

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