**Name: merin joseph**

**Roll No:20**

**Batch:b**

**Date:23-05-2022**

**NETWORKING & SYSTEM ADMINISTRATION LAB**

**Experiment No.: 27**

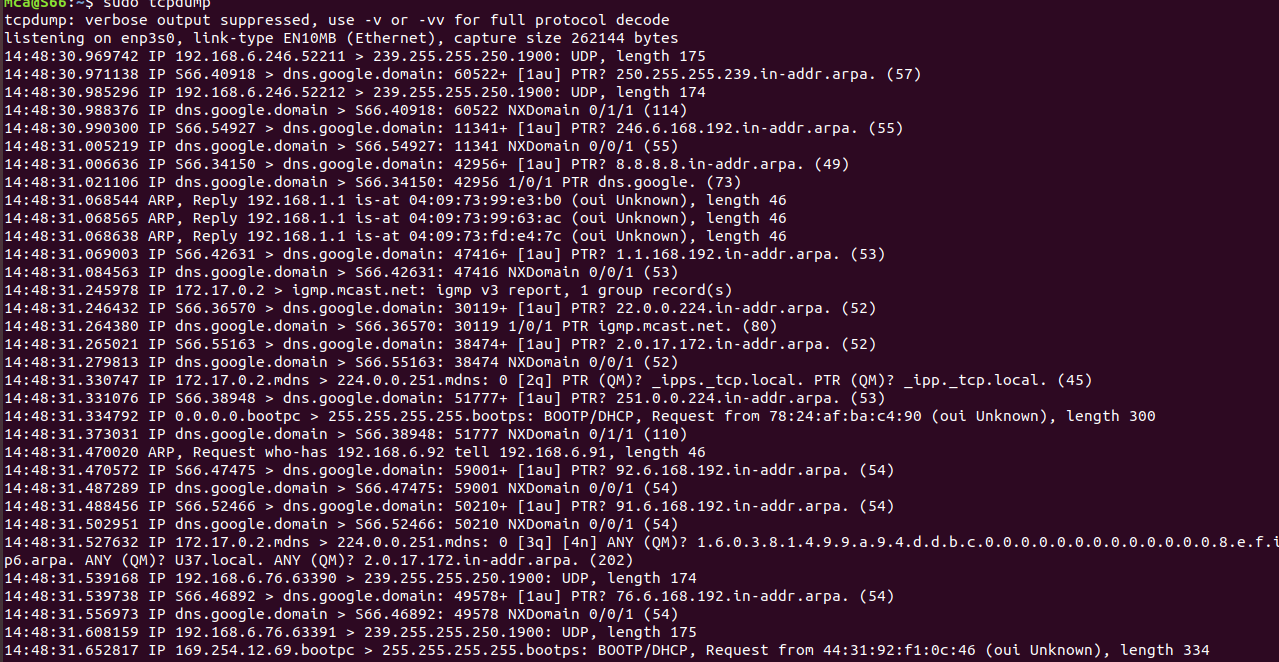
**Aim**

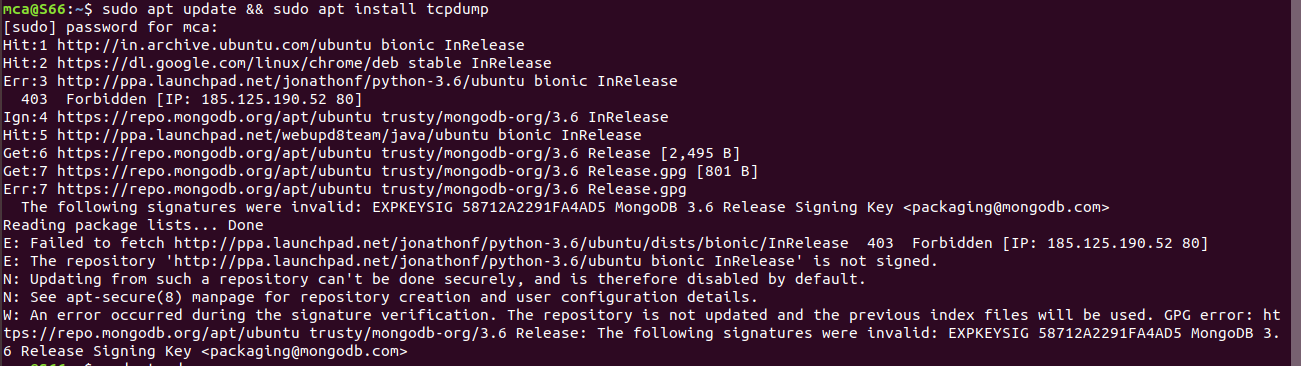
Analyzing network packet stream using tcpdump and wireshark. Perform basic network service tests using nc.

**Procedure**

1. How to Install tcpdump in Linux

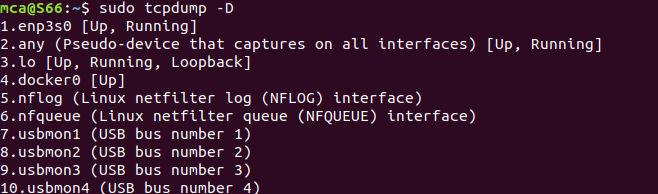
Many Linux distributions already shipped with the tcpdump tool, if in case you don’t have it on a system, you can install it using the command.

$ sudo apt-get install tcpdump [On Debian, Ubuntu and Mint]

****

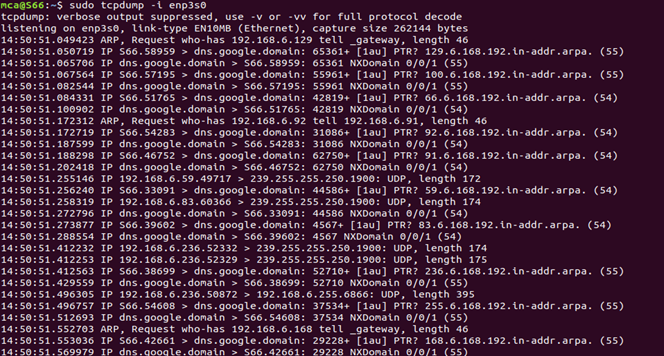
1. Display Available Interfaces

To list the number of available interfaces on the system, run the following command with -D option.



1. Capture Packets from Specific Interface

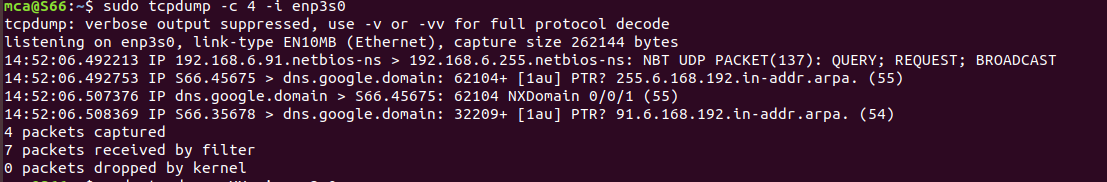
The command screen will scroll up until you interrupt and when we execute the tcpdump command it will captures from all the interfaces, however with -i switch only capture from the desired interface.



1. Capture Only N Number of Packets

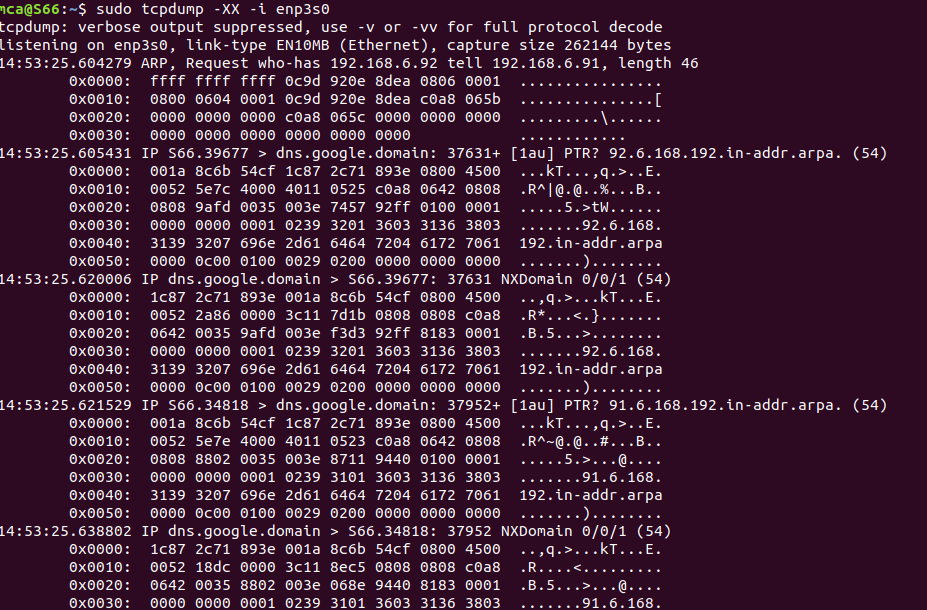
When you run the tcpdump command it will capture all the packets for the specified interface, until you hit the cancel button. But using -c option, you can capture a specified number of packets.

# tcpdump –c 5 –i enp3s0



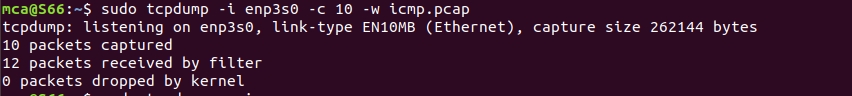
1. Display Captured Packets in HEX and ASCII

The following command with option -XX capture the data of each packet, including its link level header in HEX and ASCII format



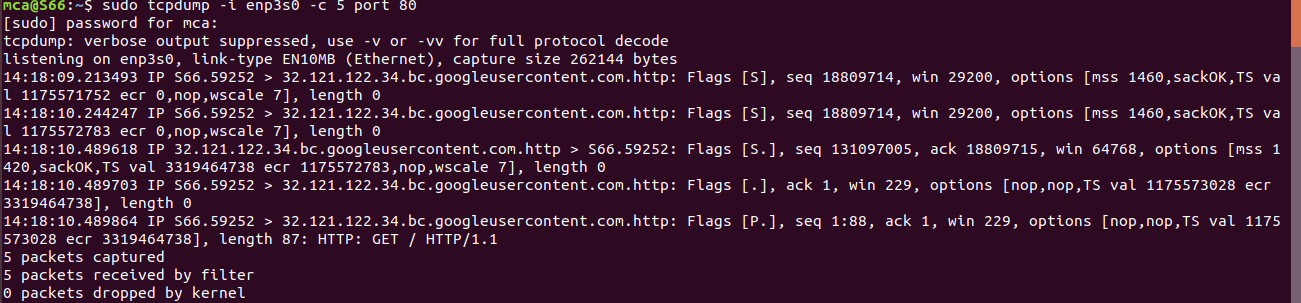
1. Capture and Save Packets in a File

As we said, that tcpdump has a feature to capture and save the file in a .pcap format, to do this just execute the command with -w option.



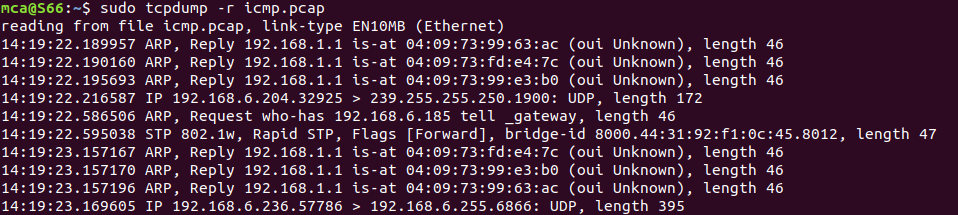
1. Capture Packet from Specific Port

Let’s say you want to capture packets for specific port 80, execute the below command by specifying port number 80 as shown below.



1. Read Captured Packets File

To read and analyze captured packet 0001.pcap file use the command with -r option.



**wire shark**

Installing Wireshark on Ubuntu 20.04

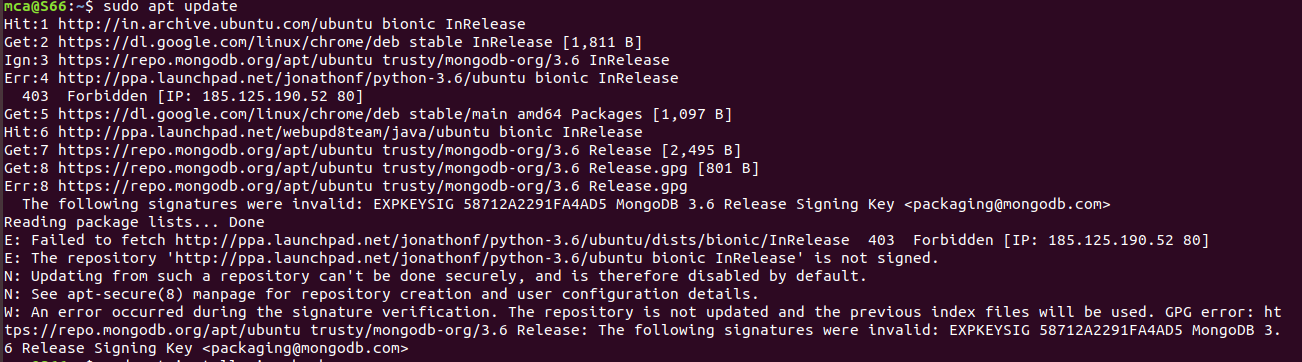
The Wireshark utility is available on all major desktop platforms, i.e., Linux, Microsoft Windows, FreeBSD, MacOS, Solaris, and many more. Follow the steps below to install Wireshark on Ubuntu 20.04.

STEP1 : Update APT

First, as always, update and upgrade your APT through the following command.

Syntax:

**$ sudo apt update**

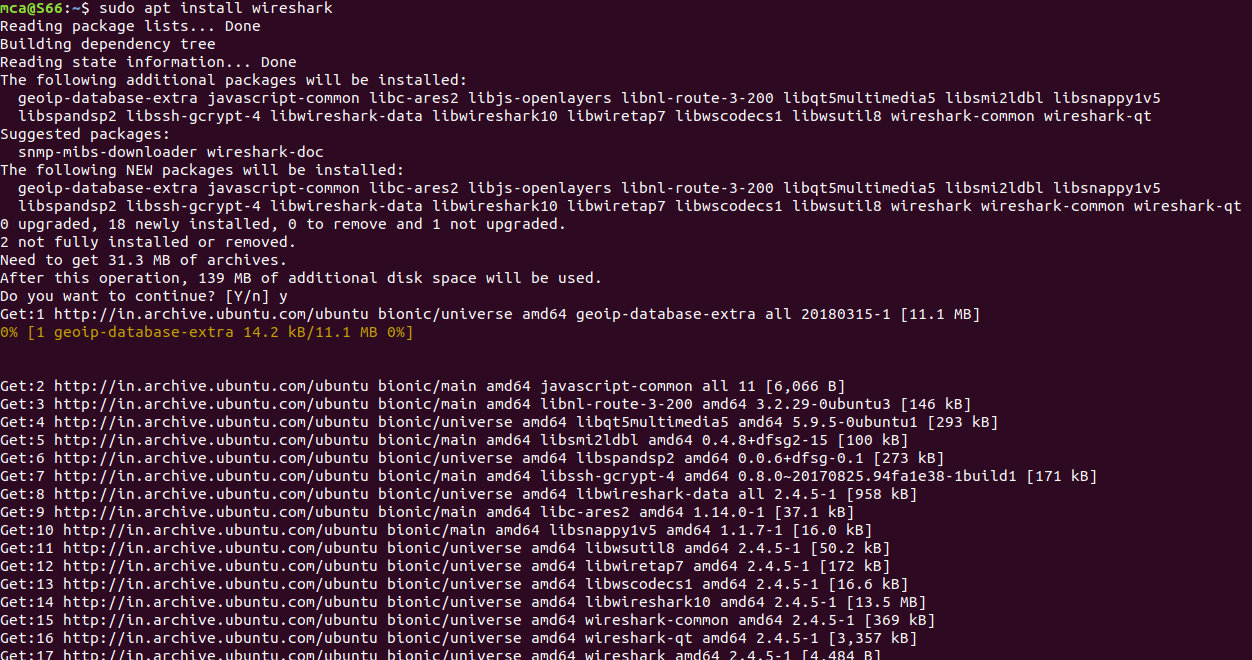
****

Step 2: Download and Install Wireshark

Now that Wireshark’s latest version has been added to the APT, you can download and install it with the following command.

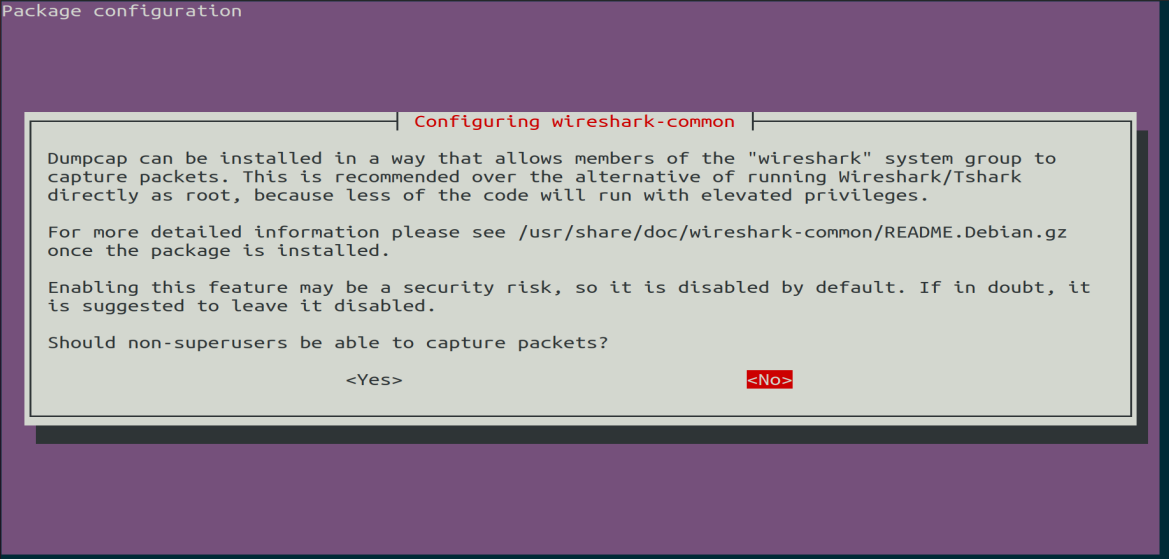
syntax

**$ sudo apt install wireshark**



Step 3: Enable Root Privileges

When Wireshark installs on your system, you will be prompted by the following window. As Wireshark requires superuser/root privileges to operate, this option asks to enable or disable permissions for all every user on the system. Press the “Yes” button to allow other users, or press the “No” button to restrict other users from using Wireshark.



Step 4:

You must add a username to the Wireshark group so that this user can use Wireshark. To do this, execute the following command, adding your required username after “wireshark” in the command.

Syntax:

**$ sudo adduser $user wireshark**

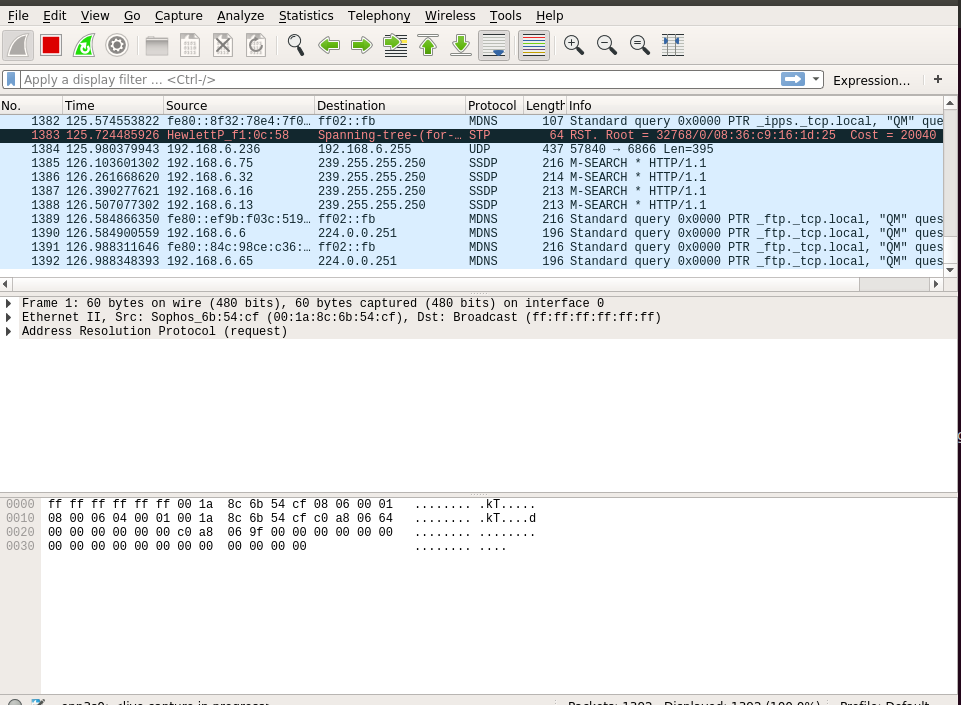


Step 5: Launch Wireshark

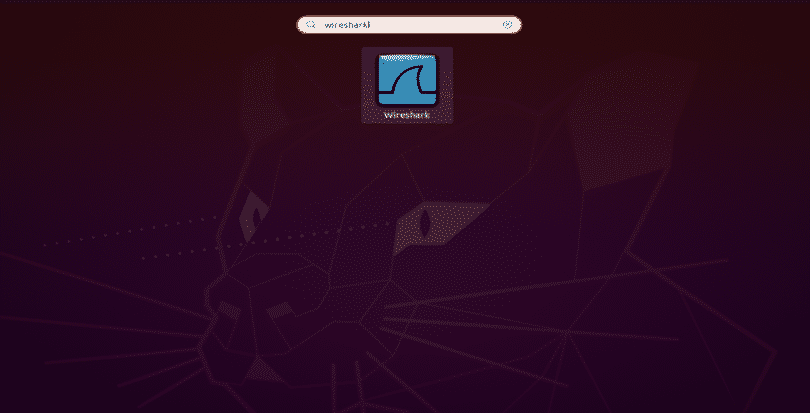
In the terminal window, type the following command to start the Wireshark application.

Syntax:

**$ wireshark**



You can also open Wireshark through the Graphical User Interface (GUI) by opening the activities on the Ubuntu desktop, and in the search bar, type “Wireshark,” and click on the application result.



**netcat**