**Name: Joel John Joseph**

**Roll No: 8**

**Batch: B**

**Date: 02/06/22**

**NETWORKING & SYSTEM ADMINISTRATION LAB**

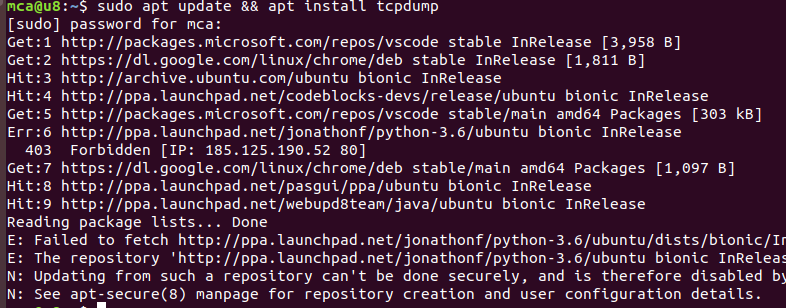
**Experiment No.: 4**

**Aim**

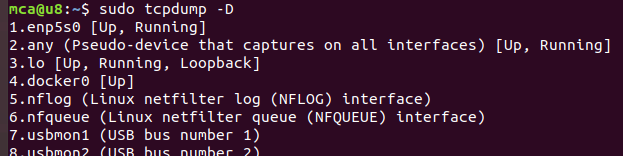
TCPDump

**Procedure**

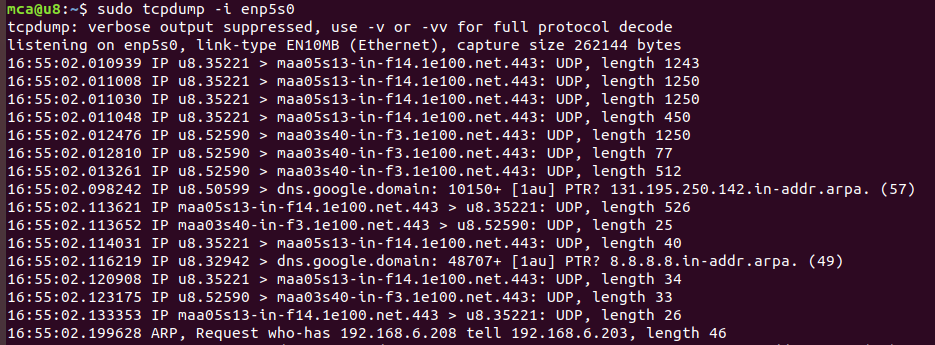
1. **sudo apt update && apt install tcpdump :** Update and install tcpdump on system.



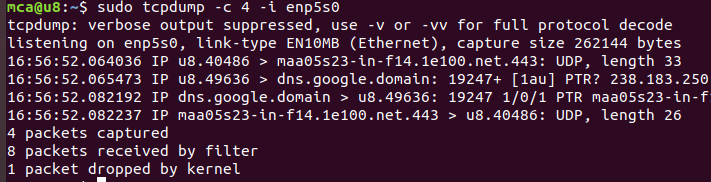
1. **sudo tcpdump –D :** To display all available interfaces



1. **sudo tcpdump –i enp3s0 :**



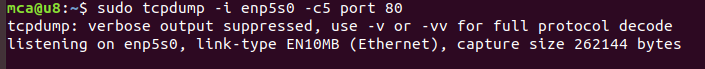
1. **sudo tcpdump –c 4 –i enp3s0 :** It will capture all the packets for the specified interface, until you **hit**the cancel button. But using -c option, you can capture a specified number of packets.



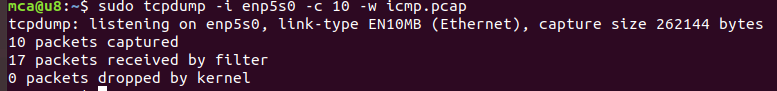
1. **sudo tcpdump –c 4 –xx –I enp3s0 :** command -xx capture the data of each packet, including its link level header in **HEX** and **ASCII**format.



1. **Sudo tcpdump –i enp3s0 –c5 port 80 :** To filter packets based on the desired service or port, use the port filter.



1. **sudo tcpdump –i enp3s0 –c 10 –w icmp.pcap :** **tcpdump**has a feature to capture and save the file in a **.pcap**format, to do this just execute the command with -w option.



1. **sudo tcpdump –r icmp.pcap :** To read and analyze captured packet **0001.pcap** file use the command with -r option.

