**Name: Vishnu Sadasivan**

**Roll No: 52**

**Batch: MCA-B**

**Date: 02-06-2022**

**NETWORKING & SYSTEM ADMINISTRATION LAB**

**Experiment No.: 25**

**Aim**

Familiarization of basic network commands in linux

**Procedure**

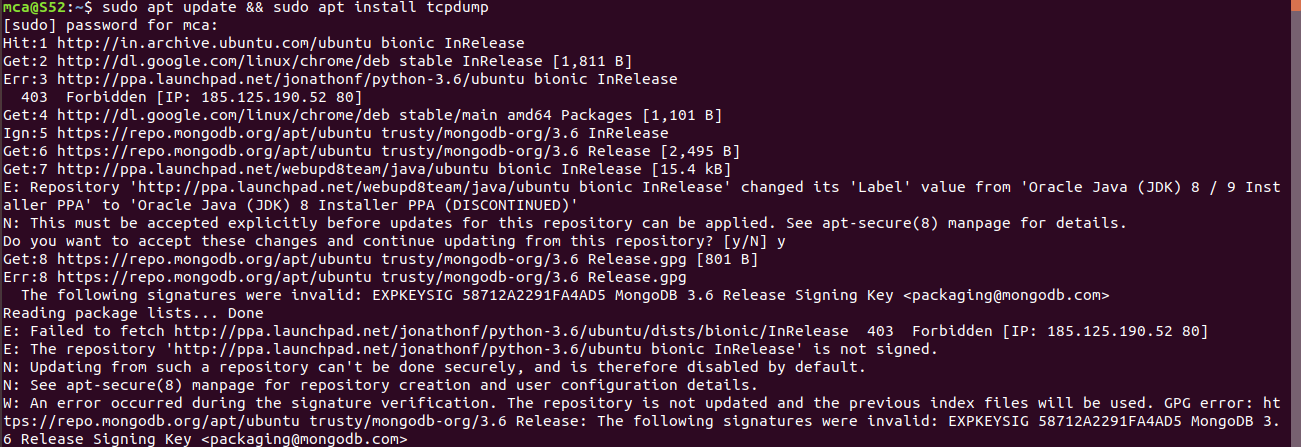
tcpdump is a data-network packet analyzer computer program that runs under a command line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software.

**1. sudo apt update && sudo install tcpdump**

This commands in Linux allows you to install the tcpdump packet analyzer on your system

**Syntax:-** $ sudo apt update && sudo install tcpdump

**Output:-**

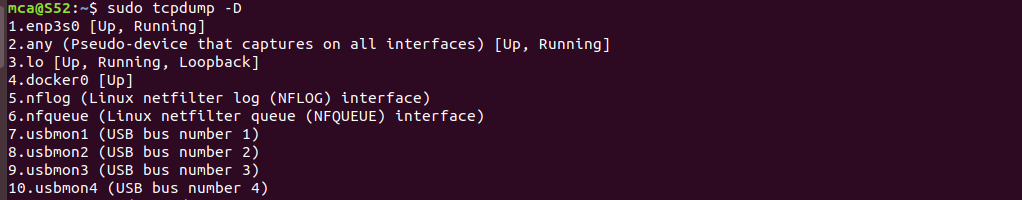


**2. sudo tcpdump -D**

To see the ist of network interfaces vailable on the system on which tcpdump can capture packets

**Syntax:-** $ sudo tcpdump -D

**Output:-**

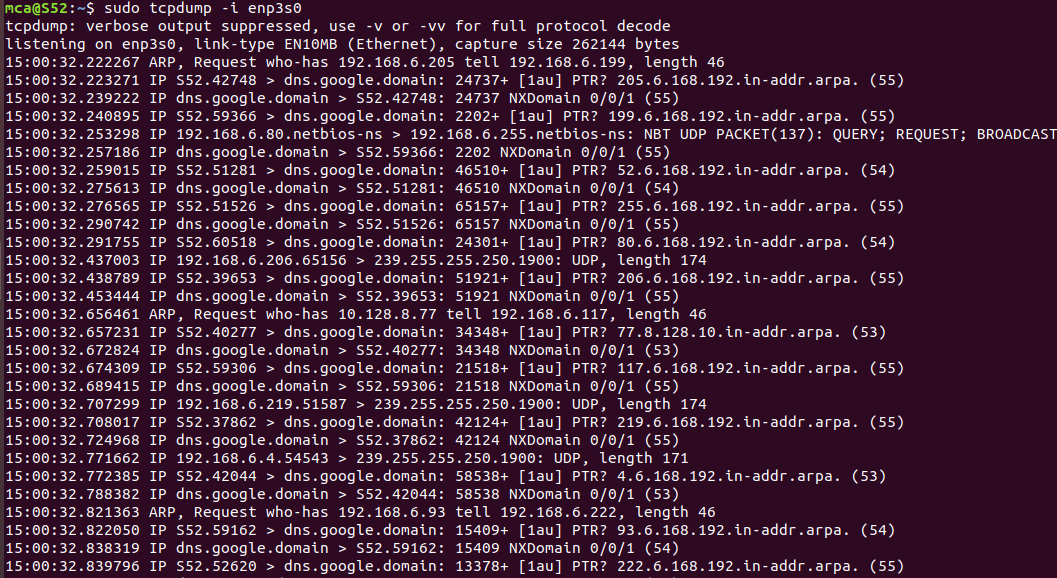


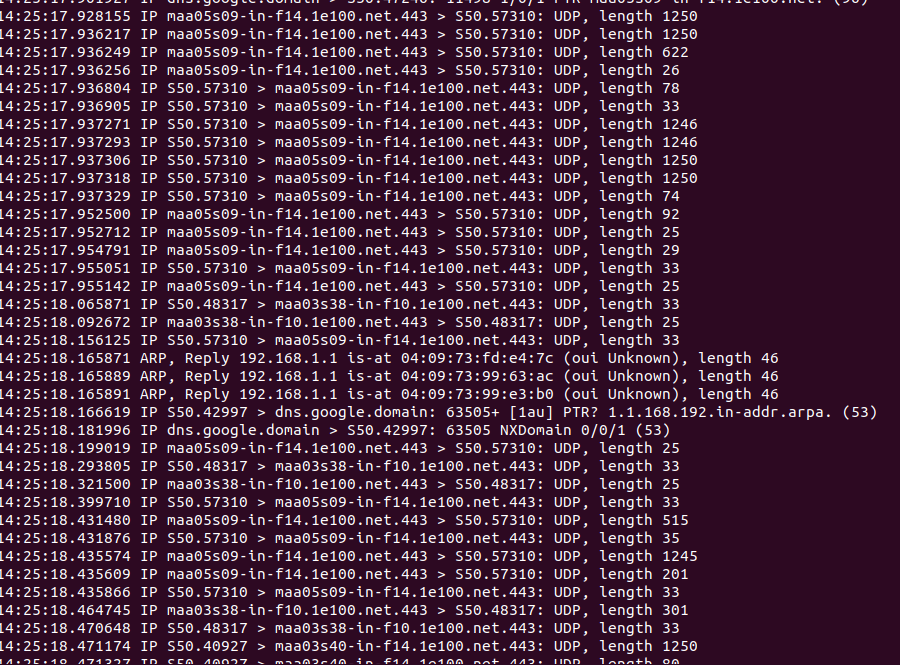
**3.** **sudo tcpdump -i enp3s0**

To capture the packets following through a specific interface, we can use the -i flag with the interface name. Without the -i interface , tcpdump will pick up the first network interface it comes across.

**Syntax:-** $ sudo tcpdump -i enp3s0

**Output:-**



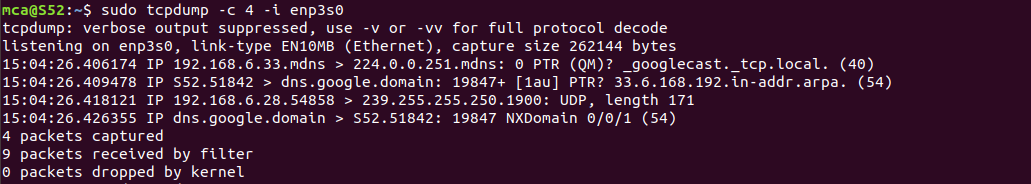
****

**4. sudo tcpdump -c 4 enp3s0 -i**

This command is used to show the details of last 4 packets only

**Syntax:-** $ sudo tcpdump -c 4 enp3s0 -i

**Output:-**



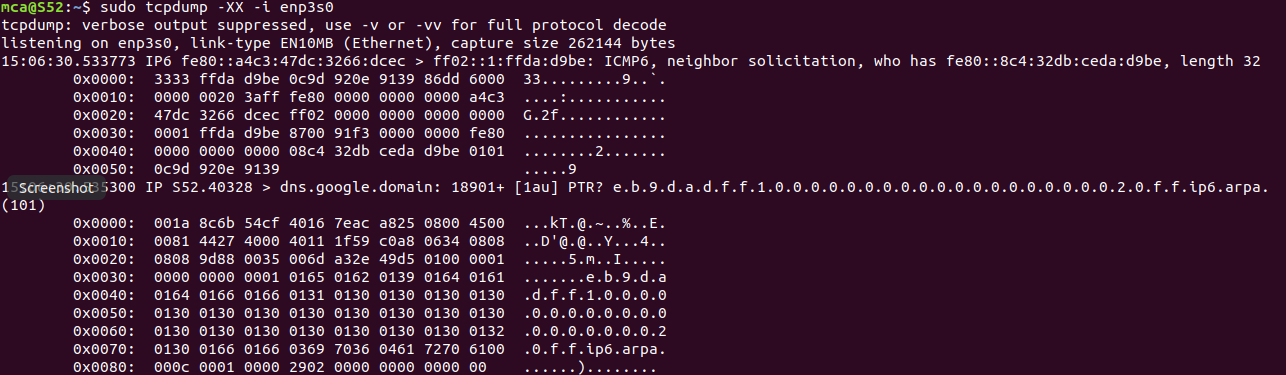
**5. sudo tcpdump -XX -i enp3s0**

This command helps to see the information of the ip address in terms of ipv6 addressing

(in hexadecimal format)

**Syntax:-** $ sudo tcpdump -XX -i enp3s0

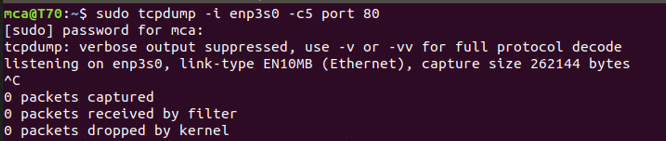
**Output:-**



**6. $ sudo tcpdump -i enp3s0 -c5 port 80**

To access information of packet from a specific port number

**Syntax:** $ sudo tcpdump -i <your\_ethernet\_interface> -c5 port <port\_number>

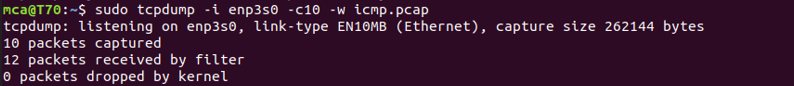
**Output:-** ****

**7. $ sudo tcpdump -i enp3s0 -c 10 -w icmp.pcap**

To store packet information limited by lines,words

**Syntax:-** $ sudo tcpdump -i <your\_ethernet\_interface> -c <lines> -w <filename>

**Output:-**

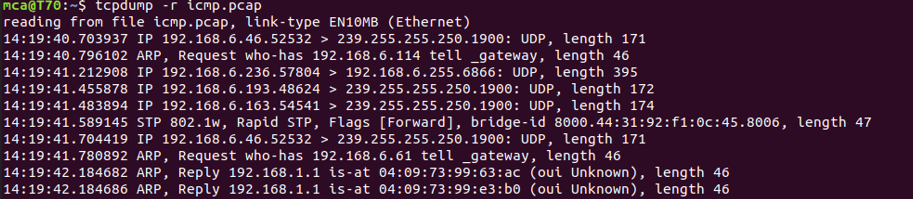
****

**8. $ sudo tcpdump -r icmp.pcap**

To read the content of a packet capture by using tcpdump

**Syntax:** $ sudo tcpdump -r <filename>

**Output:-**

****

**9. $ sudo nc -l -p 1234**

To send message from one console and receive from another console by an advanced packet analyzer

**Syntax:** **$ sudo nc -l -p 1234**

**Output:-**

** **