

EXPERIMENT NO: 10

ANALYZING NETWORK PACKET STREAM USING WIRESHARK

Wireshark is one of the best network protocols for analyzing freely available packages. Previously known as Ethereal, Wireshark is widely used by industries and educational institutes.

Features

Wireshark contains several useful features, the foremost of which are listed below:

- Inspecting thousands of protocols
- New protocols being added with every update
- Live-capturing of protocols with offline analysis
- Three-way handshake

Step 1: Update APT

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

```
$ sudo apt update
```

```
$ sudo apt upgrade
```

Step 2: Download and Install Wireshark

.

```
$ sudo apt install wireshark
```

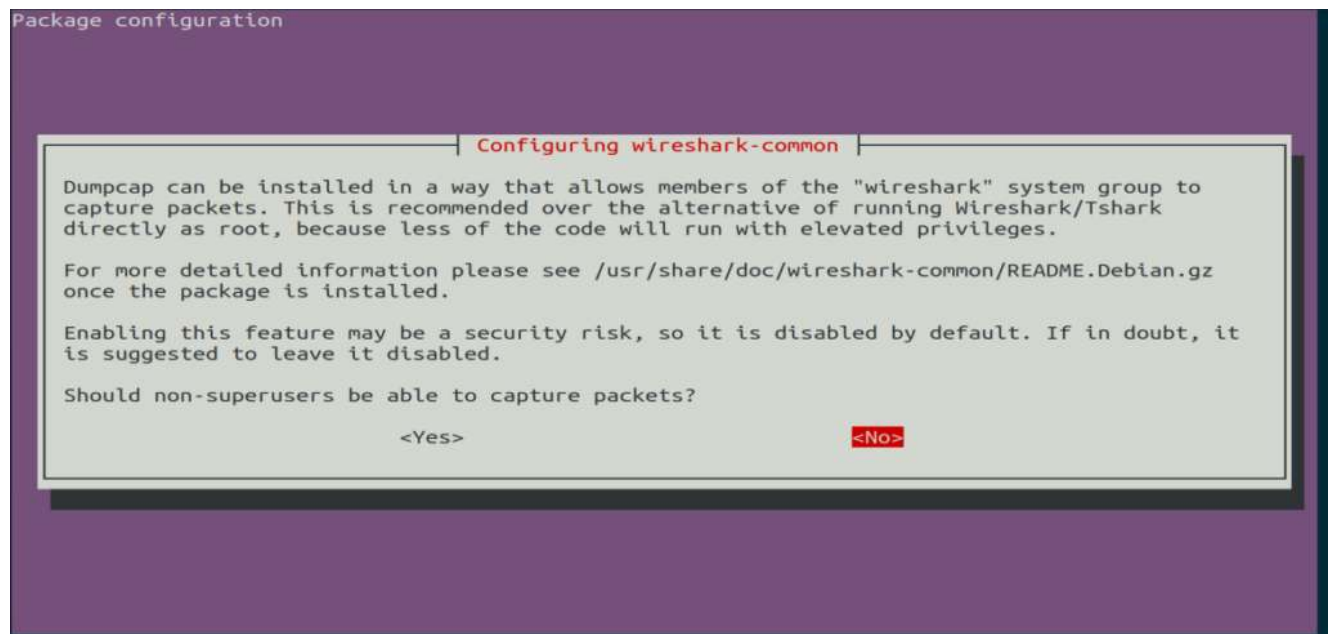
```

younis@younis-VirtualBox:~$ sudo apt install wireshark
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libc-ares2 libdouble-conversion3 liblua5.2-0 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5 libqt5multimedialwidgets5
  libqt5network5 libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl
  libspandsp2 libwireshark-data libwireshark13 libwiretap10 libwsutil11 libxcb-xinerama0
  libxcb-xinput0 qt5-gtk-platformtheme qttranslations5-l10n wireshark-common wireshark-qt
Suggested packages:
  qt5-image-formats-plugins qtwayland5 snmp-mibs-downloader geotagupdate geotag-database
  geotag-database-extra libjs-leaflet libjs-leaflet.markercluster wireshark-doc
The following NEW packages will be installed:
  libc-ares2 libdouble-conversion3 liblua5.2-0 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5 libqt5multimedialwidgets5
  libqt5network5 libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl
  libspandsp2 libwireshark-data libwireshark13 libwiretap10 libwsutil11 libxcb-xinerama0
  libxcb-xinput0 qt5-gtk-platformtheme qttranslations5-l10n wireshark wireshark-common wireshark-qt
0 upgraded, 29 newly installed, 0 to remove and 0 not upgraded.
Need to get 32.7 MB of archives.
After this operation, 163 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu focal/universe amd64 libdouble-conversion3 amd64 3.1.5-4ubuntu
1 [37.9 kB]
Get:2 http://archive.ubuntu.com/ubuntu focal/main amd64 libpcre2-16-0 amd64 10.34-7 [181 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal/universe amd64 libqt5core5a amd64 5.12.8+dfsg-0ubuntu1 [
2,005 kB]
5% [3 libqt5core5a 1,309 kB/2,005 kB 65%]

```

Step 3: Enable Root Privileges

When Wireshark installs on your system, you will be prompted by the following window. As Wireshark requires super user/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.

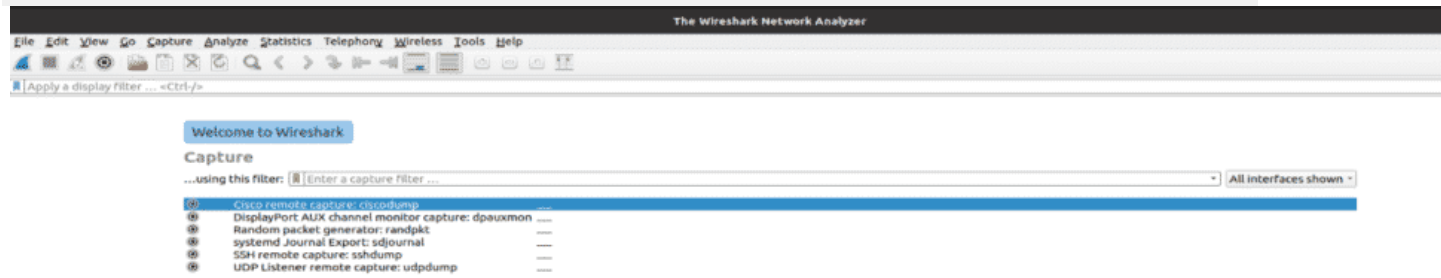
```
$ sudo dpkg-reconfigure wireshark-common
```

```
younis@younis-VirtualBox:~$ sudo dpkg-reconfigure wireshark-common  
[sudo] password for younis:
```

Select the “Yes” button to change the configuration settings to allow other users access to Wireshark.

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

\$ wireshark



RESULT

Study about analyzing network packet stream using Wireshark