

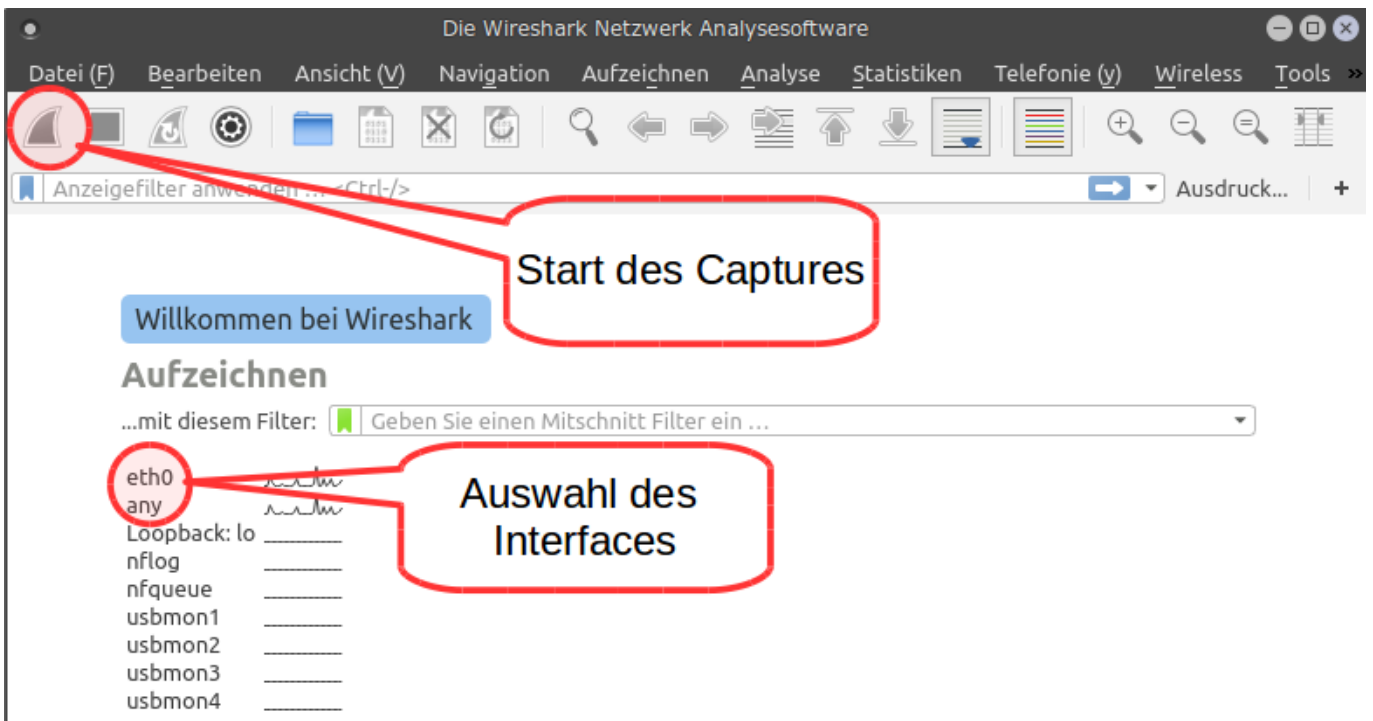
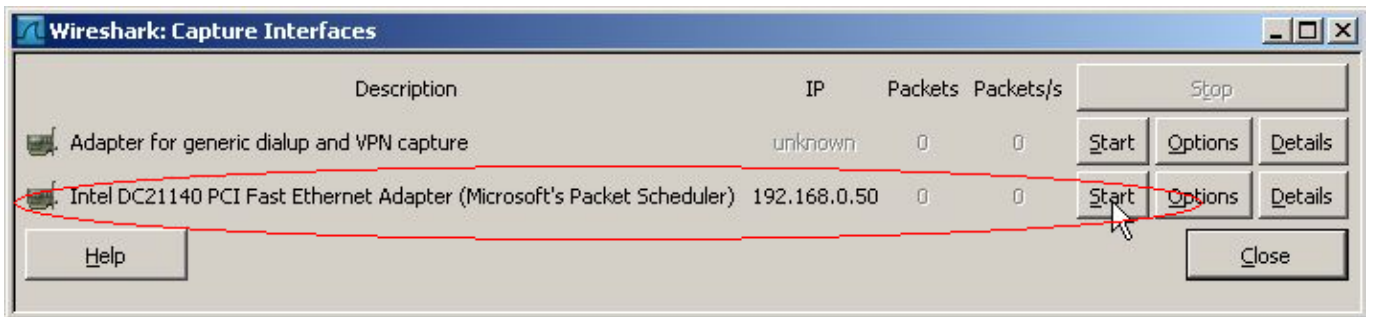
Einführung Übung zur Labornutzung

Auf dieser Seite befinden sich die grundsätzlichen Informationen zum Laborkonzept. Hier können u.a. grundlegende Befehle zur Nutzung von Linux nachgelesen werden.

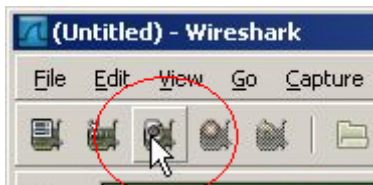
Umgang mit Wireshark

Die Protokollanalyse-Software wireshark ist sehr mächtig. Allerdings geht mit dieser Mächtigkeit eine gewisse Komplexität einher. Im Folgenden wird ein kurzer Einblick in Bestandteile der Oberfläche erklärt.

Zunächst muss der richtige Netzwerkadapter ausgewählt werden.



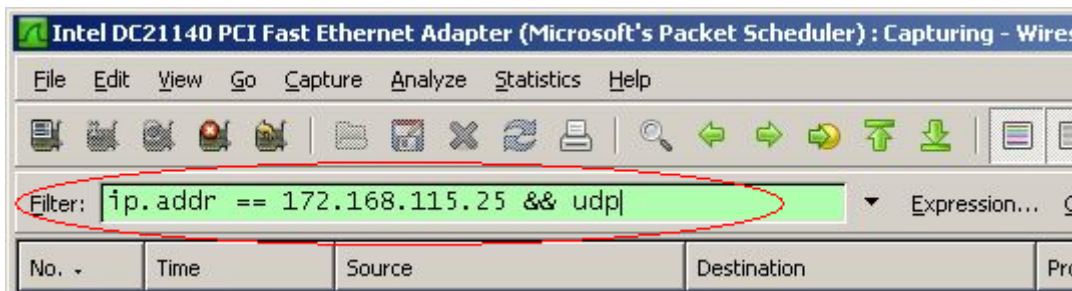
Danach kann die eigentliche Aufzeichnung gestartet werden.



Das folgende Bild zeigt den Aufbau des wireshark-Hauptfensters



Ein sehr wichtiges Mittel sind die Filterregeln, über die die Flut der Pakete übersichtlich gehalten werden können.



Filter	Bemerkung
eth.addr == aa:aa:aa:bb:bb:bb	Zeige nur Pakete in denen die MAC-Adresse aa:aa:aa:bb:bb:bb überhaupt vorkommt. ¹⁾
eth.dst == aa:aa:aa:bb:bb:bb	Zeige nur Pakete in denen die MAC-Adresse aa:aa:aa:bb:bb:bb als Empfänger ²⁾ vorkommt.
eth.src == aa:aa:aa:bb:bb:bb	Zeige nur Pakete in denen die MAC-Adresse aa:aa:aa:bb:bb:bb als Absender ³⁾ vorkommt.
ip.addr == 10.0.0.1	Zeige nur Pakete in denen die IP-Adresse 10.0.0.1 überhaupt vorkommt. ⁴⁾
ip.dst == 10.0.0.1	Zeige nur Pakete in denen die IP-Adresse 10.0.0.1 als Empfänger ⁵⁾ vorkommt.
ip.src == 10.0.0.1	Zeige nur Pakete in denen die IP-Adresse 10.0.0.1 als Absender ⁶⁾ vorkommt.
&&	logisch UND
	logisch ODER
!=	logisch UNGLEICH
==	logisch GLEICH

Wie in der Programmierung lassen sich logische Aussagen formulieren:

Zeige alle Pakete, die die MAC-Adresse ABC als Absender UND die IP-Adresse XYZ als Empfänger hat.

```
eth.src == ABC && ip.dst == 10.0.0.1
```

Aufgaben

1. Protokollieren Sie zwei unterschiedliche Ethernet-Rahmen mit. a) Welche verschiedenen Rahmenvarianten können Sie finden?

b) Welche Datenelemente enthalten diese? Notieren Sie die Namen und Größen der Datenelemente in die folgende Tabelle.

Fehlendes Datenelement gegenüber der Theorie: Ethernet-Frame-Variante 1: Datenelement Größe in Byte
Ethernet-Frame-Variante 2: Datenelement Größe in Byte

Welche Datenelemente vermissen Sie?

c) Was ist beiden Typen gemeinsam? Worin unterscheiden Sie sich?

1)

egal, ob als Absender oder Empfänger

2) 5)

,
dst: Destination

3) 6)

,
src: Source

4)

egal, ob Absender oder Empfänger

From:

<http://www.kopfload.de/> - **kopfload - Lad Dein Hirn auf!**

Permanent link:

http://www.kopfload.de/doku.php?id=lager:lok_netze:labor_uebung&rev=1387297042

Last update: **2025/11/19 16:13**

