

# Wireshark Applikationsanalyse

## Analyse und Optimierung typischer TCP/IP-Anwendungen

Neben guten TCP/IP-Kenntnissen und Erfahrung im Umgang mit Wireshark ist ein solides Verständnis über die Arbeitsweise der genutzten Anwendungen im Netzwerk die Voraussetzung für eine erfolgreiche Analyse. Dieser Kurs behandelt die Funktionsweise typischer TCP/IP-Anwendungen und deren Protokolle in Theorie und Praxis. Der Schwerpunkt liegt dabei auf der Analyse mit Wireshark zum schnellen Erkennen, Eingrenzen und Beheben von Fehlern.

### Kursinhalt

- Wireshark im Kurzüberblick
- TCP/IP-Analyse mit Wireshark – Die wichtigsten Punkte
- Anwendungen mit Wireshark analysieren
- Anwendungsperformance und Performance-Parameter
- Antwortzeiten auswerten und bewerten
- Analyse von HTTP
- Analyse von Secure Protocols – SSL/TLS, SSH und mehr
- Analyse von DNS und DNS-Serverprozessen
- Analyse von FTP und TFTP
- Analyse von Citrix und RDP
- Analyse von Multi-Tier-Datenbankanwendungen

**E-Book** Sie erhalten das ausführliche deutschsprachige Unterlagenpaket von ExperTeach – Print, E-Book und personalisiertes PDF! Bei Online-Teilnahme erhalten Sie das E-Book sowie das personalisierte PDF.

### Zielgruppe

Dieser Workshop eignet sich für Netzwerkadministratoren und alle technischen Mitarbeiter, die für Planung, Implementation und den fehlerfreien Betrieb von Netzwerken verantwortlich sind und sich speziell in die Wireshark-Analyse von TCP/IP-Anwendungen einarbeiten wollen.

### Voraussetzungen

Teilnehmer sollten solide Kenntnisse und praktische Erfahrungen im Umgang mit dem Wireshark sowie Kenntnisse von TCP/IP und IP-Adressierung besitzen. Der vorherige Besuch des Kurses Wireshark Protokollanalyse – Praktischer Einsatz im Netzwerk ist sehr zu empfehlen.

### Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: [www.experteach.ch/go/WISA](http://www.experteach.ch/go/WISA)

### 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	3 Tage	CHF 2.415,-
Online Training	3 Tage	CHF 2.415,-
Termin/Kursort	Kurssprache Deutsch	
11.09.-13.09.24	Hamburg	11.09.-13.09.24  Online

Stand 27.02.2024



**EXPERTeach**



# Inhaltsverzeichnis

## Wireshark Applikationsanalyse – Analyse und Optimierung typischer TCP/IP-Anwendungen

- 1 Anwendungen mit Wireshark analysieren**
  - 1.1 Wireshark im Kurzüberblick**
    - 1.1.1 Installation und Betrieb des Npcap-Treibers
    - 1.1.2 Messen in Ethernet Netzwerken
    - 1.1.3 Aufzeichnen mit Wireshark
    - 1.1.4 Mitschnittfilter – Capture Filter
    - 1.1.5 Einstellungen - Preferences
    - 1.1.6 Voreinstellungen und Profile
    - 1.1.7 Display Filter – Anzeigefilter
    - 1.1.8 Vergleichsoperatoren
    - 1.1.9 Logische Operatoren
    - 1.1.10 Speichern von Anzeigefiltern
  - 1.2 Anwendungstypen und Performancefaktoren**
    - 1.2.1 Durchsatzorientierte Anwendungen
    - 1.2.2 Transaktionsorientierte Anwendungen
    - 1.2.3 Echtzeitanwendungen – Voice und Streaming
  - 1.3 Netzwerkprobleme und Anwendungsprobleme**
    - 1.3.1 Typische Netzwerkprobleme
    - 1.3.2 Typische Anwendungsprobleme
  - 1.4 Vorgehen bei der Analyse (Analysetechniken)**
    - 1.4.1 Netzwerkprobleme erkennen und ausschließen
    - 1.4.2 Potentielle Probleme an Servern
    - 1.4.3 Der Einfluss von SAN oder NAS
    - 1.4.4 Client-Server-Architektur überprüfen
    - 1.4.5 Probleme in Anwendungen finden
- 2 Analyse von Secure Protocols – TLS und SSH**
  - 2.1 Security Grundlagen**
    - 2.1.1 Symmetrische Verschlüsselung
    - 2.1.2 Asymmetrische Verschlüsselung
    - 2.1.3 Hybride Verfahren
    - 2.1.4 Authentisierung
    - 2.1.5 Sichere Applikationen
  - 2.2 Sicherheit mit TLS**
    - 2.2.1 SSL und TLS
    - 2.2.2 Der TLS Protokollstapel
    - 2.2.3 Aufgaben von TLS
    - 2.2.4 Aufbau einer TLS-Verbindung für HTTPS
    - 2.2.5 TLS-Fehlersuche
    - 2.2.6 TLS-Decrypt über RSA-Keys – Beispiel HTTPS
    - 2.2.7 TLS-Decrypt über Logfiles
  - 2.3 Analyse von SSH**
    - 2.3.1 SSH Transport Protocol
    - 2.3.2 SSH Authentication Protocol
    - 2.3.3 SSH Connection Protocol
- 3 Analyse von HTTP, HTTP/2, QUIC und HTTP/3**
  - 3.1 HTTP und World Wide Web**
    - 3.1.1 HTTP-Versionen
    - 3.1.2 Kommunikationsverhalten von HTTP/1.0
    - 3.1.3 Kommunikationsverhalten von HTTP/1.1
    - 3.1.4 Kommunikationsverhalten von HTTP/2
  - 3.2 HTTP Version 1.1**
    - 3.2.1 Requests und Responses
    - 3.2.2 HTTP Request Header
    - 3.2.3 HTTP Responses
    - 3.3 Analyse von HTTP/1.1 mit Wireshark
      - 3.3.1 HTTP-Fehler in Wireshark
      - 3.3.2 HTTP-Antwortzeiten
      - 3.3.3 Browsertypen
      - 3.3.4 HTTP Connection Persistence
      - 3.3.5 Caching im Client
      - 3.3.6 HTTP Cookies
    - 3.4 HTTP/1.1 über Proxys**
      - 3.4.1 Explizite Proxys
      - 3.4.2 Transparente Proxys
      - 3.4.3 Reverse Proxys
      - 3.4.4 Aufgaben von Web Proxys
      - 3.4.5 Authentisierung mit Proxys
    - 3.5 HTTP Version 2**
      - 3.5.1 HTTP/2-Versionen
      - 3.5.2 HTTP over TCP (H2C)
      - 3.5.3 HTTP over TLS (H2)
      - 3.5.4 HTTP/2-Datenaustausch
      - 3.5.5 HTTP/2 - Verbindungsabbau
      - 3.5.6 Flusststeuerung mit HTTP/2-WINDOW
      - 3.5.7 HTTP/2 PRIORITY
    - 3.6 Google QUIC, IETF-QUIC und HTTP/3**
      - 3.6.1 Verbindungsaufbau von Google-QUIC
      - 3.6.2 IETF-QUIC
      - 3.6.3 HTTP/3 in Wireshark
  - 4 Analyse von DNS**
    - 4.1 DNS – Das Adressbuch
      - 4.1.1 Funktionsweise und Abfragen
      - 4.2 DNS-Analyse mit Wireshark
        - 4.2.1 Wichtige DNS-Typen
        - 4.2.2 DNS Kompression
        - 4.2.3 DNS Fehler im Wireshark
        - 4.2.4 DNS-Antwortzeiten in Wireshark
        - 4.2.5 Typische DNS Probleme und Hintergründe
      - 4.3 Primary und Secondary Name Server
        - 4.3.1 DNS-Zonentransfer
      - 4.4 Dynamisches DNS
      - 4.5 DNS over TLS (DoT) und DNS over HTTPS (DoH)
  - 5 Analyse von Datenbankanwendungen**
    - 5.1 Prinzipien und Komponenten
    - 5.2 Einfache Systeme
    - 5.3 Multi Tier - Umgebungen
      - 5.3.1 Kommunikationsmuster für Multi-Tier-Umgebungen
    - 5.3.2 Auswertung der Prozessdaten
    - 5.4 Auswerten der Antwortzeiten mit Wireshark
      - 5.4.1 Antwortzeiten Back-End
      - 5.4.2 Auswertetechnik Wireshark
  - 6 Analyse von Citrix und RDP**
    - 6.1 Terminal Services
      - 6.1.1 Analyse von TS-Sitzungen
    - 6.2 Analyse von Citrix
      - 6.2.1 Das ICA-Protokoll
      - 6.2.2 Session Reliability
    - 6.3 Remote Desktop Protocol**
      - 6.3.1 Verbindungsaufbau von RDP verschlüsselt
      - 6.3.2 RDP über UDP
  - A Lab-Übungen und Lösungen**
    - A.1 Lab Übungen – Kapitel 1**
      - A.1.1 Optionale Lab Übung: Anzeigefilter
    - A.2 Lab Übungen – Kapitel 2**
      - A.2.1 Lab Übung: TLS in Wireshark analysieren
      - A.2.2 Lab Übung: TLS Decrypt
      - A.2.3 Lab Übung: SSH
    - A.3 Lab Übungen – Kapitel 3**
      - A.3.1 Lab Übung: HTTP/2-Grundfunktionen und Decrypt
      - A.3.2 Lab Übung: HTTP/2 und QUIC im Überblick
      - A.3.3 Lab Übung: Untersuchung von QUIC
    - A.4 Lab Übungen – Kapitel 4**
      - A.4.1 Lab Übung: DNS-Probleme 1
      - A.4.2 Lab Übung: DNS-Probleme-2
      - A.4.3 Lab Übung: DNS-Probleme-3
    - A.5 Lab Übungen – Kapitel 5**
      - A.5.1 Lab Übung: Datenbankabfrage für Bibliothekensoftware
      - A.5.2 Lab Übung: Langsame Datenbankabfrage für Vertriebssoftware
      - A.5.3 Lab Übung: Datenbankabfragen im Produktionsumfeld
    - A.6 Lab Übungen – Kapitel 6**
      - A.6.1 Lab Übungen – Anhang B
        - A.7.1 Lab Übung: FTP-Basisfunktionen
        - A.7.2 Lab Übung: FTP-Probleme 1
        - A.7.3 Lab Übung: FTP-Probleme 2
        - A.7.4 Lab Übung: TFTP-Basisfunktionen
        - A.7.5 Lab Übung: FTP vs. TFTP - Wer ist schneller?
        - A.7.6 Lab Übung: Sichere File Transfers
      - A.8 Lösungen der Lab Übungen
        - A.8.1 Lösungen der Lab Übungen – Kapitel 1
        - A.8.2 Lösungen der Lab Übungen – Kapitel 2
        - A.8.3 Lösungen der Lab Übungen – Kapitel 3
        - A.8.4 Lösungen der Lab Übungen – Kapitel 4
        - A.8.5 Lösungen der Lab Übungen – Kapitel 5
        - A.8.6 Lösungen der Lab Übungen – Anhang B
    - B Analyse von File Transfers**
      - B.1 Analyse von FTP**
        - B.1.1 Active FTP
        - B.1.2 Passive FTP
        - B.1.3 FTP-Fehler und Antwortcodes
      - B.2 Analyse von TFTP**
        - B.2.1 TFTP Basisfunktionen
        - B.2.2 TFTP-Probleme und Fehlermeldungen
        - B.2.3 TFTP Optionen
      - B.3 FTP und TFTP im Vergleich**
      - B.4 Sichere File Transfers**
        - B.4.1 Secure Copy – Verschlüsselte Übertragung

