP-Analyse der Transportschicht

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

Zielgruppe

Dieser Workshop eignet sich für Netzwerker, die lernen möchten, mit Hilfe des Wireshark komplexe Analysen und Fehlersuche von Netzwerk und Anwendungen durchzuführen.

Voraussetzungen

Die Teilnehmer sollten sattelfest im Ethernet- und TCP/IP-Umfeld sein. Der vorherige Besuch eines der beiden Kurse TCP/IP oder Ethernet, Routing & Switching - Technologiegrundlagen für Unternehmensnetzwerke ist sehr zu empfehlen.

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.de/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 | € 3.990,- | |
| Online Training | 5 Tage | € 2.995,- | |
| Termin/Kursort | Kurssprache Deutsch | | |
| 23.06.-27.06.25 | Düsseldorf | 12.01.-16.01.26 | Berlin |
| 23.06.-27.06.25 | Online | 12.01.-16.01.26 | Hamburg |
| 21.07.-25.07.25 | Frankfurt | 12.01.-16.01.26 | Online |
| 21.07.-25.07.25 | Online | 12.01.-16.01.26 | Online |
| 18.08.-22.08.25 | München | 09.02.-13.02.26 | München |
| 18.08.-22.08.25 | Online | 09.02.-13.02.26 | Online |
| 15.09.-19.09.25 | Berlin | 09.02.-13.02.26 | Zürich |
| 15.09.-19.09.25 | Hamburg | 09.03.-13.03.26 | Frankfurt |
| 15.09.-19.09.25 | Online | 09.03.-13.03.26 | Online |
| 13.10.-17.10.25 | Online | 13.04.-17.04.26 | Online |
| 13.10.-17.10.25 | Wien | 13.04.-17.04.26 | Wien |
| 13.10.-17.10.25 | Zürich | 18.05.-22.05.26 | Düsseldorf |
| 10.11.-14.11.25 | Frankfurt | 18.05.-22.05.26 | Online |
| 10.11.-14.11.25 | Online | 15.06.-19.06.26 | Hamburg |
| 01.12.-05.12.25 | Frankfurt | 15.06.-19.06.26 | Online |
| 01.12.-05.12.25 | Online | | |

Stand 27.05.2025



Inhaltsverzeichnis

Wireshark Protokollanalyse – Praktischer Einsatz im Netzwerk

| | | | | | |
|--------|--|-------|---|-------|---|
| 1 | Einführung in die Analyse mit Wireshark | 4.3 | Statistiken – Endpunkte | 7.1 | Das Internet Protokoll im Überblick |
| 1.1 | Was ist Wireshark? | 4.4 | Statistiken – Verbindungen | 7.1.1 | Das Netzwerkprotokoll und seine Adressierung |
| 1.1.1 | Was sieht Wireshark? | 4.5 | Statistiken – I/O-Graph | 7.1.2 | Adressierung und ARP |
| 1.1.2 | Wireshark Architektur | 4.6 | TCP-Statistiken | 7.1.3 | Doppelte IP-Adressen |
| 1.1.3 | Installation und Betrieb des Npcap-Treibers | 4.6.1 | TCP Stream Graph – Round-Trip-Time | 7.2 | Dynamic Host Configuration Protocol (DHCP) |
| 1.2 | Messen in Ethernet Netzwerken | 4.6.2 | TCP Stream Graph – Durchsatz | 7.2.1 | DHCP Standardfunktionen: DORA |
| 1.2.1 | Ethernet-Daten auswerten | 4.6.3 | TCP Stream Graph – Window Skalierung | 7.2.2 | Weitere DHCP-Funktionen |
| 1.3 | Messen in Wireless LAN Netzwerken | 4.6.4 | TCP Stream Graph – Time Sequence Graph (Stevens) | 7.2.3 | DHCP-Relay |
| 1.3.1 | Capture ohne Monitor Mode | 4.6.5 | TCP Stream Graph – Time Sequence Graph (tcptrace) | 7.2.4 | DHCP-Statistiken |
| 1.3.2 | Capture in Monitor Mode – Linux | 4.7 | Grenzen der Wireshark-Statistiken | 7.3 | MTU, PMTU, Fragmentierung |
| 1.4 | Erste Schritte mit Wireshark | 5 | Analyse und Fehlersuche | 7.3.1 | MTU |
| 1.4.1 | Aufzeichnungsoptionen – Capture Options | 5.1 | Paketanalyse erklärt | 7.3.2 | IP-Fragmentierung |
| 1.4.2 | Display Filter während der Aufzeichnung | 5.1.1 | Netzwerkdokumentation | 7.3.3 | PMTU und PMTU-Discovery |
| 1.4.3 | Speichern einer Aufzeichnung | 5.1.2 | Baselining | 7.3.4 | Anpassung der MSS |
| 1.4.4 | Einstellung der Sprache | 5.2 | Fehler systematisch eingrenzen | 7.4 | Internet Control Message Protocol |
| 2 | Mit Wireshark arbeiten | 5.2.1 | Troubleshooting-Methoden | 7.4.1 | ICMP Echo und ICMP Echo Reply |
| 2.1 | Anzeigeoptionen und Navigation | 5.2.2 | Bottom Up – Fehlersuche mit dem OSI-Modell | 7.4.2 | ICMP – Destination Unreachable |
| 2.1.1 | Einstellungen – Preferences | 5.3 | Fehlersuche im Netz ohne Wireshark | 7.4.3 | ICMP Time Exceeded |
| 2.1.2 | Ändern der Ansicht – Layout | 5.3.1 | Duplex Mismatch im Ethernet | 7.5 | Analyse von DNS |
| 2.1.3 | Einstellen von Schriftart und Farben | 5.3.2 | Überlastung im Router oder am WAN | 7.5.1 | Funktionsweise und Abfragen |
| 2.1.4 | Anpassen der Spalten – Columns | 5.3.3 | Paketfilter und Firewalls | 7.5.2 | DNS in Wireshark |
| 2.1.5 | Zeitoptionen | 5.4 | Messtechnik mit Wireshark | 7.5.3 | Wichtige DNS-Typen |
| 2.1.6 | Speichern der Einstellungen | 5.4.1 | Messpunkte wählen | 7.5.4 | DNS Fehler in Wireshark |
| 2.1.7 | Paket finden – Find Packet | 5.4.2 | Port Monitoring – SPAN | 7.5.5 | DNS-Antwortzeiten in Wireshark |
| 2.2 | Voreinstellungen und Profile | 5.4.3 | Test Access Point – TAP | 7.5.6 | Typische DNS Probleme und Hintergründe |
| 2.2.1 | Benutzerprofile – Configuration Profiles | 5.4.4 | Wireshark auf dem Endgerät | A | Lab-Übungen und Lösungen |
| 2.3 | Anzeigefilter – Display Filter | 5.4.5 | Auswerten von VLAN und VLAN Tags | A.1 | Lab Übungen – Kapitel 1 |
| 2.3.1 | Eingabe und Syntax | 5.5 | Sniffing in VMware | A.2 | Lab Übungen – Kapitel 2 |
| 2.3.2 | Das Filterergebnis | 5.5.1 | Promiscuous Mode für Standard vSwitch | A.2.1 | Lab Übung – Spalten anlegen |
| 2.3.3 | Grundlegende Anzeigefilter | 5.5.2 | Port Mirroring auf Distributed vSwitch | A.2.2 | Lab Übung – Profile (Configuration Profiles) |
| 2.3.4 | Vergleichsoperatoren | 5.5.3 | ESXi CLI | A.2.3 | Lab Übung – Anzeigefilter (Display Filter) |
| 2.3.5 | Layer Operator – mehrfache Felder | 5.6 | Netzwerkperformance mit Wireshark | A.2.4 | Opt. Lab Übung – Paket finden (Find Packet) |
| 2.3.6 | Filtern aus einer Liste von Werten | 5.6.1 | Round Trip Time – Initial RTT | A.3 | Lab Übungen – Kapitel 3 |
| 2.3.7 | Text filtern mit contains and matches | 5.6.2 | Round Trip Time – während einer Verbindung | A.3.1 | Lab Übung – Erweiterte Profileinstellungen |
| 2.3.8 | Logische Operatoren | 5.6.3 | Service Response Time – SRT | A.3.2 | Lab Übung – Kommandozeilentools – Teil 1 |
| 2.3.9 | Speichern von Anzeigefiltern | 5.6.4 | Durchsatz und Overhead | A.3.3 | Lab Übung – Kommandozeilentools – Teil 2 |
| 2.3.10 | „This“-Filter | 5.7 | Auswerten von Laufzeitproblemen | A.3.4 | Lab Übung – Kommandozeilentools – Teil 3 |
| 2.3.11 | Kontext-Filter – Als Filter anwenden | 5.7.1 | Hohe Round-Trip-Zeiten | A.3.5 | Lab Übung – Kommandozeilentools – Teil 4 |
| 2.3.12 | Kontext-Filter – Verbindungsfilter | 5.7.2 | Hohe Service-Response-Zeiten | A.4 | Lab Übungen – Kapitel 4 |
| 2.3.13 | Filter aus Statistiken – Endpunkte | 5.8 | Netzwerkprobleme und Anwendungsprobleme | A.4.1 | Lab Übung – Durchsatz und zeitlicher Verlauf |
| 2.3.14 | Filter aus Statistiken – Verbindungen | 5.9 | Applikationstypen und Performancefaktoren | A.4.2 | Lab Übung – Auswerten eines Speedtests |
| 2.3.15 | Follow TCP Stream | 5.9.1 | Durchsatzorientierte Anwendungen | A.5 | Lab Übungen – Kapitel 5 |
| 2.3.16 | Anzeigefilter – Tipps aus der Praxis | 5.9.2 | Transaktionsorientierte Anwendungen | A.5.1 | Lab Übung – Durchsatz |
| 2.4 | Mitschnittpoptionen und Mitschnittfilter | 5.9.3 | Echtzeitanwendungen – Voice und Streaming | A.5.2 | Lab Übung – Overhead |
| 2.4.1 | Voreinstellungen für den Mitschnitt | 6 | TCP/IP-Analyse der Transportschicht | A.5.3 | Lab Übung – Effizienz und Fehlanpassung |
| 2.4.2 | Optionen der Aufzeichnung – Eingabe | 6.1 | Transport über UDP und TCP | A.6 | Lab Übungen – Kapitel 6 |
| 2.4.3 | Optionen der Aufzeichnung – Ausgabe | 6.1.1 | Adressierung einer Applikation | A.6.1 | Lab Übung – TCP-Verbindungsaufbau |
| 2.4.4 | Optionen der Aufzeichnung – Optionen | 6.1.2 | UDP – Einfach und unsichert | A.6.2 | Lab Übung – TCP-Verbindungsaufbau |
| 2.4.5 | Mitschnittfilter – Capture Filter | 6.1.3 | TCP – Verbindungsorientiert und gesichert | A.6.3 | Lab Übung – TCP Zero Window |
| 2.4.6 | Aufzeichnen von Datensätzen – File Sets | 6.2 | TCP-Funktionen in Wireshark | A.6.4 | Lab Übung – TCP Bandwidthorientiert Delay Product |
| 2.4.7 | Mehrere Interfaces | 6.2.1 | TCP-Verbindungsaufbau | A.6.5 | Lab Übung – TCP Retransmissions – 1 |
| 2.5 | Ein- und Ausgabe | 6.2.2 | Sequenzierung von Daten | A.6.6 | Lab Übung – TCP Retransmissions – 2 |
| 2.5.1 | Ein- und Ausgabe – Speichern | 6.2.3 | Verbindungsabbau | A.6.7 | Optionale Lab Übung – Des Kunden Pein |
| 2.5.2 | Speichern von gefilterten Paketen | 6.2.4 | TCP-Reset | A.7 | Lab Übungen – Kapitel 7 |
| 2.5.3 | Ein- und Ausgabe – Exportieren | 6.2.5 | Sequenzierung in Wireshark | A.7.1 | Lab Übung – DHCP mit Windows 7 |
| 3 | Erweiterte Funktionen des Wireshark Analyzers | 6.3 | TCP-Window und Performance | A.7.2 | Lab Übung – DHCP Decline |
| 3.1 | Namensauflösung – Name Resolution | 6.3.1 | Sliding Window Mechanismus | A.7.3 | Lab Übung – IP-Fragmentierung |
| 3.1.1 | Namensauflösung – Physikalische Adressen | 6.3.2 | Window Size in Wireshark | A.7.4 | Lab Übung – PMTU Discovery |
| 3.1.2 | Namensauflösung – Transportadressen | 6.3.3 | Window Mechanismus und Performance | A.7.5 | Lab Übung – Black Hole |
| 3.1.3 | Namensauflösung – Netzwerkadressen | 6.3.4 | TCP Window Scaling Option | A.7.6 | Lab Übung – ICMP |
| 3.2 | Was ist Protocol Reassembly? | 6.3.5 | Bytes in flight und Window Size | A.7.7 | Lab Übung – DNS Probleme |
| 3.2.1 | Packet Reassembly am Beispiel von TCP | 6.4 | Paketverluste, Retransmissions und Timing | A.7.8 | Lab Übung – DNS Recursive Root Lookup |
| 3.2.2 | Packet Reassembly im Detail | 6.4.1 | Wiederholung bei Paketverlust | A.8 | Lösungen der Lab Übungen |
| 3.3 | Farben in der Paketliste | 6.4.2 | Retransmissions in Wireshark | A.8.1 | Lösungen der Lab Übungen – Kapitel 2 |
| 3.3.1 | Einfärbungsregeln – Coloring Rules | 6.4.3 | Eingrenzen von Retransmissions | A.8.2 | Lösungen der Lab Übungen – Kapitel 3 |
| 3.3.2 | Verbindung einfärben – Colorize Conversation | 6.4.4 | Selective Acknowledgements (SACK) | A.8.3 | Lösungen der Lab Übungen – Kapitel 4 |
| 3.3.3 | Mit Filter einfärben – Colorize with Filter | 6.4.5 | Retransmission – Timing | A.8.4 | Lösungen der Lab Übungen – Kapitel 5 |
| 3.4 | Kommandozeile – Command Line Tools | 6.5 | TCP-Probleme mit Wireshark auswerten | A.8.5 | Lösungen der Lab Übungen – Kapitel 6 |
| 3.4.1 | Command Line – capinfos | 6.5.1 | RTT und RTD in Wireshark | A.8.6 | Lösungen der Lab Übungen – Kapitel 7 |
| 3.4.2 | Command Line – tshark | 6.5.2 | Experteninformationen für TCP | B | Referenzen |
| 3.4.3 | Command Line – mergecap | 6.6 | Weitere TCP-Funktionen | B.1 | Aufzeichnen mit dem Windows pktmon |
| 3.4.4 | Command Line – editcap | 6.6.1 | Delayed Acknowledgements | B.2 | Links zu Tools und Zusatzinfos |
| 4 | Wireshark Statistiken | 6.6.2 | TCP-Push | B.3 | Weitergehende Anzeigefilter |
| 4.1 | Statistiken → Eigenschaften der Mitschnittdatei | 6.7 | Tipps zur Fehlersuche | B.3.1 | Filtern auf Bitebene |
| 4.2 | Protokollhierarchie | 7 | TCP/IP-Analyse der Netzwerkschicht | B.3.2 | Reguläre Ausdrücke – Regex |
| | | | | B.3.3 | Beispiele für Display Filter |

