tcpdump

tcpdump is een gereedschap (packet sniffer) voor diagnose en analyse van computernetwerken.

Het programma draait op de meeste UNIX(-achtige) systemen zoals Linux, Solaris, HP-UX, AIX, Mac OS X en anderen.

Hierbij wordt de netwerkkaart in promisuous mode gezet en wordt gebruik gemaakt van libpcap om pakketjes

die op het netwerk worden verzonden af te vangen.

Om op de eerste ethernet adapter op poort 80 (http) te luisteren:

```
# tcpdump -i eth0 dst port 80
```