tcpdump

> Dump traffic on a network.

- List available network interfaces:

```
tcpdump -D
```

- Capture the traffic of a specific interface:

```
tcpdump -i {{eth0}}
```

- Capture all TCP traffic showing contents (ASCII) in console:

```
tcpdump -A tcp
```

- Capture the traffic from or to a host:

```
tcpdump host {{www.example.com}}
```

- Capture the traffic from a specific interface, source, destination and destination port:

```
tcpdump -i {{eth0}} src {{192.168.1.1}} and dst {{192.168.1.2}} and dst port {{80}}
```

- Capture the traffic of a network:

```
tcpdump net {{192.168.1.0/24}}
```

- Capture all traffic except traffic over port 22 and save to a dump file:

```
tcpdump -w {{dumpfile.pcap}} not port {{22}}
```

- Read from a given dump file:

```
tcpdump -r {{dumpfile.pcap}}
```