

# 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-Applikationen 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.de/go/WISA](http://www.experteach.de/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.	
<b>Termine in Deutschland</b>	<b>3 Tage</b>	<b>€ 2.195,-</b>	
<b>Online Training</b>	<b>3 Tage</b>	<b>€ 2.195,-</b>	
<b>Termin/Kursort</b>	<b>Kurssprache Deutsch</b>		
11.09.-13.09.24	Hamburg	24.03.-26.03.25	Hamburg
11.09.-13.09.24	Online	24.03.-26.03.25	Online

Stand 07.05.2024



**EXPERTeach**



# Inhaltsverzeichnis

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

<b>1 Anwendungen mit Wireshark analysieren</b>	<b>3.2.3</b> HTTP Responses	<b>6.2.1</b> Das ICA-Protokoll
<b>1.1</b> Wireshark im Kurzüberblick	<b>3.3</b> Analyse von HTTP/1.1 mit Wireshark	<b>6.2.2</b> Session Reliability
<b>1.1.1</b> Installation und Betrieb des Npcap-Treibers	<b>3.3.1</b> HTTP-Fehler in Wireshark	<b>6.3</b> Remote Desktop Protocol
<b>1.1.2</b> Messen in Ethernet Netzwerken	<b>3.3.2</b> HTTP-Antwortzeiten	<b>6.3.1</b> Verbindungsaufbau von RDP verschlüsselt
<b>1.1.3</b> Aufzeichnen mit Wireshark	<b>3.3.3</b> Browsertypen	<b>6.3.2</b> RDP über UDP
<b>1.1.4</b> Mitschnittfilter – Capture Filter	<b>3.3.4</b> HTTP Connection Persistence	
<b>1.1.5</b> Einstellungen - Preferences	<b>3.3.5</b> Caching im Client	<b>A Lab-Übungen und Lösungen</b>
<b>1.1.6</b> Voreinstellungen und Profile	<b>3.3.6</b> HTTP Cookies	<b>A.1</b> Lab Übungen – Kapitel 1
<b>1.1.7</b> Display Filter – Anzeigefilter	<b>3.4</b> HTTP/1.1 über Proxys	<b>A.1.1</b> Optionale Lab Übung: Anzeigefilter
<b>1.1.8</b> Vergleichsoperatoren	<b>3.4.1</b> Explizite Proxys	<b>A.2</b> Lab Übungen – Kapitel 2
<b>1.1.9</b> Logische Operatoren	<b>3.4.2</b> Transparente Proxys	<b>A.2.1</b> Lab Übung: TLS in Wireshark analysieren
<b>1.1.10</b> Speichern von Anzeigefiltern	<b>3.4.3</b> Reverse Proxys	<b>A.2.2</b> Lab Übung: TLS Decrypt
<b>1.2</b> Anwendungstypen und Performancefaktoren	<b>3.4.4</b> Aufgaben von Web Proxys	<b>A.2.3</b> Lab Übung: SSH
<b>1.2.1</b> Durchsatzorientierte Anwendungen	<b>3.4.5</b> Authentisierung mit Proxys	<b>A.3</b> Lab Übungen – Kapitel 3
<b>1.2.2</b> Transaktionsorientierte Anwendungen	<b>3.5</b> HTTP Version 2	<b>A.3.1</b> Lab Übung: HTTP/2-Grundfunktionen und Decrypt
<b>1.2.3</b> Echtzeitanwendungen – Voice und Streaming	<b>3.5.1</b> HTTP/2-Versionen	<b>A.3.2</b> Lab Übung: HTTP/2 und QUIC im Überblick
<b>1.3</b> Netzwerkprobleme und Anwendungsprobleme	<b>3.5.2</b> HTTP over TCP (H2C)	<b>A.3.3</b> Lab Übung: Untersuchung von QUIC
<b>1.3.1</b> Typische Netzwerkprobleme	<b>3.5.3</b> HTTP over TLS (H2)	<b>A.4</b> Lab Übungen – Kapitel 4
<b>1.3.2</b> Typische Anwendungsprobleme	<b>3.5.4</b> HTTP/2-Datenaustausch	<b>A.4.1</b> Lab Übung: DNS-Probleme 1
<b>1.4</b> Vorgehen bei der Analyse (Analysetechniken)	<b>3.5.5</b> HTTP/2 - Verbindungsabbau	<b>A.4.2</b> Lab Übung: DNS-Probleme-2
<b>1.4.1</b> Netzwerkprobleme erkennen und ausschließen	<b>3.5.6</b> Flusststeuerung mit HTTP/2-WINDOW	<b>A.4.3</b> Lab Übung: DNS-Probleme-3
<b>1.4.2</b> Potentielle Probleme an Servern	<b>3.5.7</b> HTTP/2 PRIORITY	<b>A.5</b> Lab Übungen – Kapitel 5
<b>1.4.3</b> Der Einfluss von SAN oder NAS	<b>3.6</b> Google QUIC, IETF-QUIC und HTTP/3	<b>A.5.1</b> Lab Übung: Datenbankabfrage für Bibliothekensoftware
<b>1.4.4</b> Client-Server-Architektur überprüfen	<b>3.6.1</b> Verbindungsaufbau von Google-QUIC	<b>A.5.2</b> Lab Übung: Langsame Datenbankabfrage für Vertriebssoftware
<b>1.4.5</b> Probleme in Anwendungen finden	<b>3.6.2</b> IETF-QUIC	<b>A.5.3</b> Lab Übung: Datenbankabfragen im Produktionsumfeld
	<b>3.6.3</b> HTTP/3 in Wireshark	<b>A.6</b> Lab Übungen – Kapitel 6
<b>2 Analyse von Secure Protocols – TLS und SSH</b>	<b>4 Analyse von DNS</b>	<b>A.7</b> Lab Übungen – Anhang B
<b>2.1</b> Security Grundlagen	<b>4.1</b> DNS – Das Adressbuch	<b>A.7.1</b> Lab Übung: FTP-Basisfunktionen
<b>2.1.1</b> Symmetrische Verschlüsselung	<b>4.1.1</b> Funktionsweise und Abfragen	<b>A.7.2</b> Lab Übung: FTP-Probleme 1
<b>2.1.2</b> Asymmetrische Verschlüsselung	<b>4.2</b> DNS-Analyse mit Wireshark	<b>A.7.3</b> Lab Übung: FTP-Probleme 2
<b>2.1.3</b> Hybride Verfahren	<b>4.2.1</b> Wichtige DNS-Typen	<b>A.7.4</b> Lab Übung: TFTP-Basisfunktionen
<b>2.1.4</b> Authentisierung	<b>4.2.2</b> DNS Kompression	<b>A.7.5</b> Lab Übung: FTP vs. TFTP - Wer ist schneller?
<b>2.1.5</b> Sichere Applikationen	<b>4.2.3</b> DNS Fehler im Wireshark	<b>A.7.6</b> Lab Übung: Sichere File Transfers
<b>2.2</b> Sicherheit mit TLS	<b>4.2.4</b> DNS-Antwortzeiten in Wireshark	<b>A.8</b> Lösungen der Lab Übungen
<b>2.2.1</b> SSL und TLS	<b>4.2.5</b> Typische DNS Probleme und Hintergründe	<b>A.8.1</b> Lösungen der Lab Übungen – Kapitel 1
<b>2.2.2</b> Der TLS Protokollstapel	<b>4.3</b> Primary and Secondary Name Server	<b>A.8.2</b> Lösungen der Lab Übungen – Kapitel 2
<b>2.2.3</b> Aufgaben von TLS	<b>4.3.1</b> DNS-Zonentransfer	<b>A.8.3</b> Lösungen der Lab Übungen – Kapitel 3
<b>2.2.4</b> Aufbau einer TLS-Verbindung für HTTPS	<b>4.4</b> Dynamisches DNS	<b>A.8.4</b> Lösungen der Lab Übungen – Kapitel 4
<b>2.2.5</b> TLS-Fehlersuche	<b>4.5</b> DNS over TLS (DoT) und DNS over HTTPS (DoH)	<b>A.8.5</b> Lösungen der Lab Übungen – Kapitel 5
<b>2.2.6</b> TLS-Decrypt über RSA-Keys – Beispiel HTTPS		<b>A.8.6</b> Lösungen der Lab Übungen – Anhang B
<b>2.2.7</b> TLS-Decrypt über Logfiles		
<b>2.3</b> Analyse von SSH	<b>5 Analyse von Datenbankanwendungen</b>	<b>B Analyse von File Transfers</b>
<b>2.3.1</b> SSH Transport Protocol	<b>5.1</b> Prinzipien und Komponenten	<b>B.1</b> Analyse von FTP
<b>2.3.2</b> SSH Authentication Protocol	<b>5.2</b> Einfache Systeme	<b>B.1.1</b> Active FTP
<b>2.3.3</b> SSH Connection Protocol	<b>5.3</b> Multi Tier - Umgebungen	<b>B.1.2</b> Passive FTP
	<b>5.3.1</b> Kommunikationsmuster für Multi-Tier-Umgebungen	<b>B.1.3</b> FTP-Fehler und Antwortcodes
<b>3 Analyse von HTTP, HTTP/2, QUIC und HTTP/3</b>	<b>5.3.2</b> Auswertung der Prozessdaten	<b>B.2</b> Analyse von TFTP
<b>3.1</b> HTTP und World Wide Web	<b>5.4</b> Auswerten der Antwortzeiten mit Wireshark	<b>B.2.1</b> TFTP Basisfunktionen
<b>3.1.1</b> HTTP-Versionen	<b>5.4.1</b> Antwortzeiten Back-End	<b>B.2.2</b> TFTP-Probleme und Fehlermeldungen
<b>3.1.2</b> Kommunikationsverhalten von HTTP/1.0	<b>5.4.2</b> Auswertetechnik Wireshark	<b>B.2.3</b> TFTP Optionen
<b>3.1.3</b> Kommunikationsverhalten von HTTP/1.1		<b>B.3</b> FTP und TFTP im Vergleich
<b>3.1.4</b> Kommunikationsverhalten von HTTP/2	<b>6 Analyse von Citrix und RDP</b>	<b>B.4</b> Sichere File Transfers
<b>3.2</b> HTTP Version 1.1	<b>6.1</b> Terminal Services	<b>B.4.1</b> Secure Copy – Verschlüsselte Übertragung
<b>3.2.1</b> Requests und Responses	<b>6.1.1</b> Analyse von TS-Sitzungen	
<b>3.2.2</b> HTTP Request Header	<b>6.2</b> Analyse von Citrix	

