

# Schulung *Wireshark*

## Factsheet

---

**THEMA** Netzwerkanalyse mit Wireshark

---

**KURZBESCHREIBUNG** Wireshark ist ein frei verfügbares und mächtiges Tool für die Analyse von Netzwerkverkehr. Insbesondere bei der Fehlersuche kann Wireshark wertvolle Erkenntnisse liefern. Diese Modul führt in die Grundlagen ein und erklärt die für die Fehlersuche interessanten Funktionen.

---

**ZIELGRUPPE** Netzwerkadministratoren, Softwareentwickler

---

**VORAUSSETZUNG** Grundkenntnisse Netzwerke  
Notebook mit Ethernetport und Admin Rechten

---

**AUFBAUENDE MODULE** -

---

**DAUER** 1 Halbtage, inkl. Übungen, Fragen und Diskussion

---

**KURSART** Frontalschulung, Übungen, Diskussion

## Inhalt

- Eigenschaften paketorientierter Netzwerke
- Wireshark und das Schichtenmodell
- Filter (*Capture* und *Display*)
- Adressauflösung
- Zeitdarstellung
- statistische Analysen
- Analyse wichtiger Protokolle (ARP, DHCP, DNS, http, ...)
- Analyse TCP
- Analyse *Voice over IP*
- Möglichkeiten zur Analyse verschlüsselter Datenströme

## Ziele

Nach der Absolvierung des Moduls können die Teilnehmende Wireshark zur Analyse von Netzwerkverkehr einsetzen. Es ist bekannt, wie relevante Pakete beim Aufzeichnen als auch beim Anzeigen gefiltert werden können. Weiter haben sie gelernt, wie bei der Fehlersuche in verschiedenen Szenarien vorgegangen werden kann.