

# Wireshark & Voice over IP

## Analysis of call flow and media streams

Voice over IP is an application that is particularly prone to errors due to its special requirements. Special skills and tools are required to analyze problems with connection setup, connection stability or voice quality. A VoIP environment also uses a variety of standardized and manufacturer-specific signaling protocols for voice, video and instant messaging. In this course, participants will learn about the functions and analysis of the most important VoIP processes and protocols with the help of Wireshark. One focus is on the practical detection of typical problems.

### Course Contents

- Overview of VoIP - motivation and basics
- VoIP - standards, components and protocols
- Media streams - functions, codecs, RTP and RTCP
- Call signaling with Wireshark - SIP, Skinny and H.323
- Wireshark evaluations for VoIP
- Practical analysis of SIP - registration, authentication, connection setup
- Performance features with SIP - forwarding, conference, instant messaging, etc.
- Analysis of dropped calls and voice quality with Wireshark
- Fax over IP - How it works!
- Quality of service for VoIP applications
- Analysis of problems with NAT and firewalls

**E-Book** You will receive the comprehensive documentation package from ExperTeach – printed documentation, e-book, and personalized PDF! As online participant, you will receive the e-book and the personalized PDF.

### Target Group

The course is designed for networkers who are responsible for the operation and troubleshooting of networks for VoIP and want to analyze VoIP applications with the help of Wireshark.

### Prerequisites

Participants should have sound practical experience in using Wireshark as well as knowledge of TCP/IP and IP addressing. Prior attendance of the basic course Wireshark Protocol Analysis - Practical Use in the Network is highly recommended.

### This Course in the Web



You can find the up-to-date information and options for ordering under the following link:

[www.expertech-training.com/go/WISU](http://www.expertech-training.com/go/WISU)

### Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in a non-committal manner. This can also be done by phone under +49 6074/4868-0.

### Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

### Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

| Training                      |                           | Prices, excl. of V.A.T. |                |
|-------------------------------|---------------------------|-------------------------|----------------|
| <b>Classes in Germany</b>     |                           | <b>3 Days</b>           | <b>€ 2,195</b> |
| <b>Classes in Austria</b>     |                           | <b>3 Days</b>           | <b>€ 2,195</b> |
| <b>Classes in Switzerland</b> |                           | <b>3 Days</b>           | <b>€ 2,850</b> |
| <b>Online Training</b>        |                           | <b>3 Days</b>           | <b>€ 2,195</b> |
| Date/course venue             | Course language           | German                  |                |
| 06/05-08/05/24  Frankfurt     | 28/08-30/08/24  Online    |                         |                |
| 06/05-08/05/24  Online        | 16/10-18/10/24  München   |                         |                |
| 10/06-12/06/24  Hamburg       | 16/10-18/10/24  Online    |                         |                |
| 10/06-12/06/24  Online        | 16/10-18/10/24 Zürich     |                         |                |
| 10/06-12/06/24 Zürich         | 20/11-22/11/24  Online    |                         |                |
| 17/07-19/07/24  Düsseldorf    | 20/11-22/11/24  Wien      |                         |                |
| 17/07-19/07/24  Online        | 16/12-18/12/24  Frankfurt |                         |                |
| 28/08-30/08/24 Berlin         | 16/12-18/12/24  Online    |                         |                |
| 28/08-30/08/24  Hamburg       |                           |                         |                |

Status 04/23/2024



# Table of Contents

## Wireshark & Voice over IP – Analysis of call flow and media streams

|   |   |  |
|---|---|--|
| <b>1 Motivation und Grundlagen</b>                    | <b>3 SIP Signalisierung mit Wireshark</b>                     | <b>4.4.5 T.38 – Fax in Echtzeit</b>                                |
| <b>1.1 VoIP – Anforderungen</b>                       | <b>3.1 SIP – Ein Überblick</b>                                | <b>4.4.6 Fehlerbilder bei Fax over IP</b>                          |
| <b>1.2 Architektur von VoIP</b>                       | <b>3.1.1 Standardisierung</b>                                 | <b>4.4.7 Die Analyse Schritt für Schritt</b>                       |
| <b>1.2.1 Endgeräte</b>                                | <b>3.1.2 SIP im ISO/OSI-Modell</b>                            | <b>4.5 Quality of Service im Blick</b>                             |
| <b>1.2.2 Bausteine – Protokolle</b>                   | <b>3.1.3 Adressierung: SIP URI und TEL URI</b>                | <b>4.5.1 QoS-Konzepte</b>  |
| <b>1.2.3 Datenströme</b>                              | <b>3.2 Komponenten der SIP-Architektur</b>                    | <b>4.5.2 QoS im LAN</b>  |
| <b>1.2.4 Signalisierung</b>                           | <b>3.2.1 Die Endgeräte: User Agents</b>                       | <b>4.5.3 DiffServ</b>  |
| <b>1.2.5 Medienströme</b>                             | <b>3.2.2 Der SIP Proxy</b>                                    | <b>4.5.4 QoS mit Wireshark überprüfen</b>                          |
| <b>1.3 Video over IP in Unternehmen</b>               | <b>3.2.3 SIP-Gateways</b>                                     |  |
| <b>1.3.1 Aufgaben für Videotelefonie</b>              | <b>3.3 Der Protokoll-Aufbau</b>                               | <b>A Lab-Übungen und Lösungen</b>                                  |
| <b>1.3.2 Signalisierung und Medien</b>                | <b>3.3.1 Aufbau von SIP-Nachrichten</b>                       | <b>A.1 Lab Übungen – Kapitel 1</b>                                 |
| <b>1.3.3 Videoströme über RTP</b>                     | <b>3.3.2 SIP Requests – Die SIP-Methoden</b>                  | <b>A.2 Lab Übungen – Kapitel 2</b>                                 |
| <b>1.4 Wireshark im Kurzüberblick</b>                 | <b>3.3.3 Die Requests von INVITE bis BYE</b>                  | <b>A.2.1 Lab Übung: RTP-Grundfunktionen</b>                        |
| <b>1.4.1 Messen in Ethernet Netzwerken</b>            | <b>3.3.4 SIP Responses</b>                                    | <b>A.2.2 Lab Übung – RTP Operation</b>                             |
| <b>1.4.2 Erstes Aufzeichnen mit Wireshark</b>         | <b>3.4 SDP – Das Session Description Protocol</b>             | <b>A.2.3 Lab Übung – RTP etwas schlechter</b>                      |
| <b>1.4.3 Mitschnittfilter – Capture Filter</b>        | <b>3.5 Registrierung und Authentisierung</b>                  | <b>A.2.4 Lab Übung – RTP Probleme eingrenzen</b>                   |
| <b>1.4.4 Einstellungen – Preferences</b>              | <b>3.5.1 SIP-Registrierung – Abläufe</b>                      | <b>A.3 Lab Übungen – Kapitel 3</b>                                 |
| <b>1.4.5 Voreinstellungen und Profile</b>             | <b>3.5.2 Registrierung ohne Authentisierung</b>               | <b>A.3.1 Lab Übung: SIP-Registrierung</b>                          |
| <b>1.4.6 Anzeigefilter – Display Filter</b>           | <b>3.5.3 Register mit Authentisierung</b>                     | <b>A.3.2 Lab Übung: SIP – Basic Call mit Wireshark</b>             |
|   | <b>3.5.4 Probleme bei der Registrierung</b>                   | <b>A.4 Lab Übungen – Kapitel 3 – SIP-Labor</b>                     |
| <b>2 Medienströme mit RTP</b>                         | <b>3.6 Basisfunktion – Basic Call</b>                         | <b>A.4.1 Registrierung und Basic Call</b>                          |
| <b>2.1 Das Realtime Transport Protocol</b>            | <b>3.6.1 SIP-Invite über klassischen Proxy</b>                | <b>A.4.2 Auswahl des Codecs</b>                                    |
| <b>2.1.1 Sprache mit Daten übertragen</b>             | <b>3.6.2 SIP-Server terminiert den Dialog</b>                 | <b>A.4.3 RTP-Proxy</b>   |
| <b>2.1.2 Der Aufbau von RTP-Paketen</b>               | <b>3.6.3 Domainumgebungen und DNS</b>                         | <b>A.4.4 Call Halten</b>   |
| <b>2.1.3 Das RTP-Protokoll</b>                        | <b>3.6.4 SIP – Basic Call in Wireshark</b>                    | <b>A.4.5 Einfache Dreierkonferenz</b>                              |
| <b>2.1.4 RTP-Profile</b>                              | <b>3.7 SIP Auswertung mit Wireshark</b>                       | <b>A.4.6 Call Transfer</b>   |
| <b>2.2 Realtime Transport Control Protocol (RTCP)</b> | <b>3.7.1 SIP – Nützliche Filter</b>                           | <b>A.5 Lab Übungen – Kapitel 4</b>                                 |
| <b>2.2.1 Klassisches RTCP</b>                         | <b>3.7.2 VoIP Calls – Statistiken</b>                         | <b>A.6 Lab Übungen – Anhang B</b>                                  |
| <b>2.2.2 RTCP Extended Reports (RTCP XR)</b>          | <b>3.7.3 SIP Statistiken</b>                                  | <b>A.6.1 Lab Übung: H.323 Basic Call mit Wireshark</b>             |
| <b>2.3 Messen von Sprachqualität</b>                  | <b>3.8 SIP für Video</b>                                      | <b>A.6.2 Lab Übung: H.323 Fast Start und Tunneling</b>             |
| <b>2.3.1 Mean Opinion Score (MOS)</b>                 |   | <b>A.7 Lösungen der Lab Übungen</b>                                |
| <b>2.3.2 Laufzeiten – Ende zu Ende</b>                | <b>4 VoIP – Praxis und Fehlersuche</b>                        | <b>A.7.1 Lösungen der Lab Übungen – Kapitel 1</b>                  |
| <b>2.3.3 Jitter und Jitter Buffer</b>                 | <b>4.1 Typische Verbindungsprobleme</b>                       | <b>A.7.2 Lösungen der Lab Übungen – Kapitel 2</b>                  |
| <b>2.3.4 Packet Loss und Concealment</b>              | <b>4.1.1 Keine Registrierung des Endgerätes</b>               | <b>A.7.3 Lösungen der Lab Übungen – Kapitel 3</b>                  |
| <b>2.4 RTP mit Wireshark auswerten</b>                | <b>4.1.2 Kein Verbindungsaufbau</b>                           | <b>A.7.4 Lösungen der Lab Übungen – Kapitel 5</b>                  |
| <b>2.4.1 RTP mit Wireshark aufzeichnen</b>            | <b>4.1.3 Langsamer Verbindungsaufbau</b>                      | <b>A.7.5 Lösungen der Lab Übungen – Anhang B</b>                   |
| <b>2.4.2 RTP dekodieren</b>                           | <b>4.1.4 Fehlende Leistungsmerkmale</b>                       |  |
| <b>2.4.3 RTP Statistiken</b>                          | <b>4.2 Typische Sprachprobleme</b>                            | <b>B H.323 Lab-Übungen und Lösungen</b>                            |
| <b>2.4.4 RTP Stream Analyse</b>                       | <b>4.2.1 Schlechte und schwankende Sprachqualität</b>         | <b>B.1 H.323 – Architektur</b>                                     |
| <b>2.5 DTMF – Tastentöne über VoIP</b>                | <b>4.2.2 Keine Sprache übers Netz</b>                         | <b>B.1.1 Das H.323-Terminal – Die Funktionen der Endgeräte</b>     |
| <b>2.5.1 DTMF Inband</b>                              | <b>4.3 Sicherheitsaspekte</b>                                 | <b>B.1.2 Das H.323-Gateway</b>                                     |
| <b>2.5.2 RTP-Event nach RFC 4733 (RFC 2833)</b>       | <b>4.3.1 Verschlüsselung für Signalisierung und Nutzdaten</b> | <b>B.1.3 Der H.323-Gatekeeper – Adressumsetzung und Management</b> |
| <b>2.5.3 DTMF über SIP Info</b>                       | <b>4.3.2 SRTP</b>   | <b>B.1.4 H.323-Prozeduren im TCP/IP-Protokollstack</b>             |
| <b>2.6 Sprachpausen und VAD</b>                       | <b>4.3.3 SIPS - SIP über TLS</b>                              | <b>B.2 H.323 – Ein Basic Call</b>                                  |
| <b>2.6.1 Sprachpausen und RTP</b>                     | <b>4.3.4 VoIP und Stateful Firewalls</b>                      | <b>B.2.1 RAS – Die Gatekeeper-Endpoint-Kommunikation</b>           |
| <b>2.6.2 Comfort Noise</b>                            | <b>4.3.5 NAT – Network Address Translation</b>                | <b>B.2.2 Die Phasen eines Calls</b>                                |
| <b>2.7 Videoströme über RTP</b>                       | <b>4.4 Fax über IP – So funktioniert es!</b>                  | <b>B.2.3 Optionen für H.245: Tunneling und Fast Start</b>          |
| <b>2.7.1 Video-Codecs</b>                             | <b>4.4.1 Besonderheiten bei der Faxübertragung</b>            | <b>B.3 H.323 – Nützliche Filter</b>                                |
| <b>2.7.2 Videoparameter</b>                           | <b>4.4.2 Typische Abläufe</b>                                 |  |
| <b>2.7.3 Video und Audio gemeinsam</b>                | <b>4.4.3 Das Fax als normaler VoIP Call</b>                   |  |
|   | <b>4.4.4 T.37 – Fax als E-Mail-Anhang</b>                     |  |

