Name: Priyush B. Khobragade

PRN: 211112018

Batch: 03

EXPERMINT: 08

●Aim: - -Installation and configuration of Wire shark.

●Theory:

Wireshark

Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.

It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems.

Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called as a free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.

Features:

The following are some of the many features wireshark provides:

- Available for UNIX and Windows.
- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/WinDump, Wireshark, and a number of other packet capture programs.
- Import packets from text files containing hex dumps of packet data.
- Display packets with very detailed protocol information.

Uses of Wireshark:

Wireshark can be used in the following ways:

- It is used by network security engineers to examine security problems.
- It allows the users to watch all the traffic being passed over the network.
- It is used by network engineers to troubleshoot network issues.
- It also helps to troubleshoot latency issues and malicious activities on your network.
- It can also analyze dropped packets.
- 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.

Input:

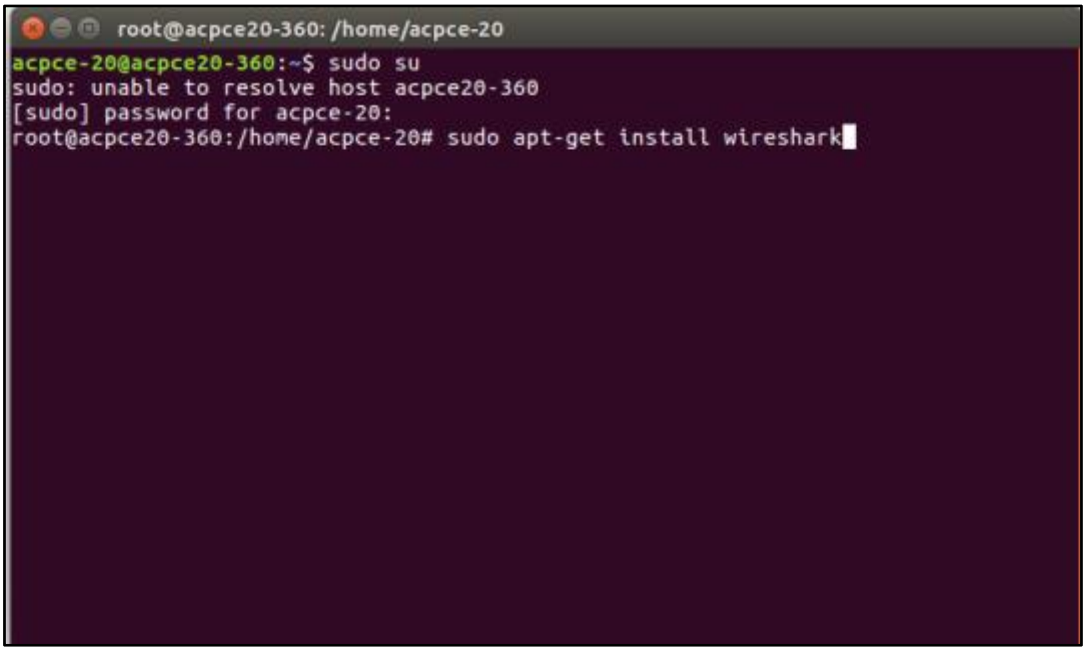
Using Command install Open Terminal(CTR+T)

acpce-20@acpce20-360:~$ sudo su

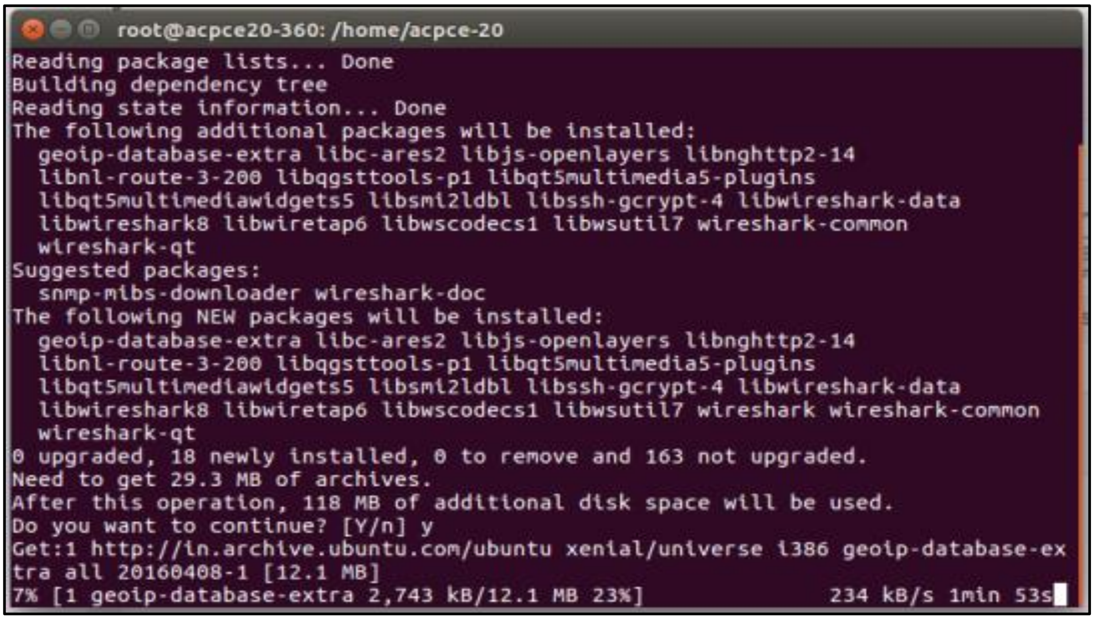
sudo: unable to resolve host acpce20-360

[sudo] password for acpce-20:

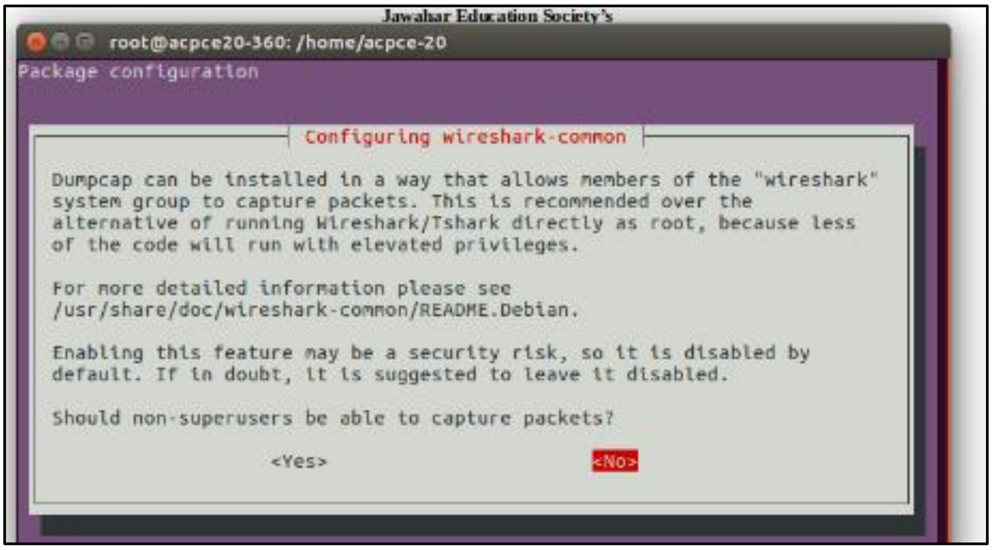
root@acpce20-360:/home/acpce-20# sudo apt-get install wireshark



```
acpce-20@acpce20-360:~$ sudo su
sudo: unable to resolve host acpce20-360
[sudo] password for acpce-20:
root@acpce20-360:/home/acpce-20# sudo apt-get install wireshark
```

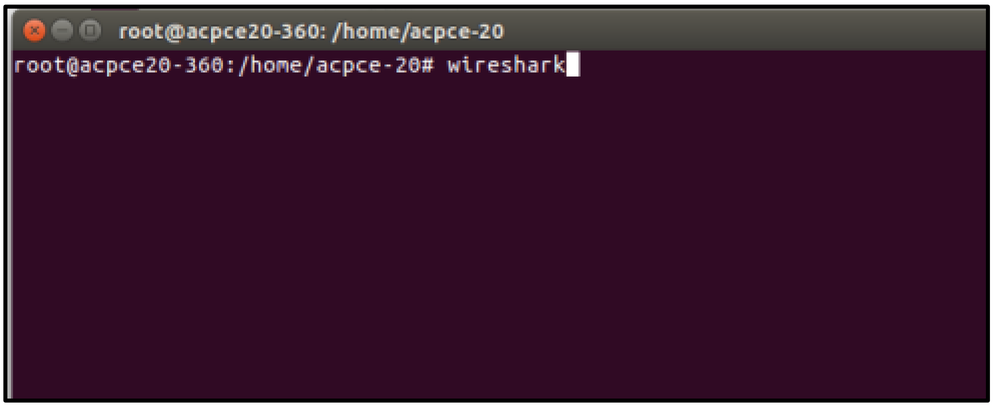


```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  geoip-database-extra libc-ares2 libjs-openlayers libnghttp2-14
  libnl-route-3-200 libqgsttools-p1 libqt5multimedia5-plugins
  libqt5multimediawidgets5 libsmi2ldbl libssh-gcrypt-4 libwireshark-data
  libwireshark8 libwiretap6 libwscodecs1 libwsutil7 wireshark-common
  wireshark-qt
Suggested packages:
  snmp-mibs-downloader wireshark-doc
The following NEW packages will be installed:
  geoip-database-extra libc-ares2 libjs-openlayers libnghttp2-14
  libnl-route-3-200 libqgsttools-p1 libqt5multimedia5-plugins
  libqt5multimediawidgets5 libsmi2ldbl libssh-gcrypt-4 libwireshark-data
  libwireshark8 libwiretap6 libwscodecs1 libwsutil7 wireshark wireshark-common
  wireshark-qt
0 upgraded, 18 newly installed, 0 to remove and 163 not upgraded.
Need to get 29.3 MB of archives.
After this operation, 118 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu xenial/universe i386 geoip-database-ex
tra all 20160408-1 [12.1 MB]
7% [1 geoip-database-extra 2,743 kB/12.1 MB 23%]              234 kB/s 1min 53s
```



Jawahar Education Society's

```
Package configuration

┤ Configuring wireshark-common ├

Dumpcap can be installed in a way that allows members of the "wireshark"
system group to capture packets. This is recommended over the
alternative of running Wireshark/Tshark directly as root, because less
of the code will run with elevated privileges.

For more detailed information please see
/usr/share/doc/wireshark-common/README.Debian.

Enabling this feature may be a security risk, so it is disabled by
default. If in doubt, it is suggested to leave it disabled.

Should non-superusers be able to capture packets?

              <Yes>                              <No>
```



```
root@acpce20-360:/home/acpce-20# wireshark
```

- **Conclusion**: Thus, we have studied about, **Installation** and **configuration** of Wire shark.