

# WLAN-Vorlesung

## Analyse mit Wireshark Teil-1

# Inhalt

- Rechtliches
- Wireshark-Grundlagen
- Installation
- WLAN-Messung

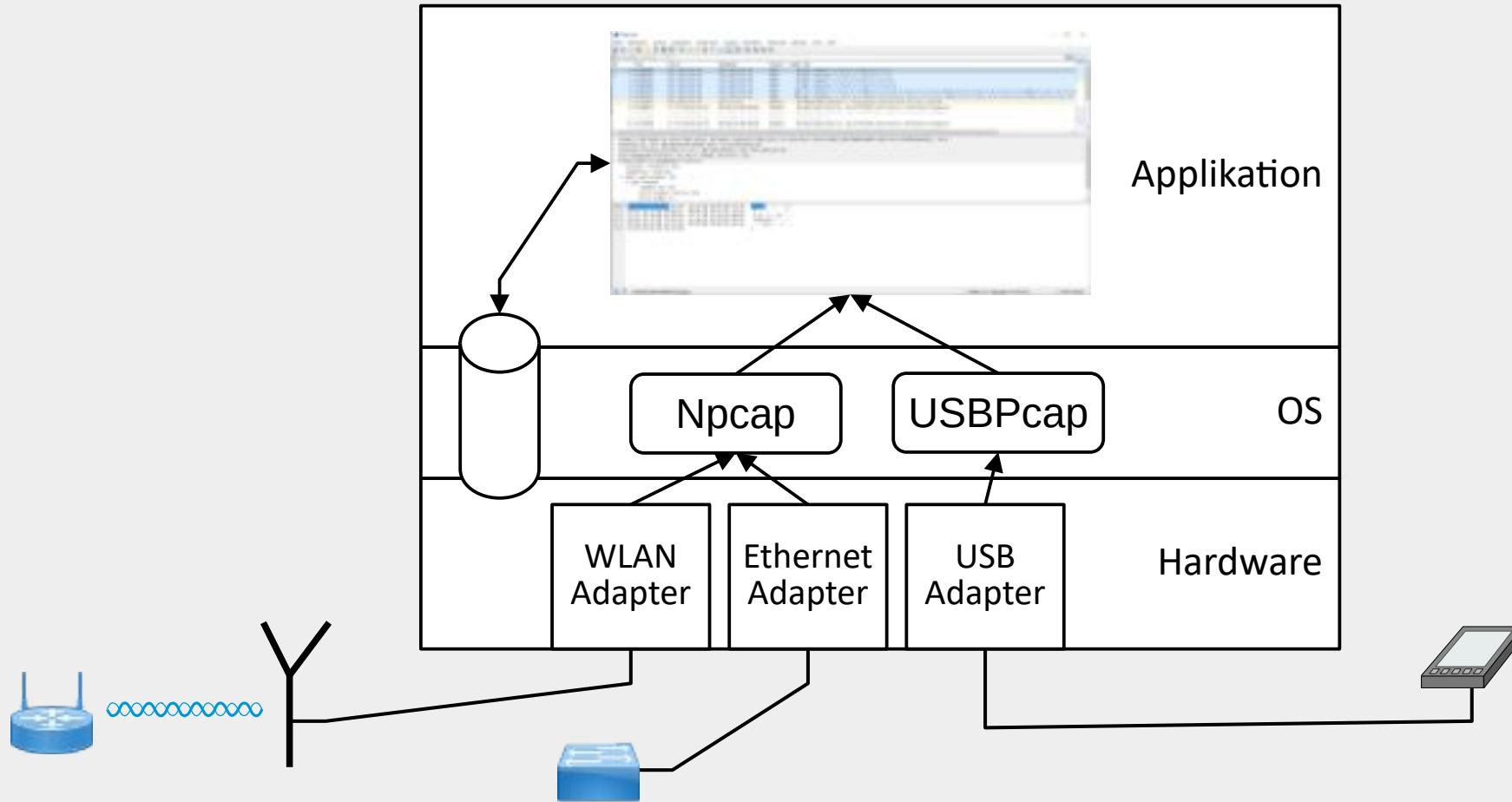
## Rechtliches

Ein Sniffer wie Wireshark, darf zum Studium oder zur Fehlersuche eingesetzt werden. Allerdings sind Tätigkeiten, wie das Beschaffen von Passwörtern, Straftaten sofern sie nicht angeordnet wurden!

Falls Sie zu einer IT-Belegschaft gehören, sollten Sie sicherstellen, dass Sie dazu beauftragt sind Datenverkehr aufzuzeichnen, um Fehler zu beheben, Optimierungen vorzunehmen, Sicherheitsprüfungen oder Programmanalysen zu machen.  
Lassen Sie sich das (schriftlich) bestätigen!

Es kann auch sinnvoll sein, sich von einem Juristen beraten zu lassen, um örtliche / nationale Vorschriften im Zusammenhang mit diesen Tätigkeiten zu kennen.

# Übersicht



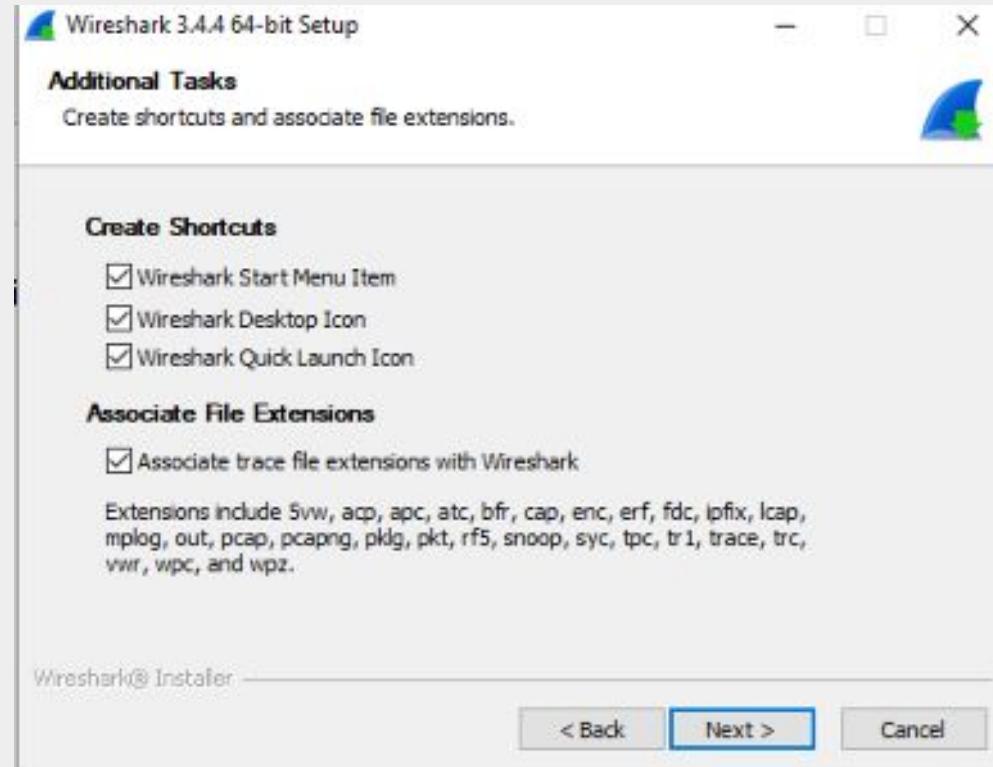
## Wireshark-Installation

Wireshark steht auf verschiedenen Betriebssystem-Plattformen zur Verfügung:

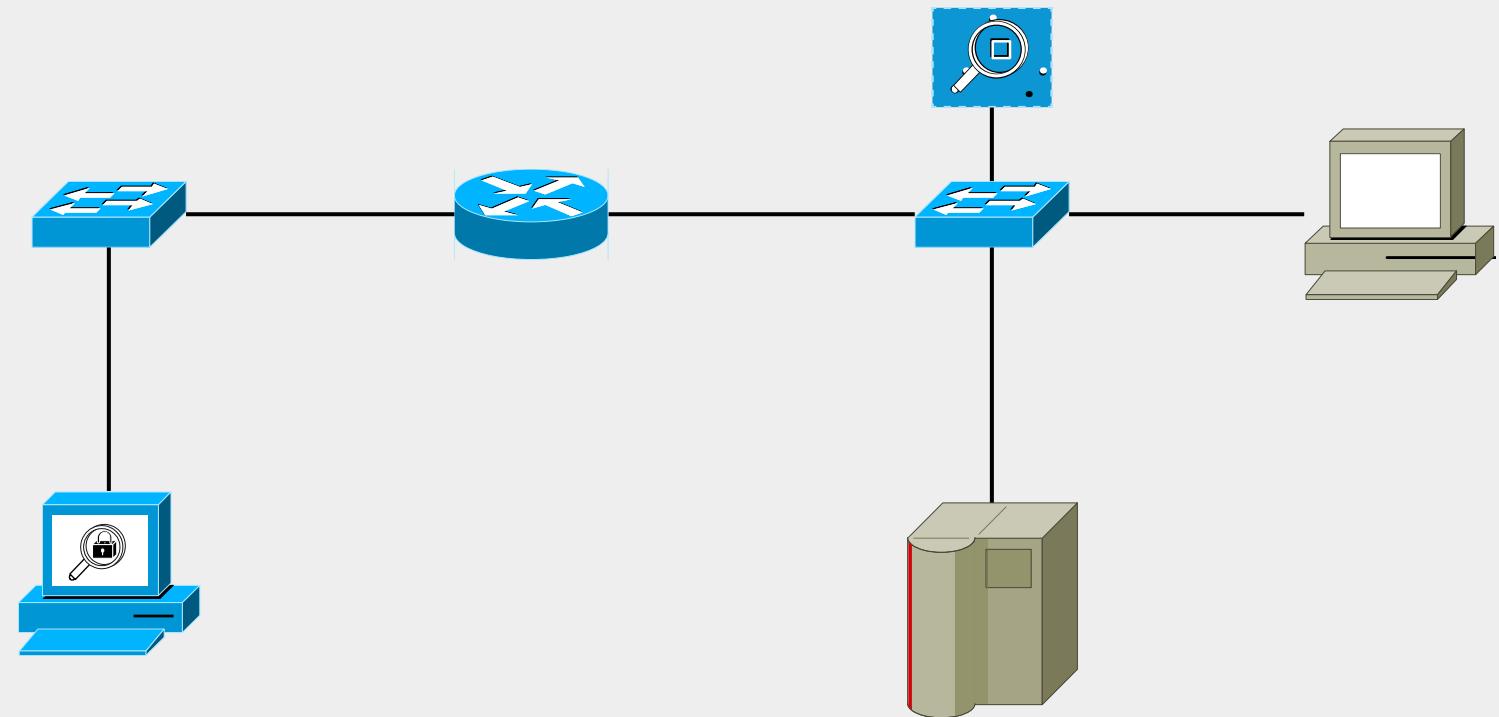
- Windows 64Bit, 32Bit und portable)
- Apple (macOS)
- Linux (diverse Varianten)
- HP-UX
- Oracle (Solaris)
- ..

Aktuelle Versionen siehe <https://www.wireshark.org/download.html>

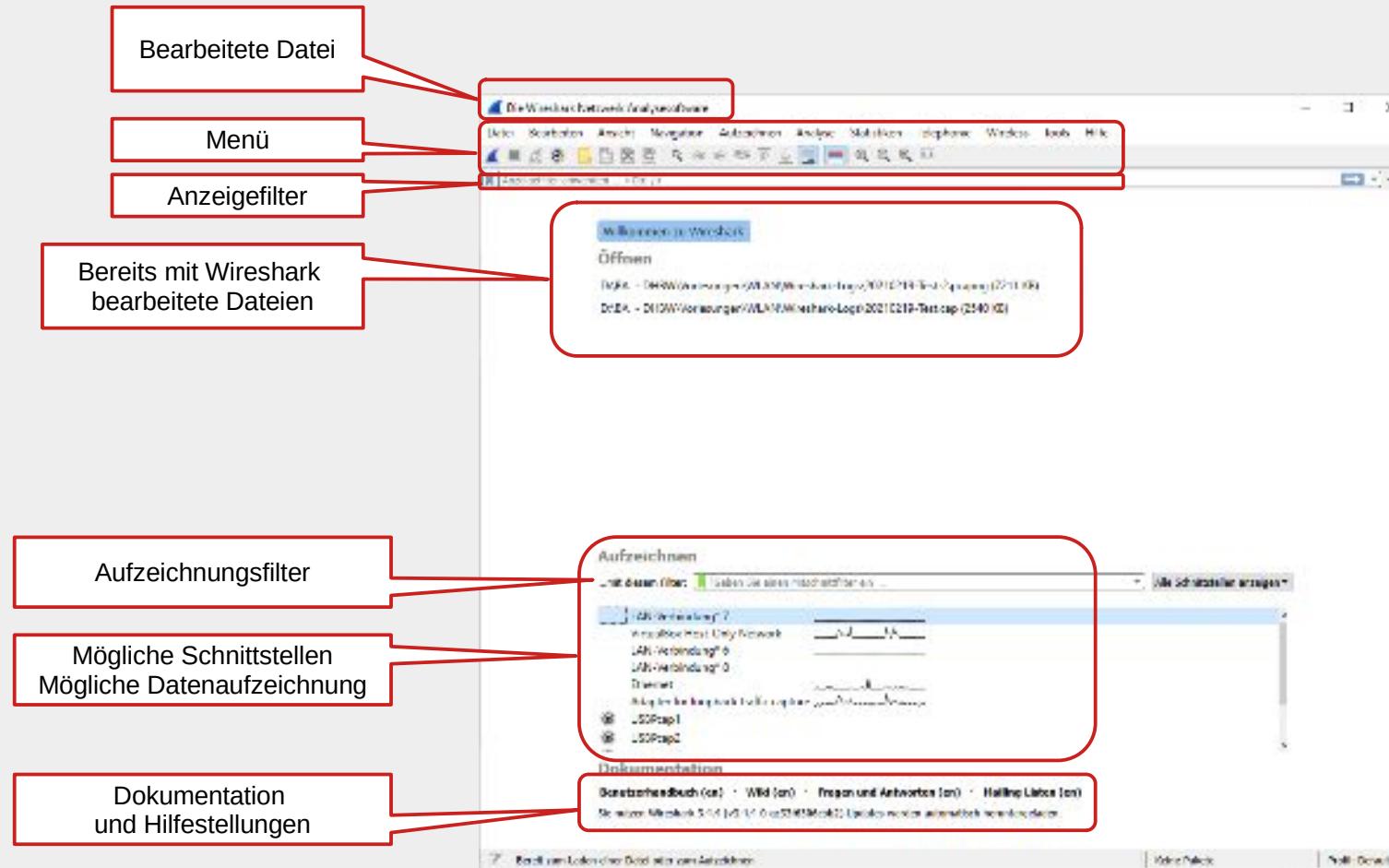
# Mögliche Dateiformate, die bearbeitet werden können



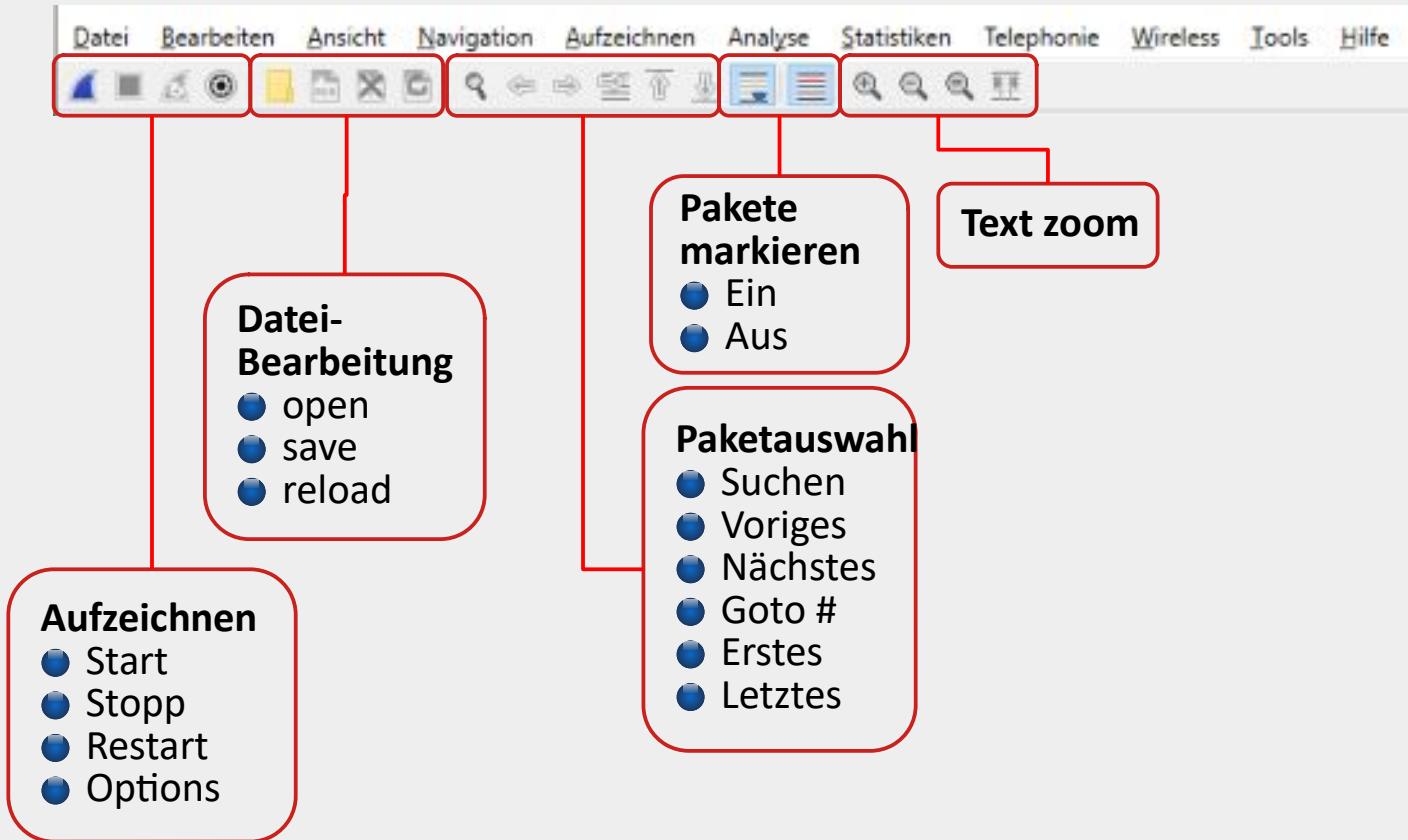
# Platzierung des Sniffers



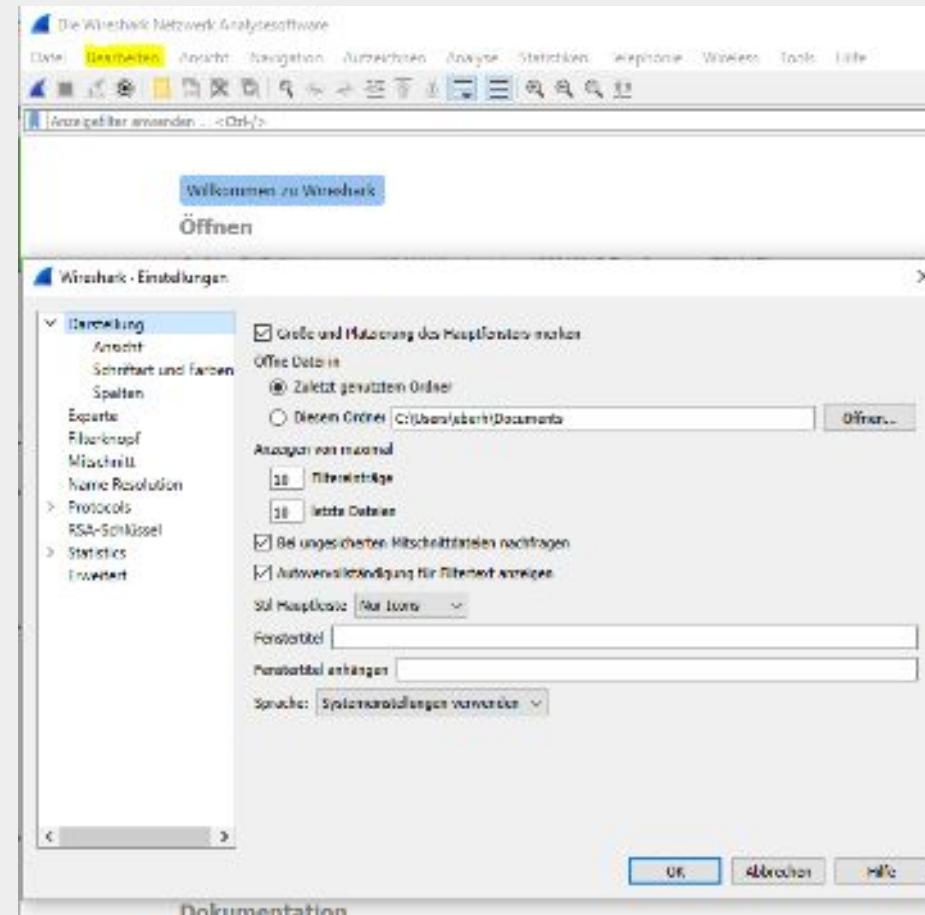
# Wireshark Startseite



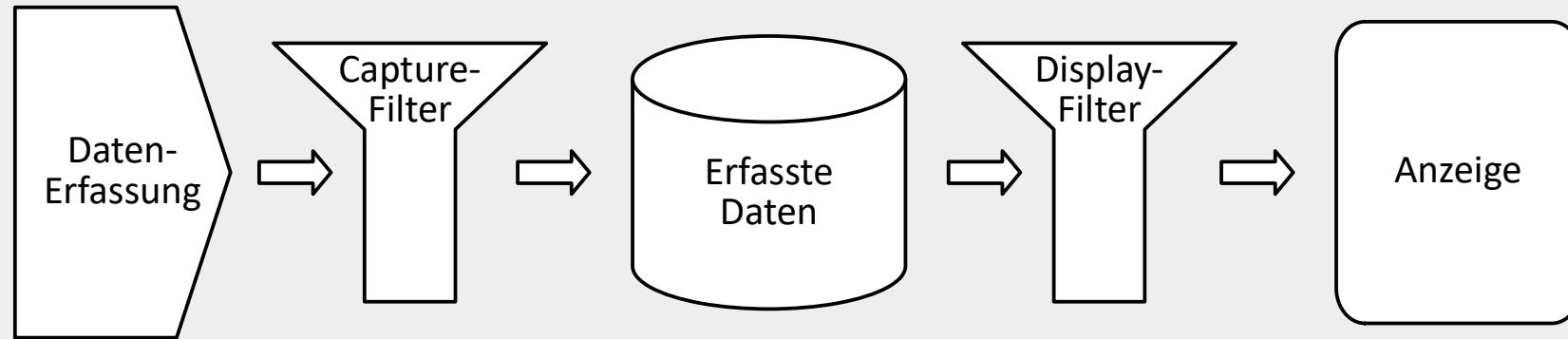
# Wireshark-Menü



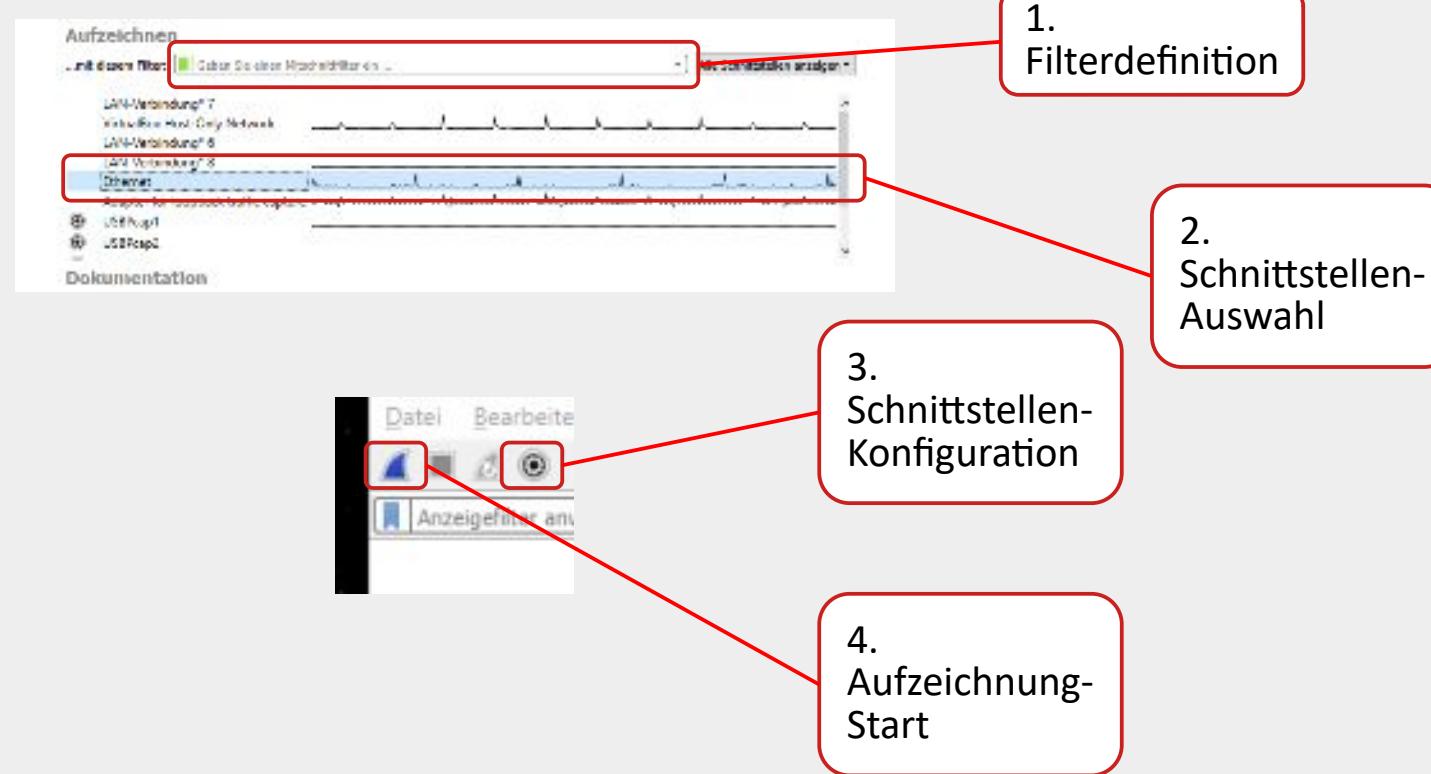
# Wireshark-Einstellungen



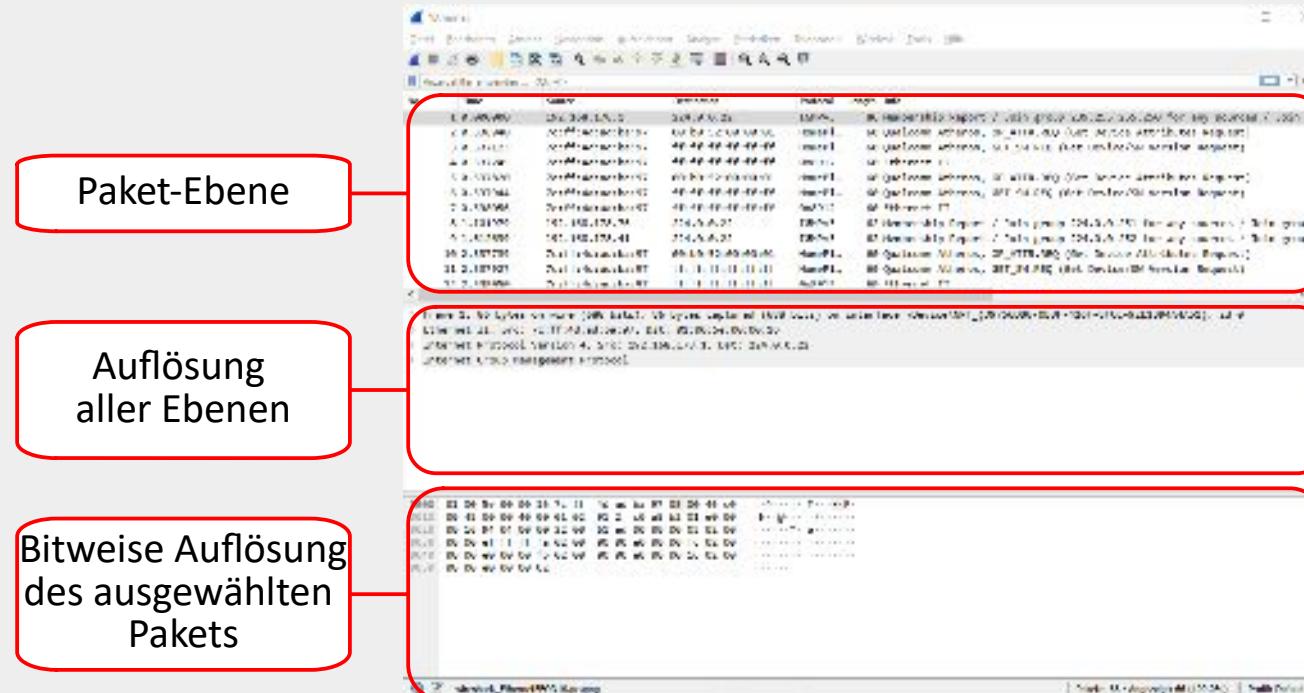
# Wireshark-Daten-Bearbeitung



# Aufzeichnungs-Start



# Darstellung des Mitschnitts



## WLAN-Vorlesung

### Analyse mit Wireshark Teil-1

- Rechtliches
- Wireshark-Grundlagen
- Installation
- WLAN-Messung

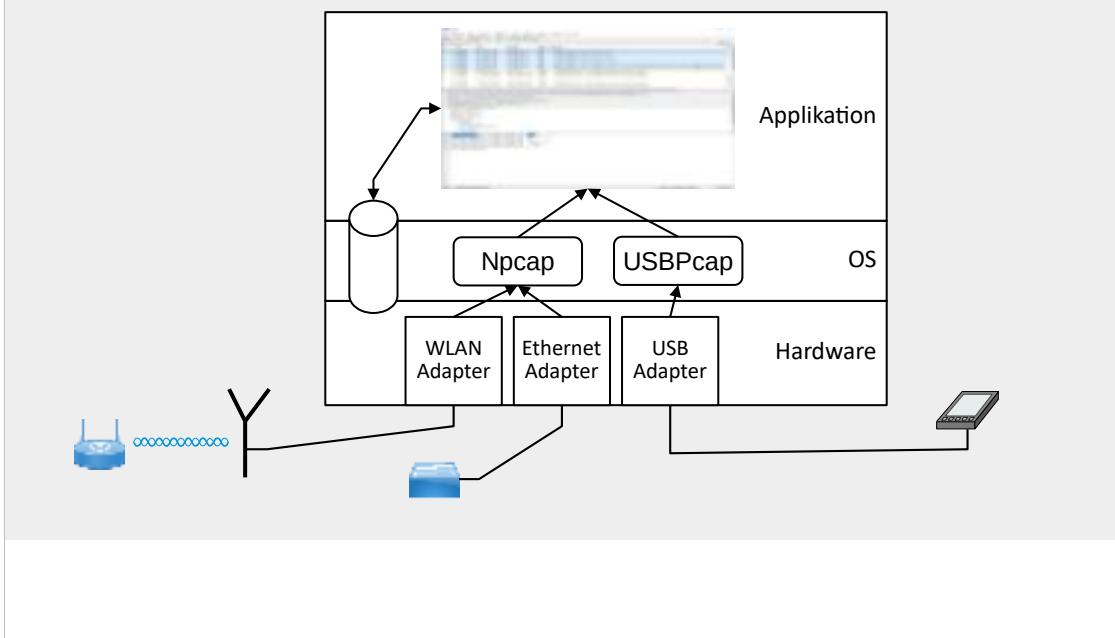
Ein Sniffer wie Wireshark, darf zum Studium oder zur Fehlersuche eingesetzt werden.  
Allerdings sind Tätigkeiten, wie das Beschaffen von Passwörtern, Straftaten sofern sie nicht angeordnet wurden!

Falls Sie zu einer IT-Belegschaft gehören, sollten Sie sicherstellen, dass Sie dazu beauftragt sind Datenverkehr aufzuziehen, um Fehler zu beheben, Optimierungen vorzunehmen, Sicherheitsprüfungen oder Programmanalysen zu machen.  
Lassen Sie sich das (schriftlich) bestätigen!

Es kann auch sinnvoll sein, sich von einem Juristen beraten zu lassen, um örtliche / nationale Vorschriften im Zusammenhang mit diesen Tätigkeiten zu kennen.

Die rechtlichen Rahmenbedingungen sind unbedingt einzuhalten, da sie persönliche Konsequenzen nach sich ziehen können!

## Übersicht



Wireshark kann die Daten verschiedener Schnittstellen aufzeichnen. Dazu zählen Ethernet, WLAN und USB. Die aufgezeichneten Daten können auf einem Datenträger (z. B. Festplatte) gespeichert werden. Bereits aufgezeichnete Daten können später nochmals analysiert werden.

Damit überhaupt Rahmen am Gerät ankommen, müssen evtl. die Geräte welche die Rahmen senden entsprechend konfiguriert werden.  
Z. B. sind auf Switches Spiegelports einzurichten. Das ist nur mit manageable Switches möglich!

Die Adapter filtern bereits auf Hardware-Ebene die Rahmen.  
Damit überhaupt Daten aufgezeichnet werden können, müssen die Adapter im Promiscuous-Mode betrieben werden.  
Ansonsten würden nur die Rahmen mitgelesen werden, die direkt an das Gerät adressiert sind (Unicasts an das Gerät, Multicasts an die Gruppen des Gerätes und alle Broadcasts)

Damit Wireshark die Daten als Applikation auch bekommt, müssen sie auf Betriebssystem-Ebene noch dafür abgetrennt werden. Dazu sind spezielle Treiber (Npcap (früher Pcap) und USBPcap) erforderlich.

Auch auf Applikationsebene sind, je nachdem was mitgelesen werden soll, weitere Konfigurationen erforderlich. Sollen z. B. beim WLAN auch die Management-Frames mitgelesen werden, muss der entsprechende Port in den Monitor-Mode konfiguriert werden.

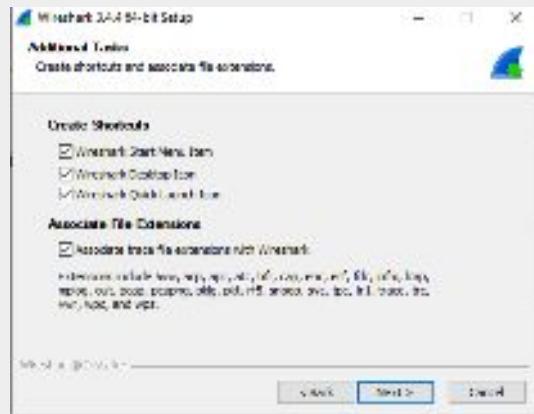
## Wireshark-Installation

Wireshark steht auf verschiedenen Betriebssystem-Plattformen zur Verfügung:

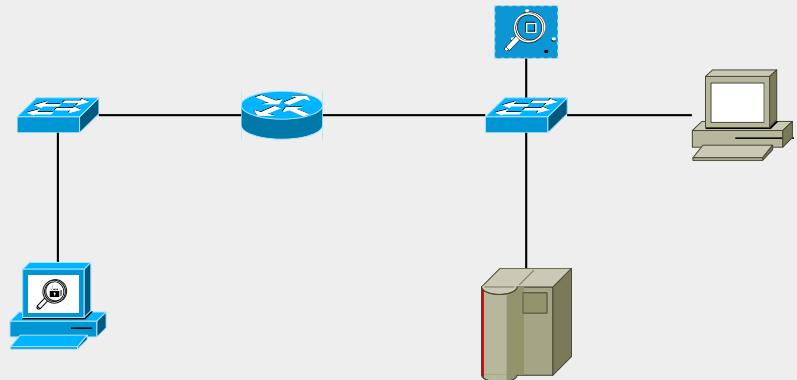
- Windows 64Bit, 32Bit und portable)
- Apple (macOS)
- Linux (diverse Varianten)
- HP-UX
- Oracle (Solaris)
- ..

Aktuelle Versionen siehe <https://www.wireshark.org/download.html>

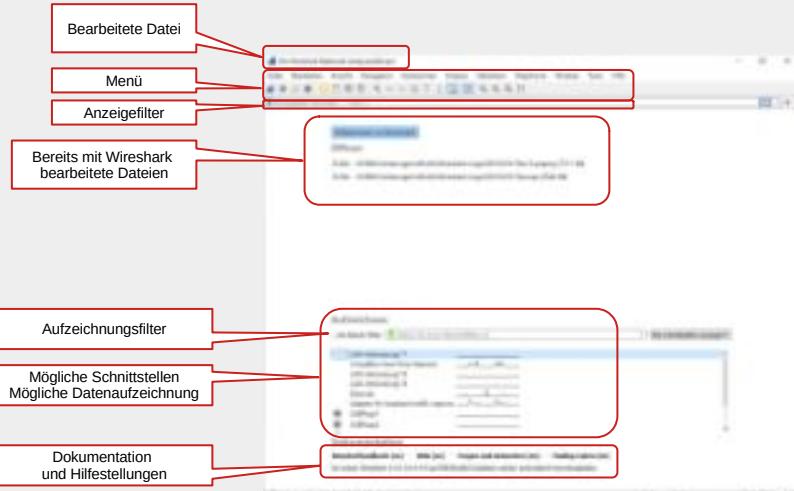
Mögliche Dateiformate,  
die bearbeitet werden können



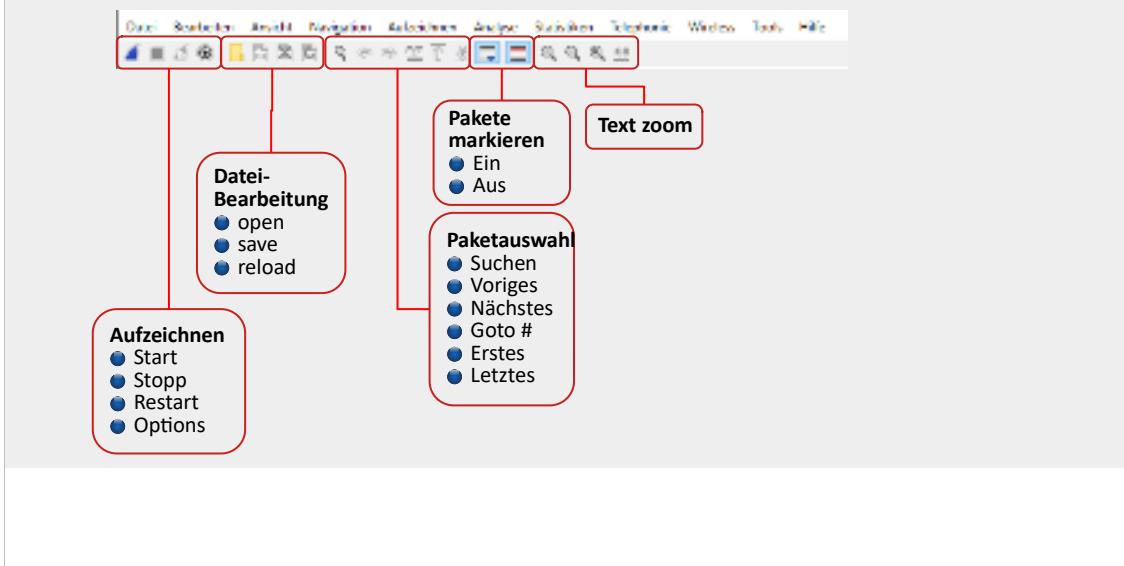
## Platzierung des Sniffers



## Wireshark Startseite

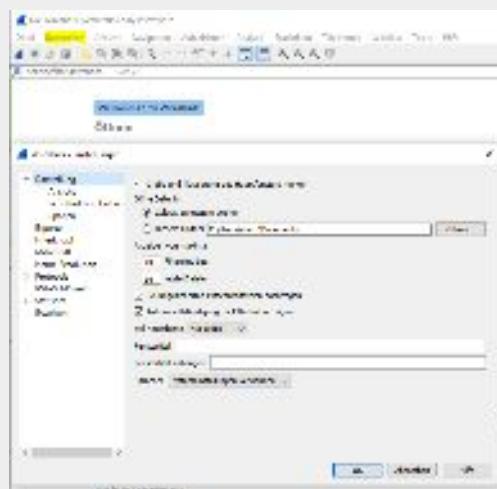


## Wireshark-Menü

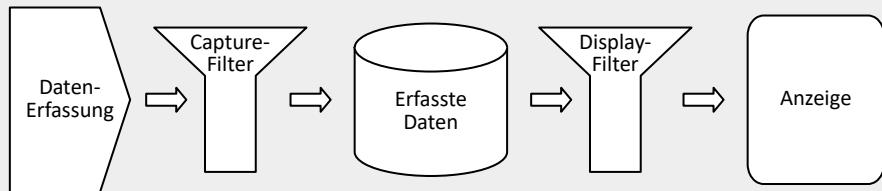


WLAN-Analyse  
Stand: 17.04.2023  
Folie: 10:13

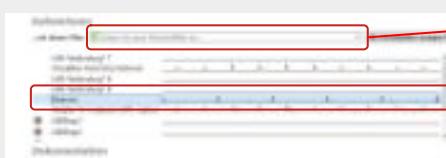
## Wireshark-Einstellungen



## Wireshark-Daten-Bearbeitung



## Aufzeichnungs-Start



1.  
Filterdefinition



2.  
Schnittstellen-  
Auswahl

3.  
Schnittstellen-  
Konfiguration

4.  
Aufzeichnung-  
Start

## Darstellung des Mitschnitts

