**NETWORKING & SYSTEM ADMINISTRATION LAB**

**Experiment No.:**

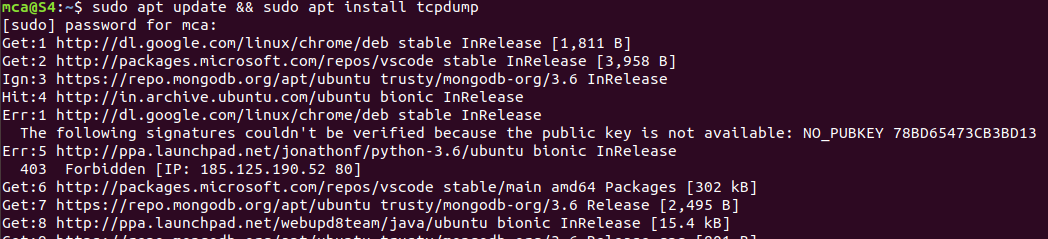
**Aim**

TCPDUMP installation

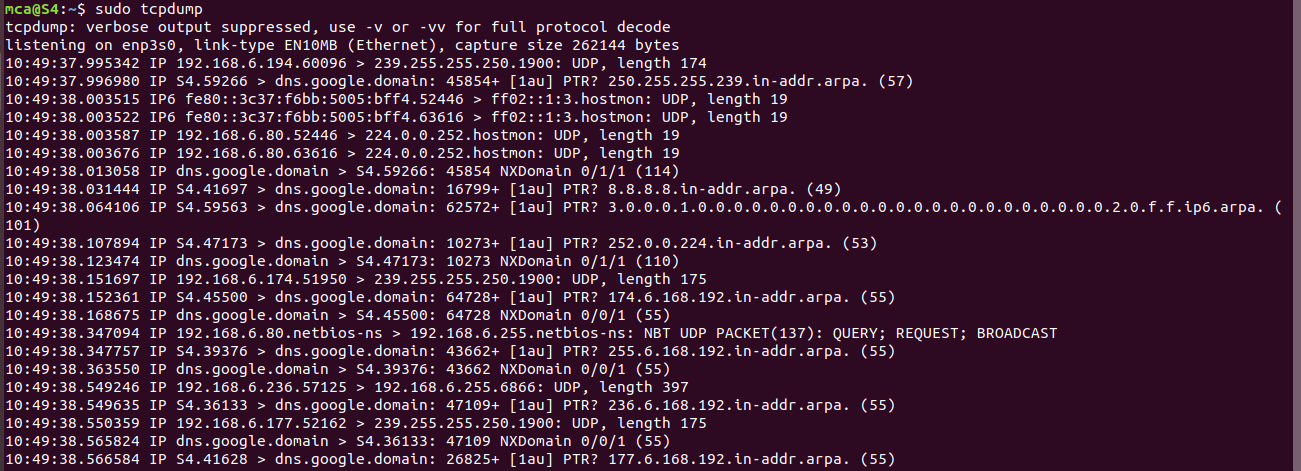
**Procedure & Output**

**Sudo apt update && sudo apt install tcpdump**

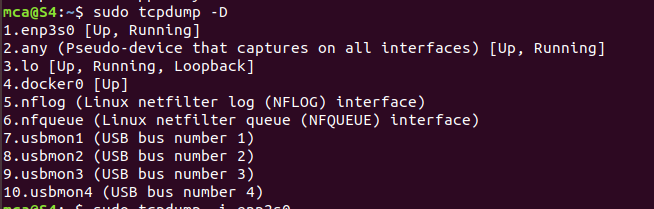
Update and install tcpdump on system.

****

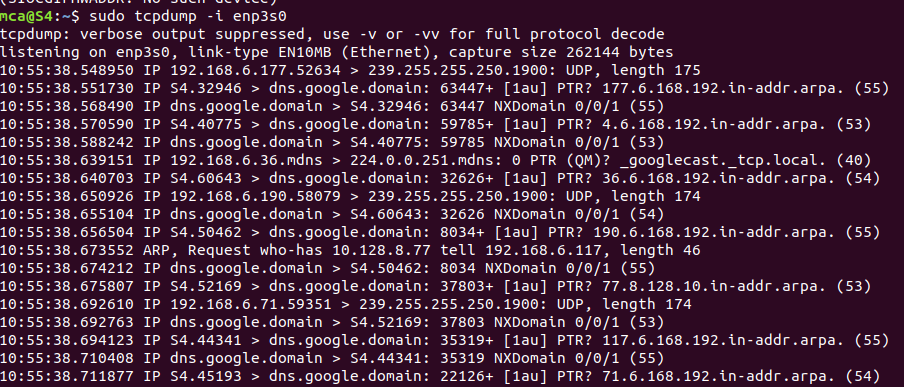
**Sudo tcpdump**

****

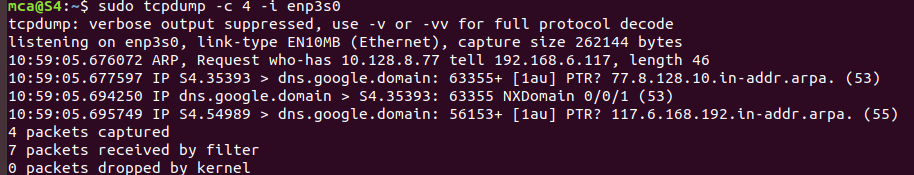
**Tcpdump –D:** To display all available interfaces

****

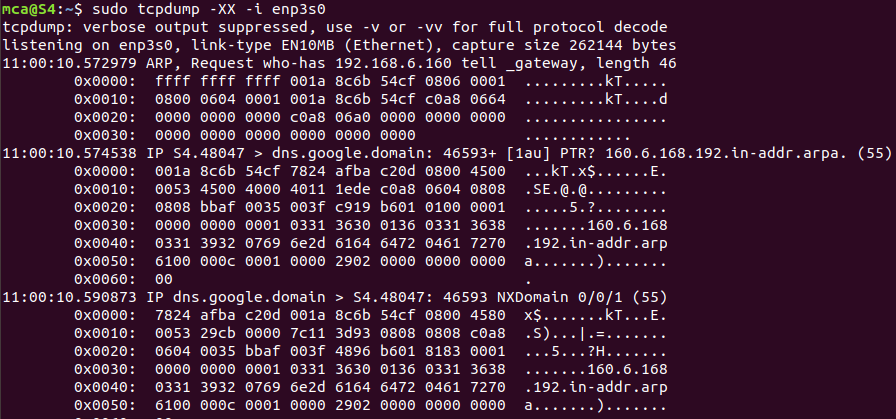
**Sudo Tcpdump –i enp3s0**

****

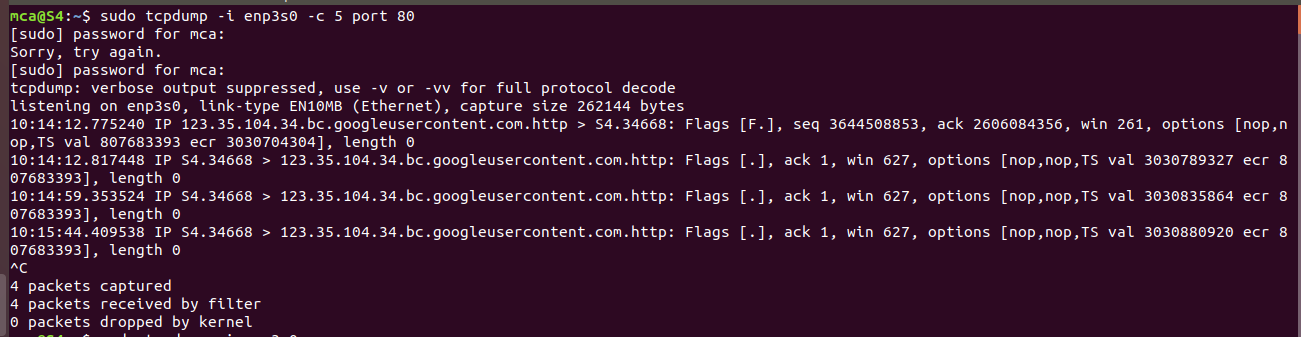
**sudotcpdump –c 4 –i enp5s0 :** It will capture all the packets for the specified interface, until you **hit**the cancel button. But using -c option, you can capture a specified number of packets.

****

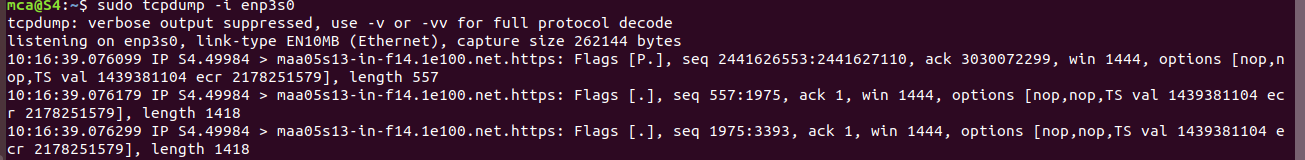
**sudotcpdump –c 4 –XX –i enp5s0 :** command -xx capture the data of each packet, including its link level header in **HEX** and **ASCII**format.

****

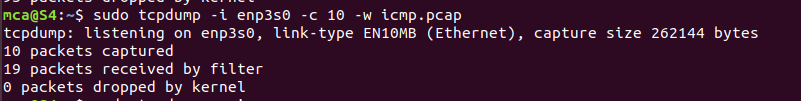
**sudotcpdump –i enp5s0 –c5 port 80 :** To filter packets based on the desired service or port, use the port filter.



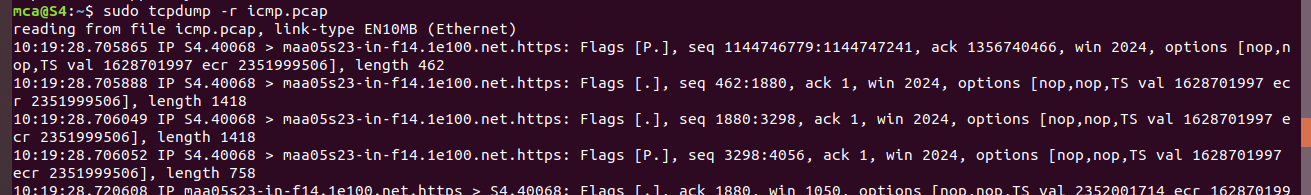
**Tcpdump –i enp3s0**



**Tcpdump –i enp3s0 –c 10 –w icmp.pcap**



**Sudo tcpdump –r icmp.pcap**To read and analyze capturedpacket **0001.pcap** file use the command with -r option.



**Sudo apt update**

