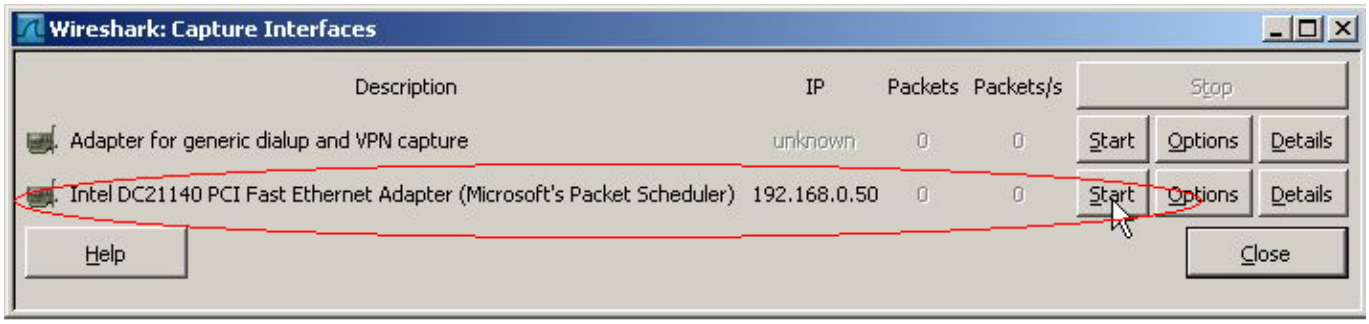
Einführung Übung zur Labornutzung

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

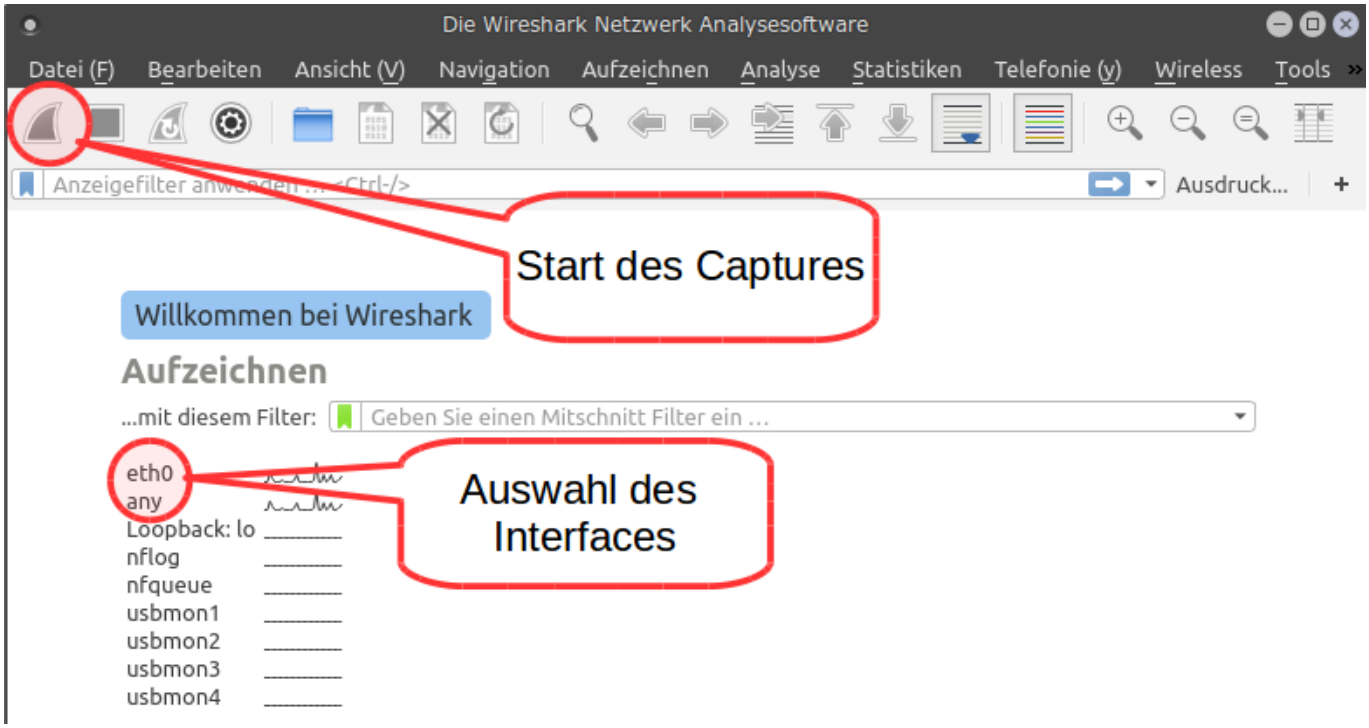
Umgang mit Wireshark

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.



Rechts neben dem Button für die Schnittstellen befindet sich der Button für die Einstellungen des Caputures [1] selbst.

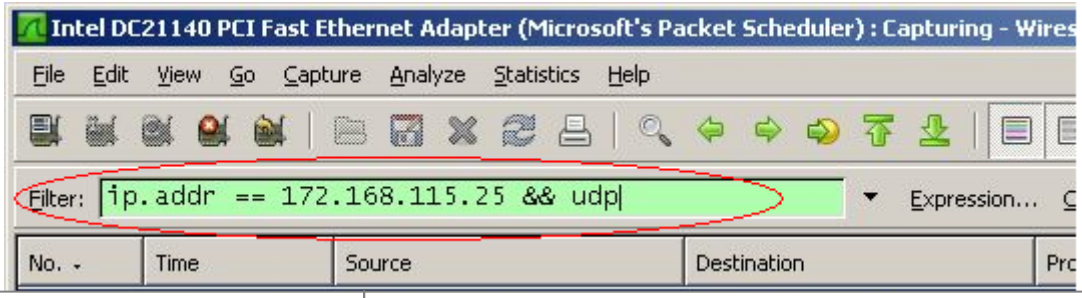


Danach kann die eigentliche Aufzeichnung gestartet werden.

Das folgende Bild zeigt den Aufbau des `wireshark`-Hauptfensters

Filerregeln im wireshark

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. [2]
`eth.dst == aa:aa:aa:bb:bb:bb`	Zeige nur Pakete in denen die MAC-Adresse `aa:aa:aa:bb:bb:bb` als Empfänger [3] 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 [4] vorkommt.
`ip.addr == 10.0.0.1`	Zeige nur Pakete in denen die IP-Adresse `10.0.0.1` überhaupt vorkommt. [5]
`ip.dst == 10.0.0.1`	Zeige nur Pakete in denen die IP-Adresse `10.0.0.1` als Empfänger [6] vorkommt.
`ip.src == 10.0.0.1`	Zeige nur Pakete in denen die IP-Adresse `10.0.0.1` als Absender [7] 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
```

Alle möglichen Filteroptionen können über den Button `Expression…` rechts neben dem Filter-Feld gefunden werden.

Aufgaben

1. Konfigurieren Sie Ihren Capture so, dass das **automatische Scrolling** während des Capture-Vorgangs DEAKTIVIERT ist.

2. Protokollieren Sie zwei unterschiedliche Ethernet-Rahmen mit.
HINWEIS: Probieren Sie die beiden Filter: `eth.type` und `eth.length` aus.

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: _ Name der ersten Ethernet-Frame-Variante: _ ^Datenelementname ^ Größe ^ | | Byte| | | Byte| | | Byte| | | Byte| Name der zweiten Ethernet-Frame-Variante: ___

Datenelementname	Größe
	Byte
	Byte
	Byte
	Byte

Welche Datenelemente vermissen Sie?

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

3. Versuchen Sie über einen Filter, der auf Ihre IP-Adresse filtert, die MAC-Adresse Ihrer Schnittstelle `eth0` zu ermitteln.

4. Machen Sie sich mit dem System vertraut und sichern Sie Ihre Erkenntnisse in einem Dokument.

[1)]
Mitschnitt
[2)]
egal, ob als Absender oder Empfänger
[3)] [6)]
,
dst: Destination
[4)] [7)]
,
src: Source
[5)]
egal, ob Absender oder Empfänger