# tcpdump



## context

dit document geeft enkele voorbeelden van tcpdump

### SSH/SNMP

```
tcpdump port 22 or port 161 and src <ipadres van bron server> -vvv
```

scan verbose op SSH en SNMP verkeer

### ping

```
tcpdump -i <NIC> host <dest> and icmp
```

### WinDump

- Windows equivalent, beschikbaar op WinDump website

## meer info

- TCPdump primer
- tcpdump command line examples

Linux

From:
https://www.louslab.be/ - **Lou's lab**

Permanent link:
**https://www.louslab.be/doku.php?id=linux:tcpdump&rev=1759150475**

Last update: **2025/09/29 12:54**