2. Run tcpdump

1. Installeer zo nodig tcpdump

2. Vind de naam van je netwerk interface met:

ip link

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s31f6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
mode DEFAULT group default qlen 1000
    link/ether 54:e1:ad:bd:78:5c brd ff:ff:ff:ff:ff:ff
3: wlp4s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP mode
DORMANT group default qlen 1000
    link/ether 9c:da:3e:72:db:4d brd ff:ff:ff:ff:ff:ff
```

interface namen die beginnen met en (enp0s21f6) zijn bedraad
interface namen die beginnen met wl (wlp4s0) zij wireless interfaces

3. run tcpdump:

sudo tcpdump -i <je interface>

Herken je iets van wat er verschijnt?

run:

sudo tcpdump -i <je interface> -A port 80

en bezoek een site via http. (bijvoorbeeld: http://google.com) via browser of curl

run:

sudo tcpdump -i <je interface> -A port 443

en bezoek een site via https. (bijvoorbeeld: https://google.com) via browser of curl

waarom kan je wel dingen lezen over poort 80 en niet via poort 443?

4. Lees een packet capture recording uit

Ik heb capture gemaakt van het mailprogramma mutt.
mutt was zo ingesteld dat het geen authenticatie deed, en geen encryptie (starttls of ssl)

de capture was gedaan met:

sudo tcpdump -i wlp4s0 -A port 25 -w mutt-dump.pcap

- wat staat er in de capture?

Je kan hiervoor tcpdump gebruiken:

tcpdump -r -A mutt_dump.pcap

Wat kan je hier van volgen?