**Name: Sreelakshmi M Nair**

**Roll No: 40**

**Batch: B**

**Date: 06/06/2022**

**NETWORKING & SYSTEM ADMINISTRATION LAB**

**Experiment No.: 23**

**Aim**

TCPDUMP installation.

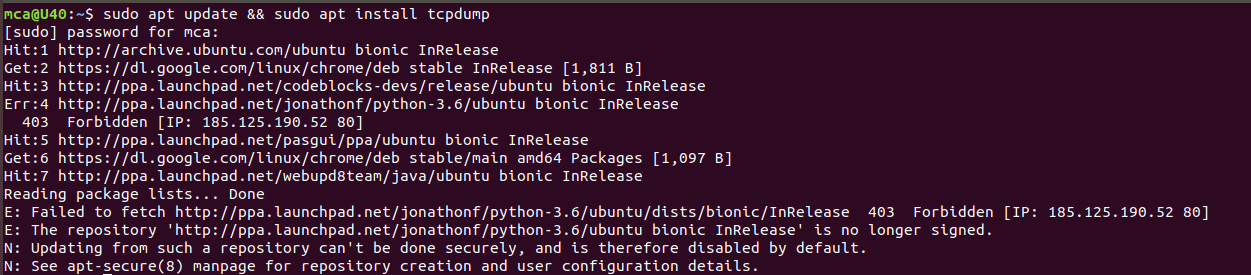
**Procedure**

**1. update and install**

This command is used to install and update tcpdump.

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

Output :-

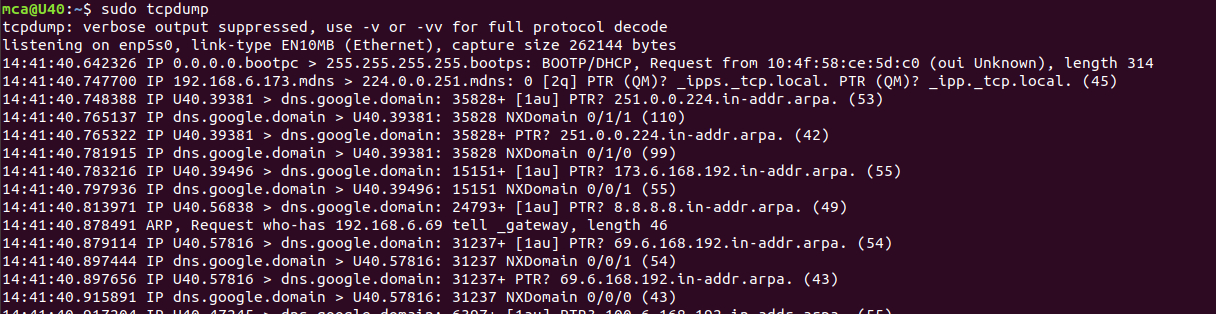


**2. sudo tcpdump**

This command is used to show all the interfaces connected to the inertnet packets.

Syntax :- $ sudo tcpdump

Output :-

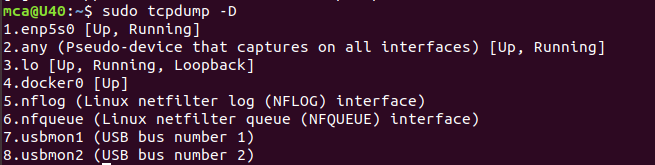


**3. -D**

This command is used to find specific interfaces.

Syntax :- $ sudo tcpdump -D

Output :-

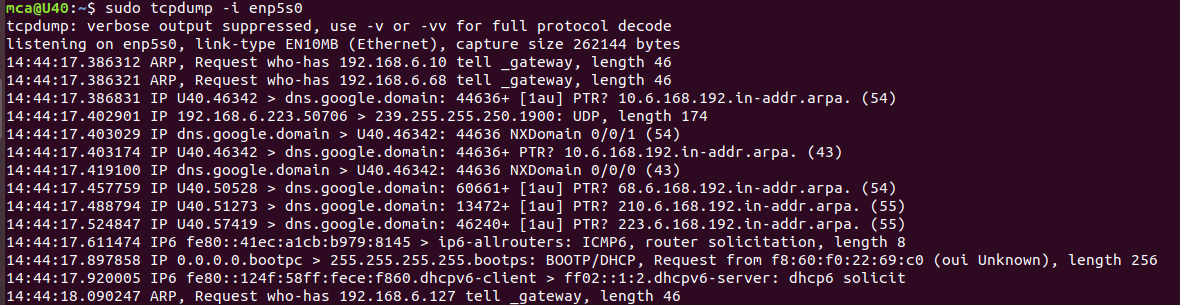


**4. -i**

This command is used to find the interface which is connected to our system.

Syntax :- $ sudo tcpdump -i enp5s0

Output :-

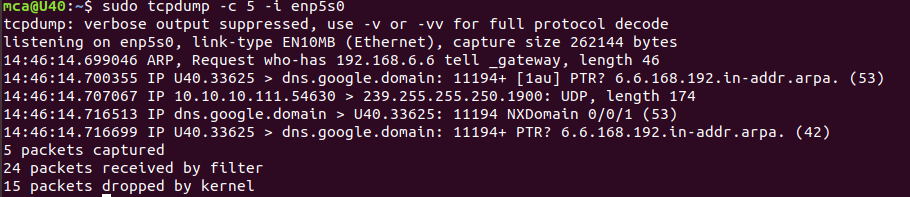


**5. -c 5 -i**

This command is used to access only 5 packets.

Syntax :- $ sudo tcpdump -c 5 -i enp5s0

Output:-

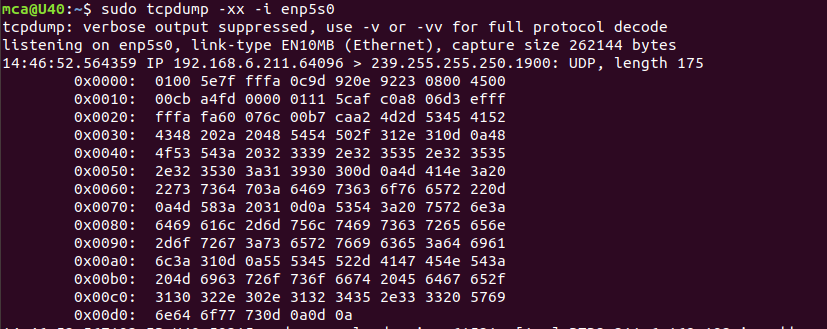


**6. -xx -i**

This command is used show all nformation in ASCII value.

Syntax :- $ sudo tcpdump -xx -i enp5s0

Output :-

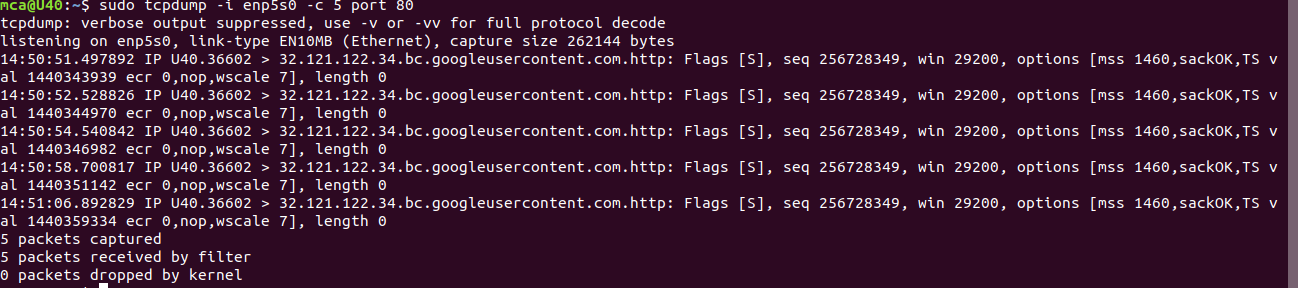


**7. sudo tcpdump -i enp5s0 -c 5 port 80**

This command is used to show a specified number of packets in that particular port number.

Syntax :- $ sudo tcpdump -i enp5s0 -c 5 port 80

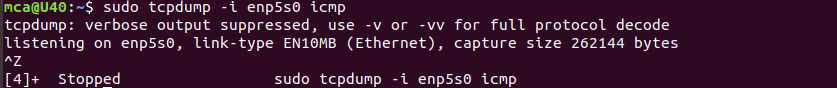
Output :-



**8. sudo tcpdump -i enp5s0 icmp**

Syntax :- $ sudo tcpdump -i enp5s0 icmp

Output :-

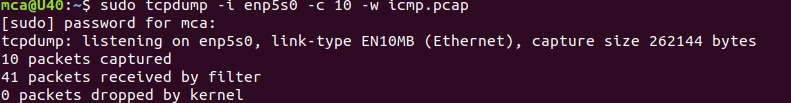


**9. sudo tcpdump -i enp5s0 -c 10 -w icmp.filename**

This command is used to capturing packets and stored in a pcap file.

Syntax :- $ sudo tcpdump -i enp5s0 -c 10 -w icmp.filename

Output :-

****

**10. sudo tcpdump -r icmp.filename**

This command use to read that particular file using -r flag.

Syntax :- $ sudo tcpdump -r icmp.filename

Output :-

