

Links & Tools

- [tcpdump Cheat Sheet](#)
- [Wireshark Sample Captures](#)
- [Useful Network Diagnostic CLI commands](#)

tcpdump Cheat Sheet

tcpdump Cheat Sheet (<https://www.comparitech.com/net-admin/tcpdump-cheat-sheet/>)

[tcpdump cheat sheet](#)

Wireshark Sample Captures

If you need to see how different protocols behave on the network here are some sample captures from Wireshark

- <https://wiki.wireshark.org/SampleCaptures>
- <https://packetlife.net/captures/>
- <https://www.netresec.com/?page=PcapFiles>
- <https://tshark.dev/search/pcaptable/>

Useful Network Diagnostic CLI commands

Useful CLI commands to do network diagnostics with tcpdump / tshark etc.

tcpdump

| Command | Description |
|---|-----------------------------------|
| <code>tcpdump -nni <network-interface> icmp</code> | show icmp packets |
| <code>tcpdump -nni <network-interface> "icmp[0] == 0"</code> | ICMP type 0 echo reply |
| <code>tcpdump -nni <network-interface> "icmp[0] == 3"</code> | ICMP destination unreachable |
| <code>tcpdump -nni <network-interface> "icmp[0] == 4"</code> | ICMP source quench |
| <code>tcpdump -nni <network-interface> "icmp[0] == 5"</code> | ICMP redirect |
| <code>tcpdump -nni <network-interface> "icmp[0] == 8"</code> | ICMP echo request |
| <code>tcpdump -nni <network-interface> "icmp[0] == 11"</code> | ICMP time exceeded |
| <code>tcpdump -nni <network-interface> "tcp[tcpflags] & (tcp-rst) !=0"</code> | Detect tcp reset and ICMP packets |