Wireshark

ITT-Netzwerke

Sebastian Meisel

4. Januar 2023

1 Installation (Ubuntu)

Um ein Programm unter Ubuntu zu installieren nutzt man am besten das Terminal. Zunächst müssen die Paketquellen aktualisiert werden:

```
sudo apt update
```

Das vorangestellte `sudo` versorgt uns dazu mit erweiterten Rechten und verlangt die Eingabe des Benutzerpassworts.
Nun können wir das eigentliche Programm installieren:

```
sudo apt install wireshark -y
```

Das `-y` am Ende bewirkt, dass wir die Installation weiterer Paket nicht extra bestätigen müssen. Dafür müssen wir einmal auf eine Frage mit `<OK>` antworten und dann unter Konfiguriere wireshark-common mit `<Ja>` bestätigen, dass auch mit einem normalen Benutzaccount Wireshark genutzt werden darf, solange er zu Gruppe wireshark gehört.

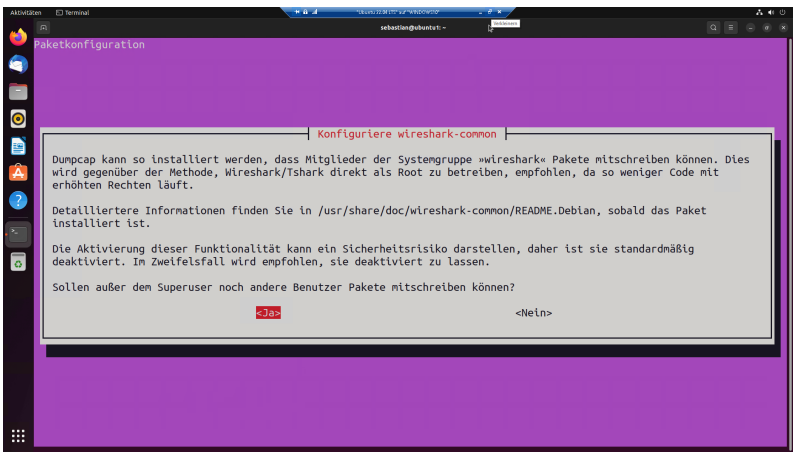

Abbildung 1: Konfiguriere wireshark-common

1.1 Gruppenzugehörigkeit

Damit unser Benutzer zur Gruppe dazu gehört, fügen wir ihn mit `usermod` hinzu:

```
sudo usermod -aG wireshark $USER
```

Das `-aG` steht für *append group*, also Gruppe hinzufügen.
Damit die Änderung der Gruppenzugehörigkeit wirksam wird, kann man sich nun aus- und neu einloggen, oder man nutzt den Befehl:

```
newgrp wireshark
```

Nun kann man mit dem Befehl `groups` die Gruppenzugehörigkeit überprüfen. Die Ausgabe sollte etwa so aussehen:
#+BEGIN$_{\text{EXAMPLE}}$ wireshark sebastian adm cdrom sudo dip plugdev lpadmin lxd sambashare #+END$_{\text{EXAMPLEx}}$
Nun kann Wireshark gestartet werden:

```
wireshark &> /dev/null &
```

Das `&> /dev/null` bewirkt, dass eventuelle Ausgaben des Programms nicht im Terminal landen. Das finale `&` bewirkt die Ausführung im Hintergrund, sodass das Terminal weiter genutzt werden kann.