# Experiment No : 9

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

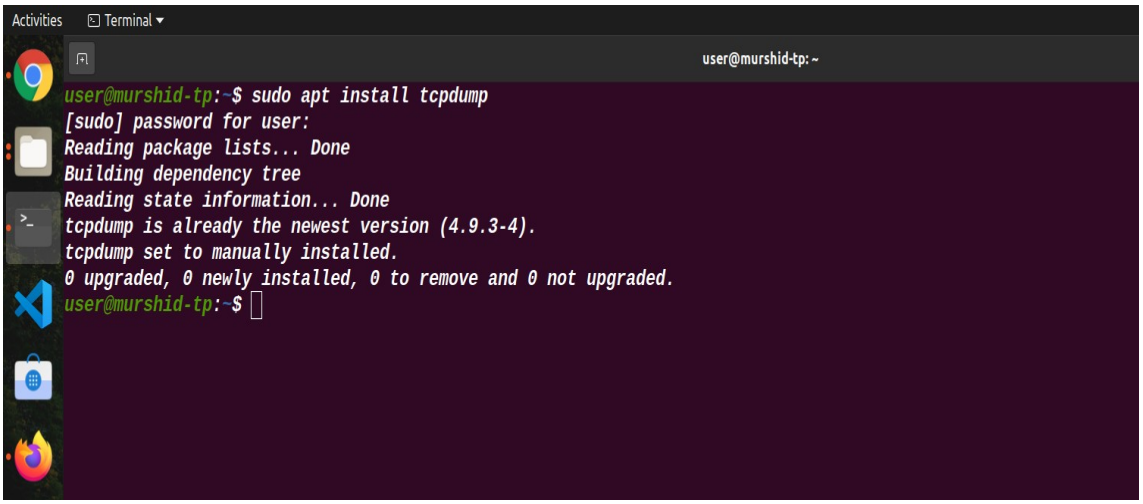
## Tcpdump

Tcpdump is a type of packet analyzer software utility that monitors and logs TCP/IP traffic passing between a network and the computer on which it is executed.
Tcpdump is an open-source network utility that is freely available under the BSD license. Tcpdump works on the command line interface and provides descriptions of packet content in several formats, depending on the command used.

Tcpdump is primarily a network monitoring and management utility that captures and records TCP/IP data on the run time. Tcpdump is designed to provide statistics about the number of packets received and captured at the operating node for network performance analysis, debugging and diagnosing network bottlenecks and other network oriented tasks.

Because it is a command line utility, data retrieved through tcpdump can vary. For example, when used with -A operator, it prints out each packet in ASCII format. Tcpdump is supported by most Unix-based operating systems, such as Linux, Mac OSX and BSD. The Windows variant of tcpdump is known as WinDump.

## Installing tcpdump

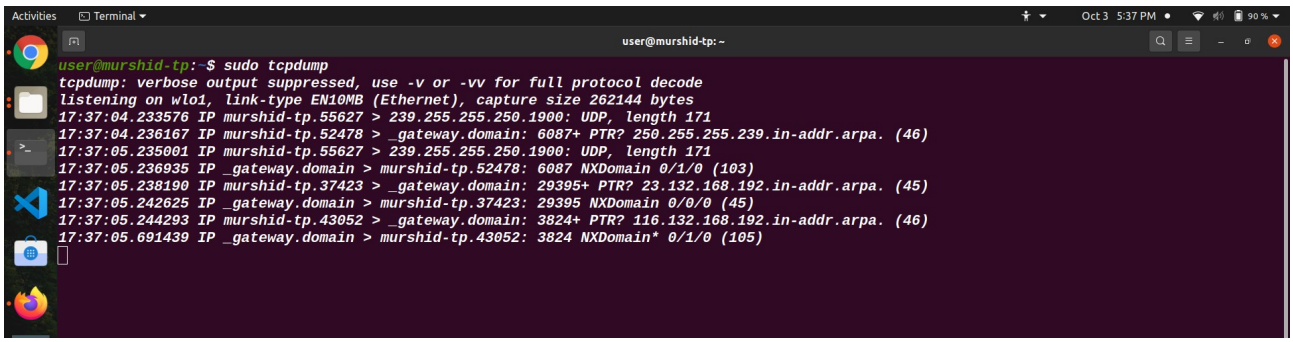


## Working with tcpdump command

**1.**To capture the packets of current network interface

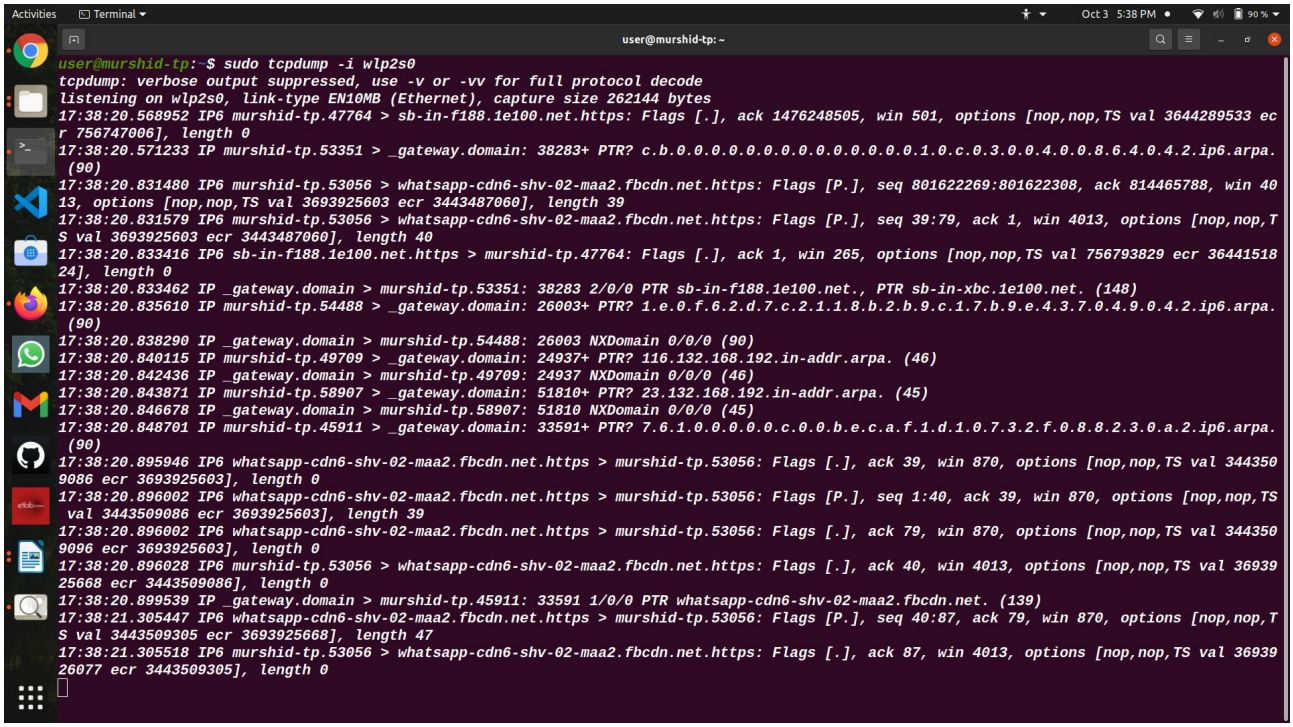
sudo tcpdump

This will capture the packets from the current interface of the network through which the system is connected to the internet.




**2.** To capture packets from a specific network interface

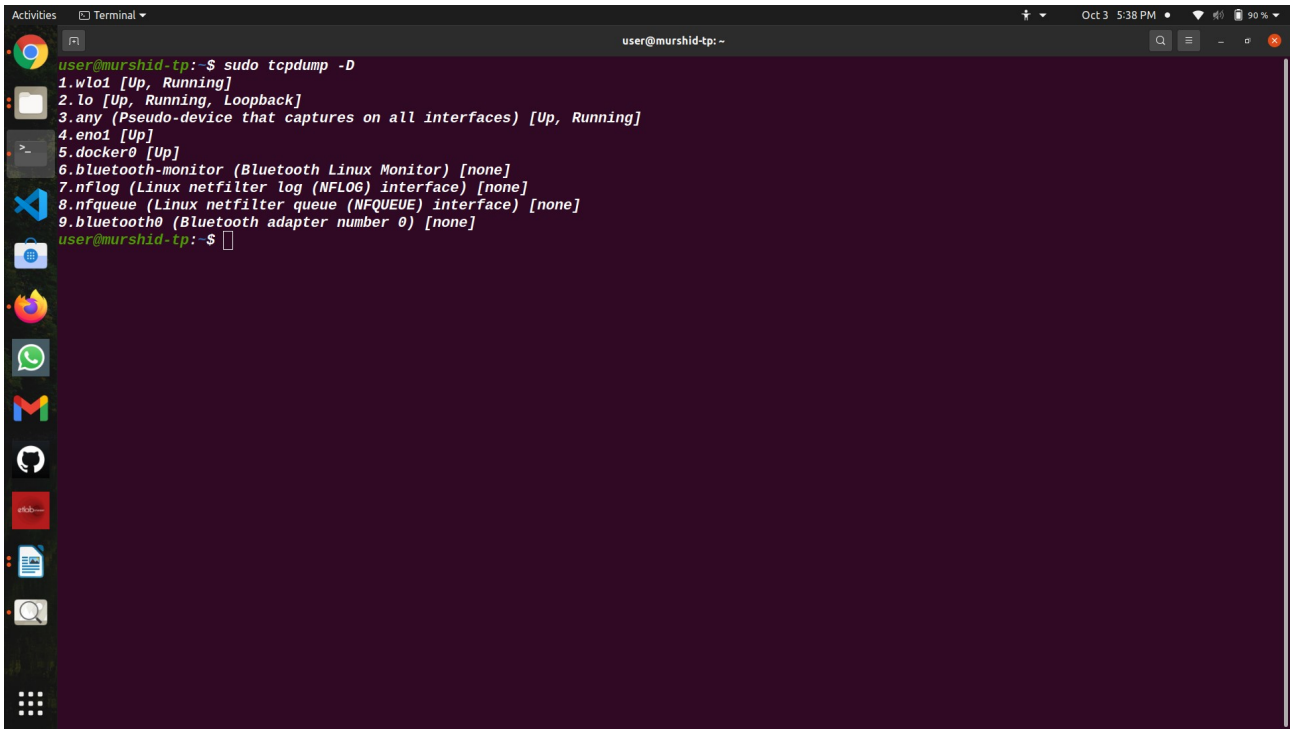
sudo tcpdump -i wlp2s0



This command will now capture the packets from wlp2s0 network interface.

**3.** To display all available interfaces

sudo tcpdump -D




## Wireshark

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network.

Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

1. **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.

2. **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.

3. **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

## Uses of Wireshark

It is used by network security engineers to examine security problems.

1.It allows the users to watch all the traffic being passed over the network.

2.It is used by network engineers to troubleshoot network issues.

3.It also helps to troubleshoot latency issues and malicious activities on your network.

4.It can also analyze dropped packets.

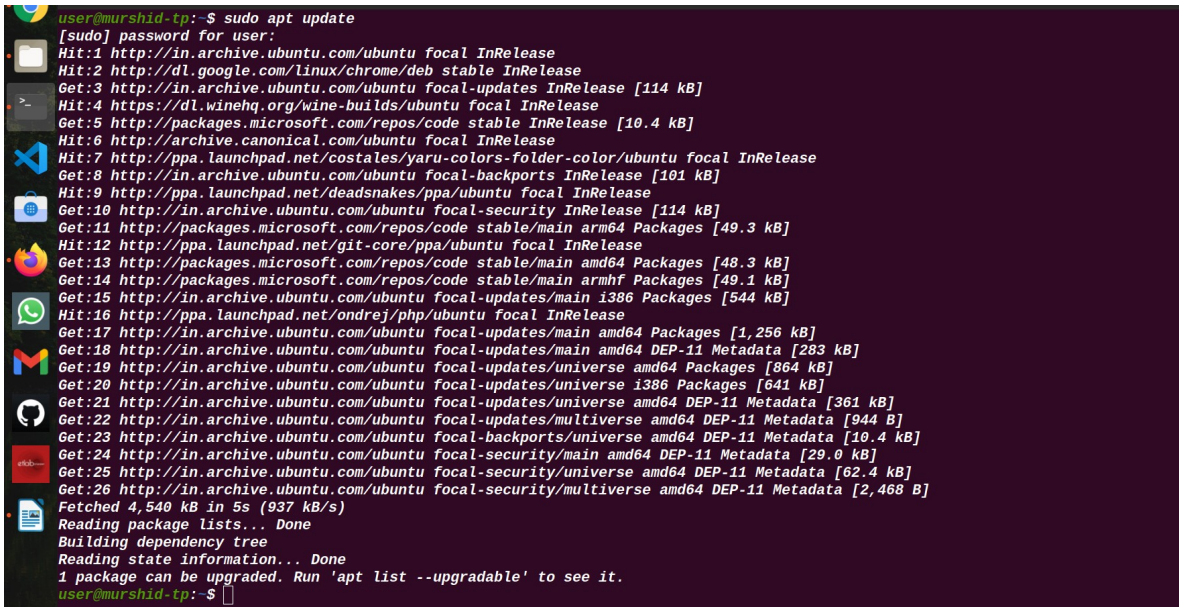
5.It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

## Wireshark installation

### Step 1: Update APT

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

*$ sudo apt update*

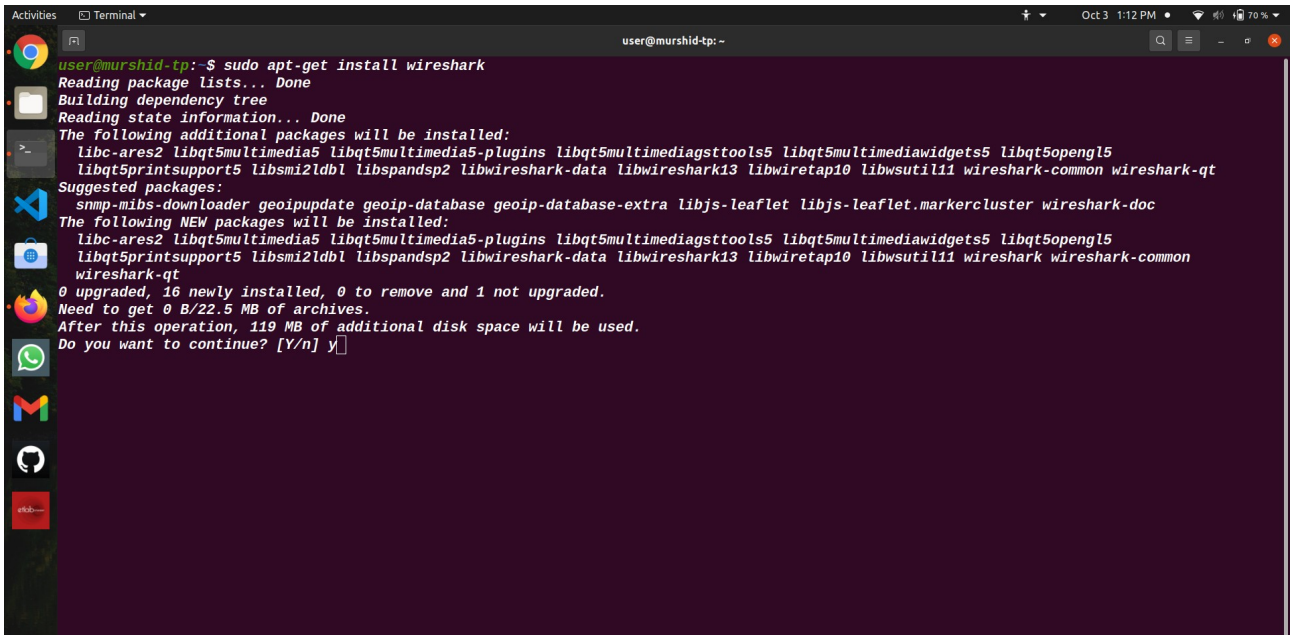


```
user@murshid-tp:~$ sudo apt update
[sudo] password for user:
Hit:1 http://in.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://dl.google.com/linux/chrome/deb stable InRelease
Get:3 http://in.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Hit:4 https://dl.winehq.org/wine-builds/ubuntu focal InRelease
Get:5 http://packages.microsoft.com/repos/code stable InRelease [10.4 kB]
Hit:6 http://archive.canonical.com/ubuntu focal InRelease
Hit:7 http://ppa.launchpad.net/costales/yaru-colors-folder-color/ubuntu focal InRelease
Get:8 http://in.archive.ubuntu.com/ubuntu focal-backports InRelease [101 kB]
Hit:9 http://ppa.launchpad.net/deadsnakes/ppa/ubuntu focal InRelease
Get:10 http://in.archive.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:11 http://packages.microsoft.com/repos/code stable/main arm64 Packages [49.3 kB]
Hit:12 http://ppa.launchpad.net/git-core/ppa/ubuntu focal InRelease
Get:13 http://packages.microsoft.com/repos/code stable/main amd64 Packages [48.3 kB]
Get:14 http://packages.microsoft.com/repos/code stable/main armhf Packages [49.1 kB]
Get:15 http://in.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages [544 kB]
Hit:16 http://ppa.launchpad.net/ondrej/php/ubuntu focal InRelease
Get:17 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [1,256 kB]
Get:18 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metadata [283 kB]
Get:19 http://in.archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [864 kB]
Get:20 http://in.archive.ubuntu.com/ubuntu focal-updates/universe i386 Packages [641 kB]
Get:21 http://in.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-11 Metadata [361 kB]
Get:22 http://in.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 DEP-11 Metadata [944 B]
Get:23 http://in.archive.ubuntu.com/ubuntu focal-backports/universe amd64 DEP-11 Metadata [10.4 kB]
Get:24 http://in.archive.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Metadata [29.0 kB]
Get:25 http://in.archive.ubuntu.com/ubuntu focal-security/universe amd64 DEP-11 Metadata [62.4 kB]
Get:26 http://in.archive.ubuntu.com/ubuntu focal-security/multiverse amd64 DEP-11 Metadata [2,468 B]
Fetched 4,540 kB in 5s (937 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
1 package can be upgraded. Run 'apt list --upgradable' to see it.
user@murshid-tp:~$
```

### Step 2: Download and Install Wireshark

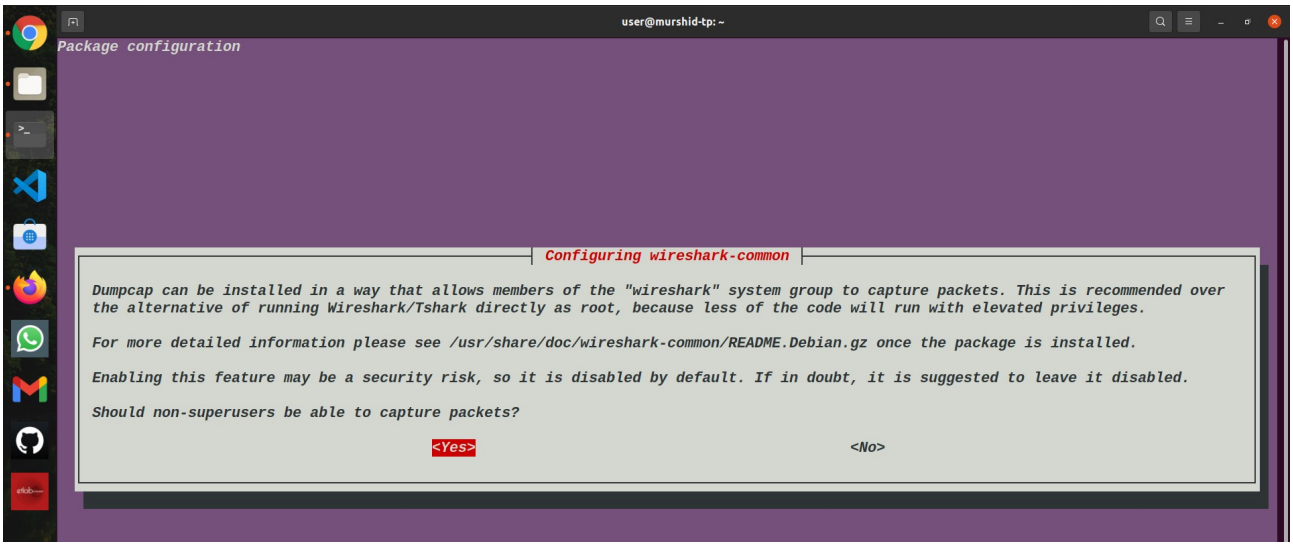
Now that Wireshark's latest version has been added to the APT, you can download and install it with the following command.

*$ sudo apt-get install wireshark*




## Step 3: Enable Root Privileges

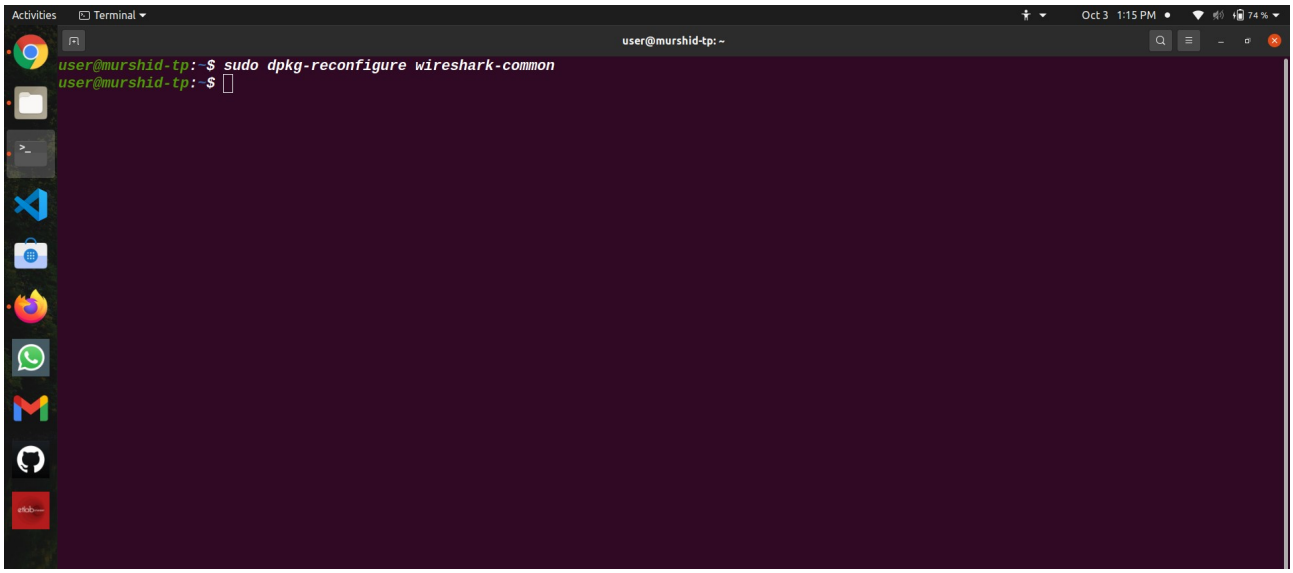
When Wireshark installs on your system, you will be prompted by the following window. As Wireshark requires superuser/root privileges to operate, this option asks to enable or disable permissions for all every user on the system. Press the “Yes” button to allow other users, or press the “No” button to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

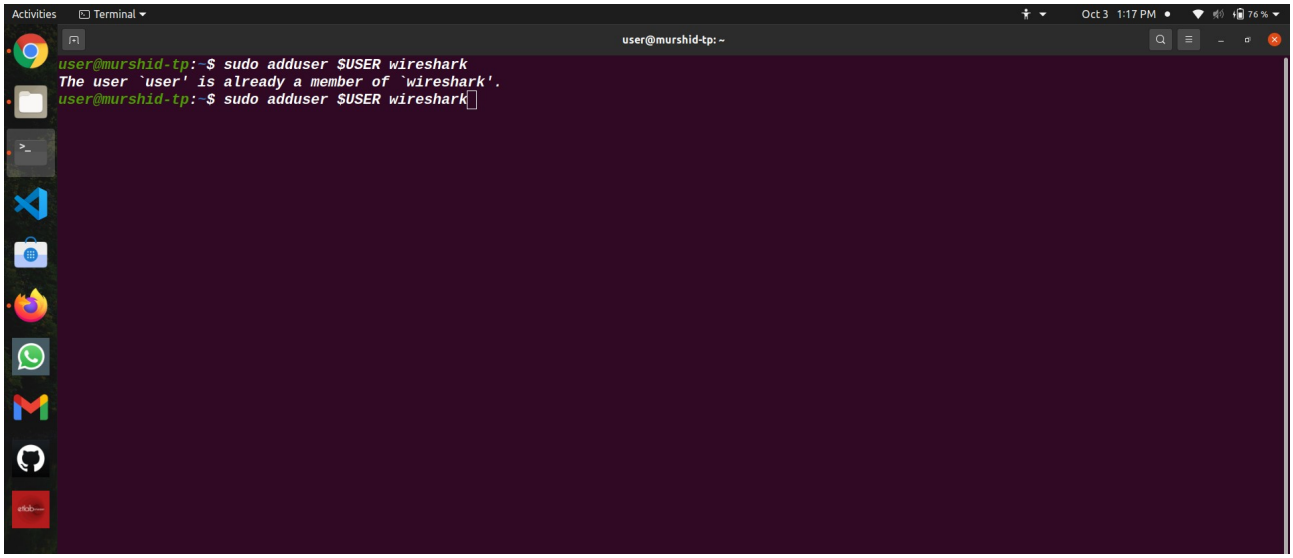


**Step 4: (Optional) Reconfigure Permission Settings**

If you have selected “No” in the above scenario, then you can change this selection again by executing the following command, which will reconfigure the Wireshark permission settings.

*$ sudo dpkq-reconfigure wireshark-common*

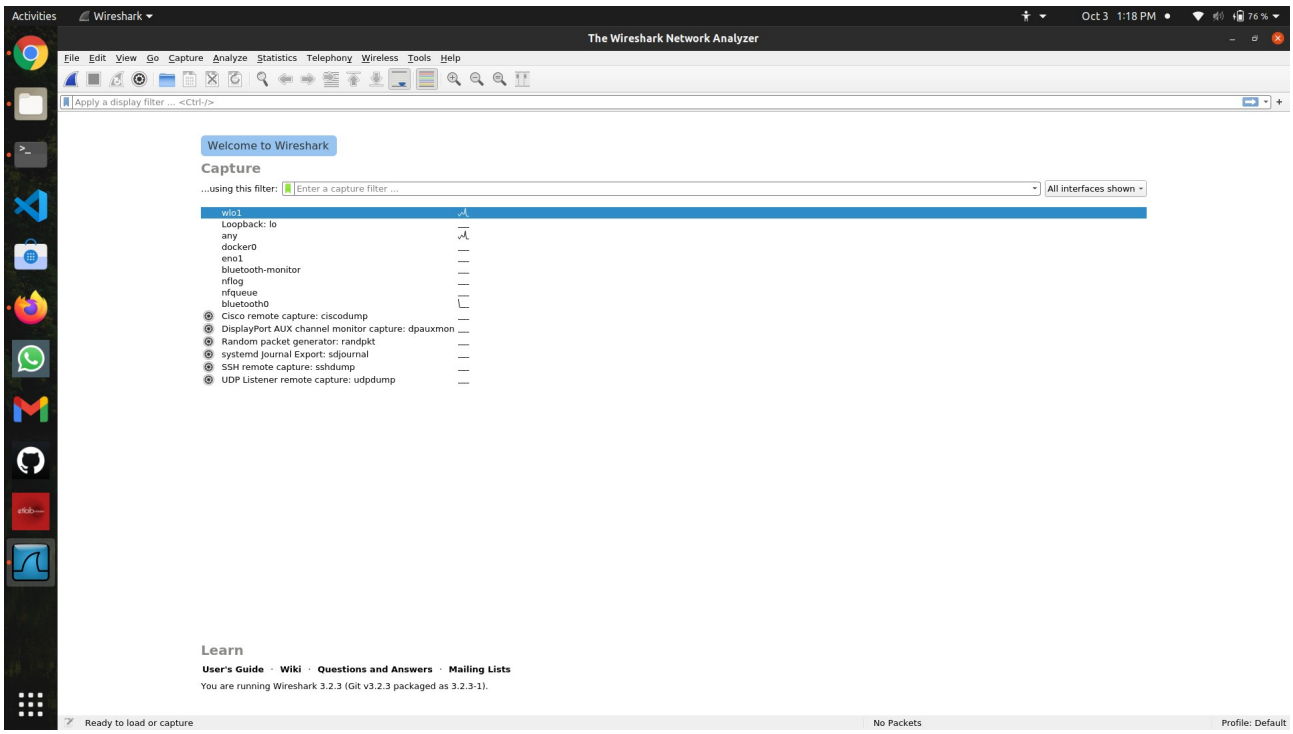


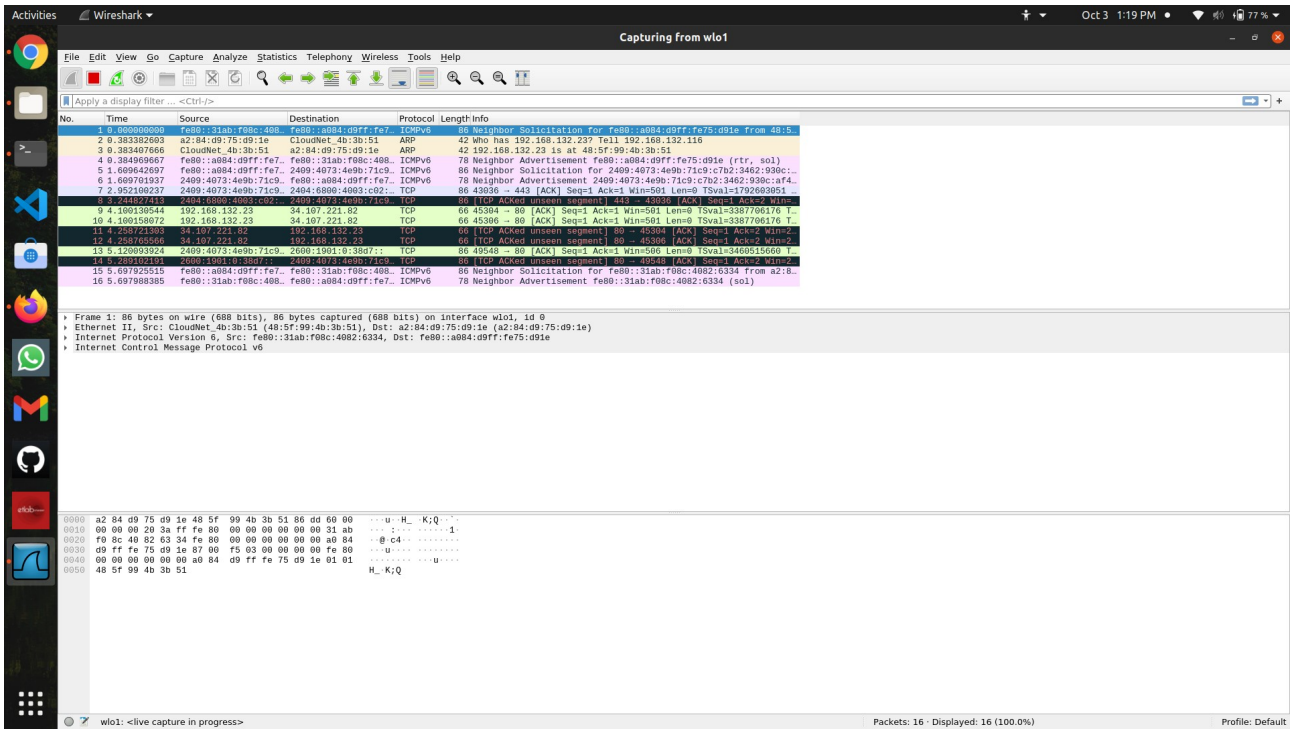




**Step 5: Launch Wireshark**

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

*$ sudo wireshark*



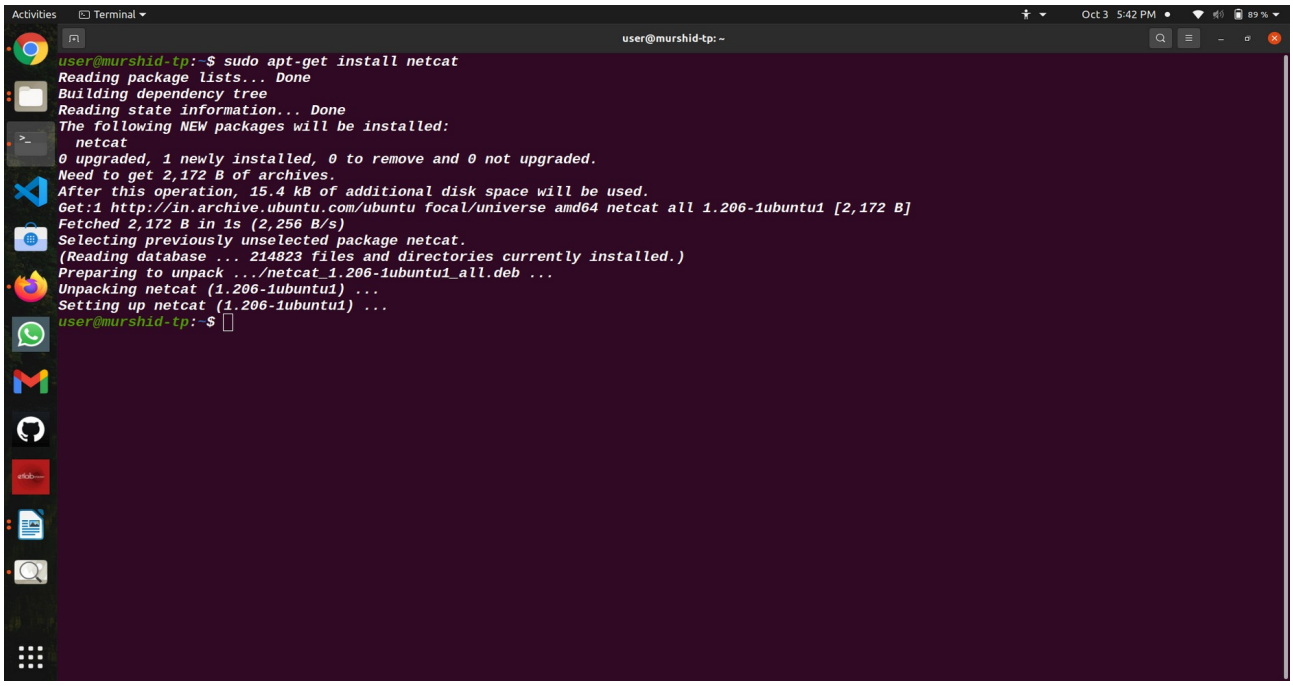

# Netcat

**Netcat (or nc in short) is a simple yet powerful [networking command-line tool] used for performing any operation in Linux related to TCP, UDP, or UNIX-domain sockets.**

**Netcat** can be used for port scanning, **port redirection**, as a port listener (for incoming connections); it can also be used to open remote connections and so many other things. Besides, you can use it as a backdoor to gain access to a target server.

**Installing netcat on linux:**

*sudo apt-get install netcat*




**Port scanning:**

**Netcat can be used for port scanning: to know which ports are open and running services on a target machine. It can scan a single or multiple or a range of open ports.**

**The -z option sets nc to simply scan for listening daemons, without actually sending any data to them. The -v option enables verbose mode and -w specifies a timeout for connection that can not be established.**

**Syntax:**

nc -vz IP_address port

**Connection timed out:**

A *connection timed out* response indicates that your connection is not working, which could mean your firewall is blocking the port. Test the connection status by adding a rule that accepts connections on the required port.

**Connection succeeded**

If the initial connection succeeds, Netcat can connect to the service. Look at the connection in more detail.

**Syntax:**

nc -vt IP Address Port

**Closing the connection**

You can terminate the connection by either pressing **Ctrl-C** or type the service-specific quit command.