TCPDump

```
tcpdump -D

tcpdump -i <interface>

tcpdump -i <interface> [capture filter]
tcpdump -i <interface> port ## and udp

# -n: no conversion
tcpdump -i <interface> -n -w dump.pcap [cf]

tcpdump -i <interface> -n -w dump_%c.pcap -Z root -C 1000 [cf]
# rotate 10 log files
tcpdump -i <interface> -n -W 10 -w dump.pcap -Z root -C 1000 [cf]
```

- for capture filters see Wireshark