

## Kurzanleitung Netzwerksniffer (*Wireshark*)

**Allgemeines:** Die verfügbaren Funktionen und Optionen werden durch Hilfetexte erklärt, wenn der Mauszeiger darüber steht.

**Vor dem ersten Start** muss das Display freigegeben werden mit dem Befehl

```
xhost +local:root
```

*Wireshark* muss i.d.R. mit root-Rechten von der Kommandozeile gestartet werden:

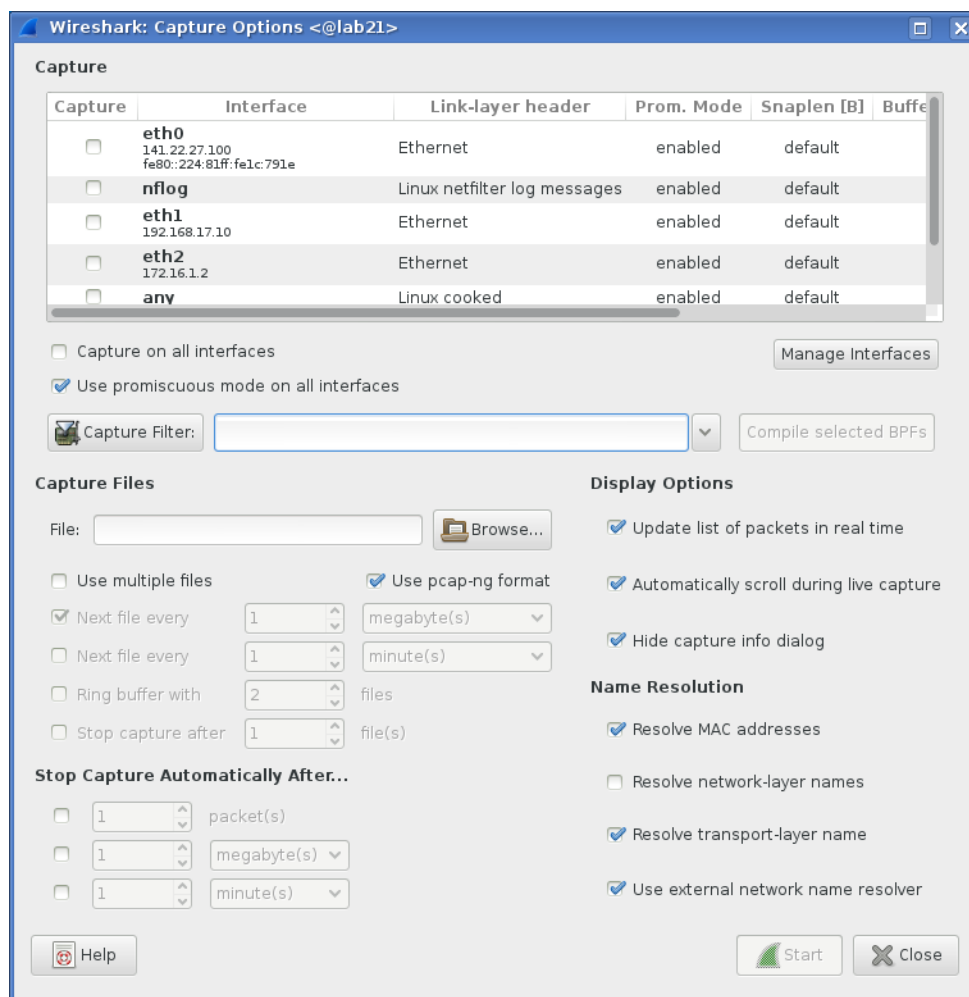
```
sudo /usr/bin/wireshark
```

Zum Starten auf einem entfernten Rechner (*ssh*-Sitzung) wird nachfolgendes Kommando empfohlen:

```
sudo XAUTHORITY=/home/networker/.Xauthority /usr/bin/wireshark
```

### 1. Schritt: Einstellen der *Capture Options*:

über  , Capture-Menü oder Hauptfenster



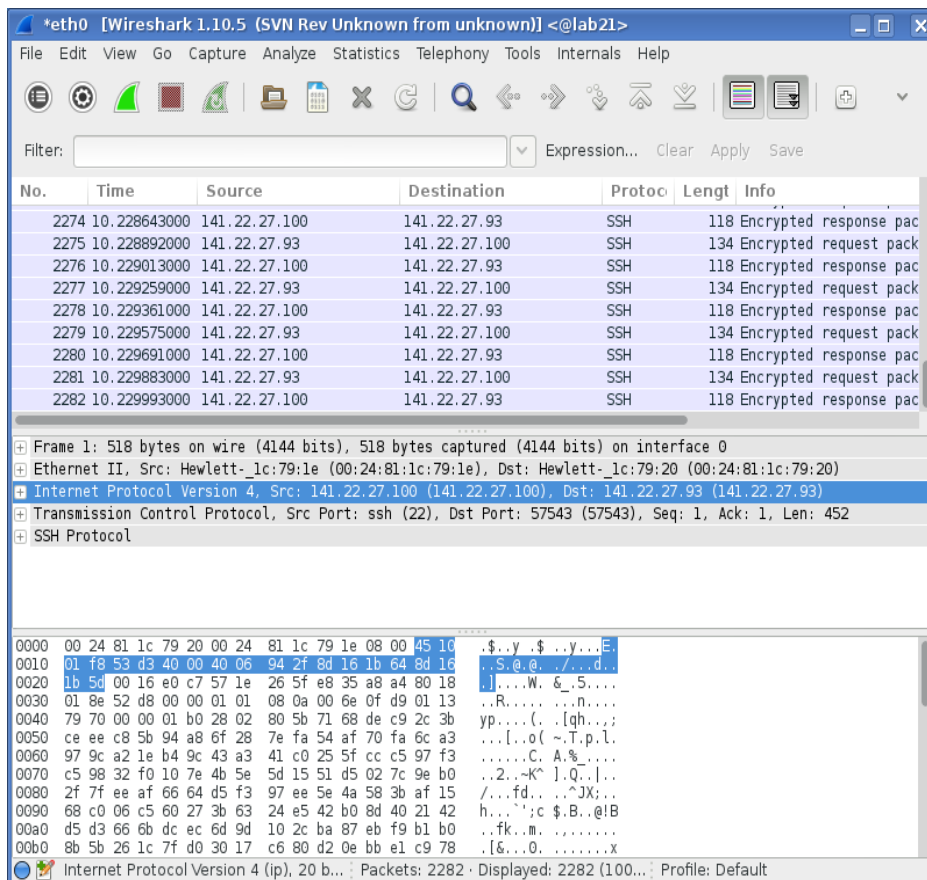
- *Interface(s)* je nach Netz.

- **Capture Filter** nach Bedarf einstellen. Für Filterbeispiele Knopf drücken.  
Näheres zu Filtern und Syntax siehe Wireshark-Dokumentation oder Man-Page.

**2. Schritt:** Sniff-Vorgang starten  (bzw. 'Capture – Start')

Stoppen des Sniff-Vorganges mit **Stop-Button**  oder mit 'Capture – Stop.'

**3. Schritt:** Auswertung



- oberes Drittel des Fensters: chronologische Liste der ersniffen Pakete
- mittleres Drittel des Fensters: Detailansicht des oben selektierten Pakets
- unteres Drittel des Fensters: Native Darstellung des selektierten Pakets in Hex (links) und ASCII (rechts)

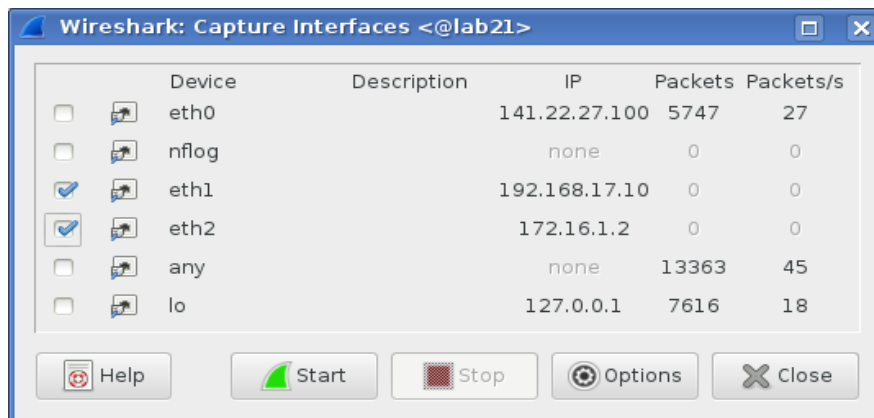
*N.B.: Einige Informationen des Sniffer können Interpretationen nativer Daten sein.*

**4. Schritt:** Abspeichern des Sniffs

- als Text: Menü *Export Packet Dissections – as “Plain Text“ file* .  
Es kann ausgewählt werden, welche Pakete und in welchem Detaillierungsgrad gespeichert werden soll. Für eine Ausgabe wie obersten Drittel ist z.B. "Packet summary line" aus- und "Packet details" abzuwählen.
- Binär zur Weiterverarbeitung mit Analyse-Tools oder zum späteren Offline-Betrachten im Sniffer: *File – Save* bzw. *File – Save As...*

### Weitere Funktionen und Einstellungen:

1. Interessant ist noch der Menüpunkt *Capture – Interfaces*. Hier bekommt man einen groben Überblick über den Netzwerkverkehr aller Interfaces.



Mit *Options* werden die Optionen für die jeweilige Netzwerkkarte wie oben eingestellt. Mit *Start* wird der Sniff-Vorgang auf den ausgewählten Netzwerkkarten gestartet.

2. **Displayfilter** (= Zeile "Filter", Text ist auch Knopf): Hier handelt es sich um einen reinen Anzeigefilter, der Pakete, die die Filterkriterien nicht erfüllen, in der Anzeige unterdrückt. Im Gegensatz zu *Capture*-Filtern können diese aber durch Löschen des Filters mit dem *Clear*-Knopf jederzeit wieder sichtbar gemacht werden, da die Pakete nach wie vor im Puffer liegen.
3. Bedeutung der Einfärbung der Pakete: siehe unter *View – Coloring Rules* bzw. entsprechenden Knopf.  
Ein-/Ausschalten der Einfärbung mit *View – Colorize Packet List*.
4. **Sequenznummern** bei TCP: voreingestellt ist die relative Nummerierung. Geändert werden kann das unter *Edit – Preferences*, dort unter *Protocols – TCP*.
5. **Follow TCP Stream**: Wählt man im obersten Drittel des Fensters (Paketliste) ein Paket aus, das zu einer TCP-Verbindung gehört, kann mit "Follow TCP Stream" aus dem Kontextmenü (rechte Maustaste) in einem gesonderten Fenster der Datenverkehr dieser Verbindung angezeigt werden. Dabei wird automatisch ein **Displayfilter** gesetzt.

- 6. Statistik:** Unter dem Menüpunkt *Statistics* kann man sich Einzelheiten über alle ersniffen Kommunikationssitzungen zeigen lassen. Dabei wird nach verschiedenen Kriterien (Protokoll, Schicht, etc.) sortiert.
  
- 7. Man-Pages:** Können über das Help-Menü („Manual Pages“) erreicht werden: