

tcpdump

- i. To see the list of network interfaces available on the system on which tcpdump can capture packets:- **sudo tcpdump -D**
- ii. To capture the packets following through a specific interface:- **sudo tcpdump -i wlp1s0**
- iii. to show the details of last 4 packets:- **sudo tcpdump -c 4 wlp1s0 -i**
- iv. to see the information of the ip address in terms of ipv6 addressing (in hexadecimal format):- **sudo tcpdump -XX -i wlp1s0**
- v. To access information of packet from a specific port number:- **sudo tcpdump -i wlp1s0 -c5 port 80**
- vi. To store packet information limited by lines, words:- **sudo tcpdump -i wlp1s0 -c 10 -w icmp.pcap**
- vii. To read the content of a packet capture by using tcpdump:- **sudo tcpdump -r icmp.pcap**