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.

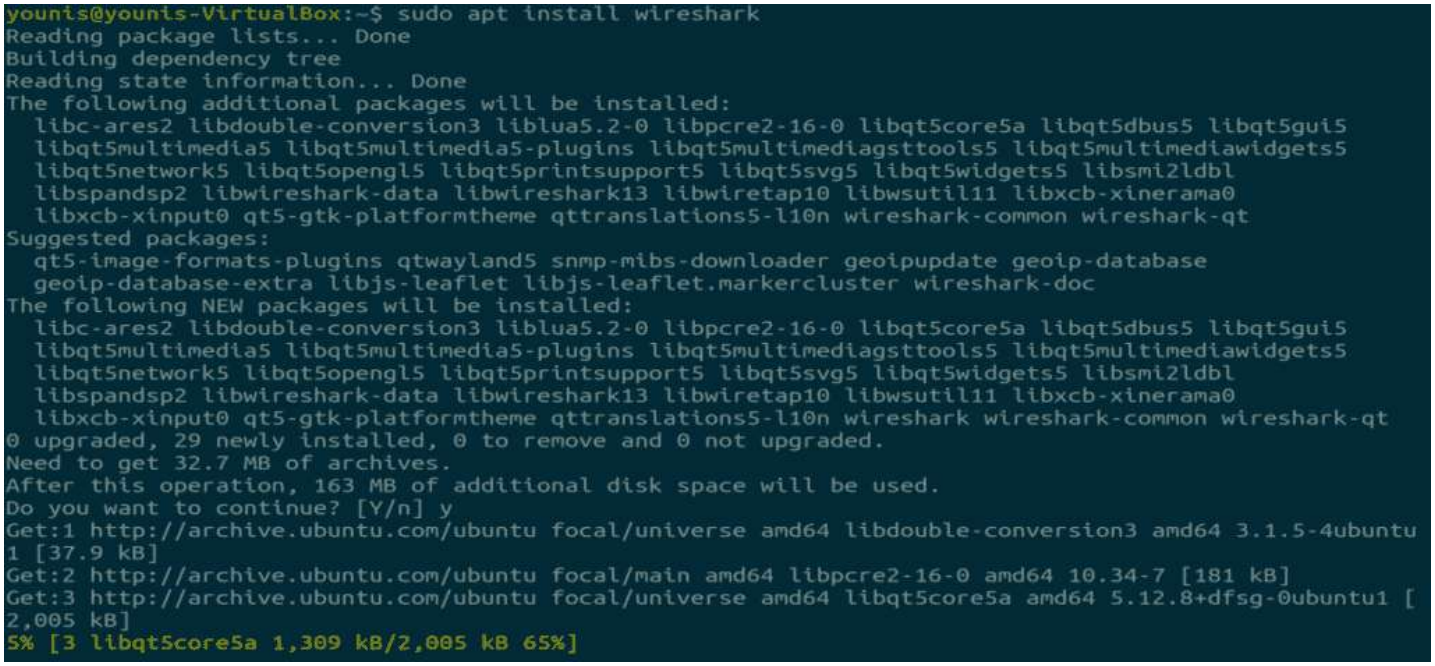
```
$ sudo apt update
```

```
$ sudo apt upgrade
```

Step 2: Download and Install Wireshark

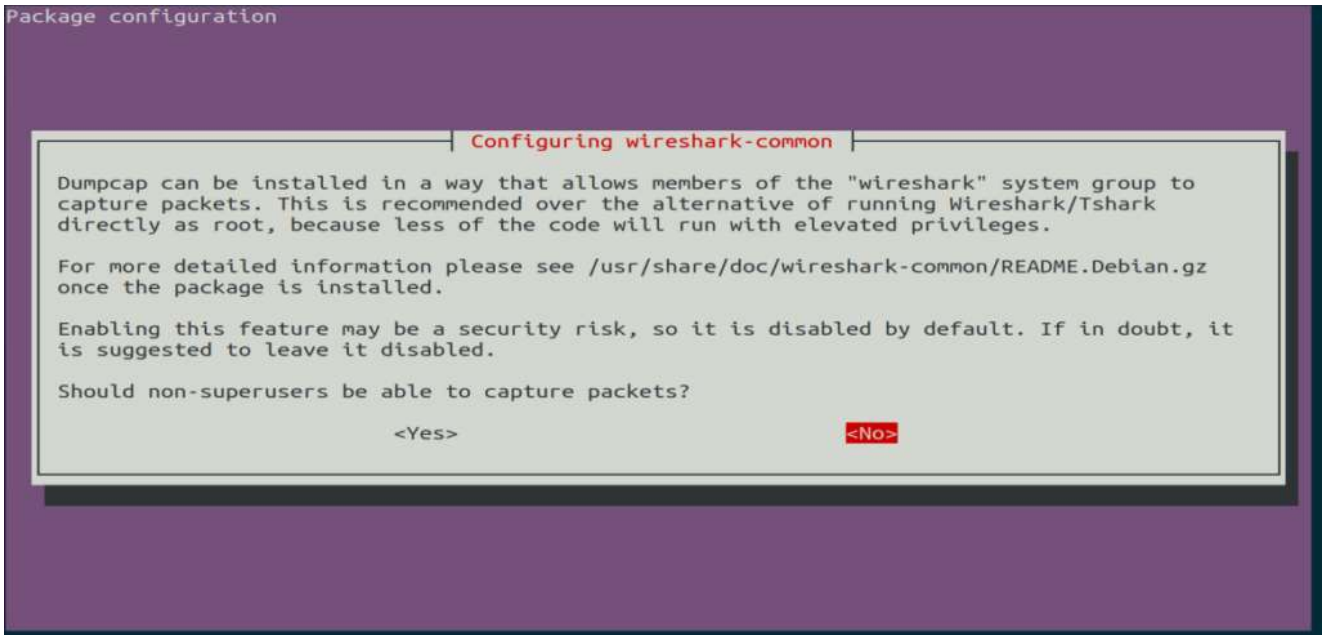
.

```
$ sudo apt install wireshark
```



Step 3: Enable Root Privileges

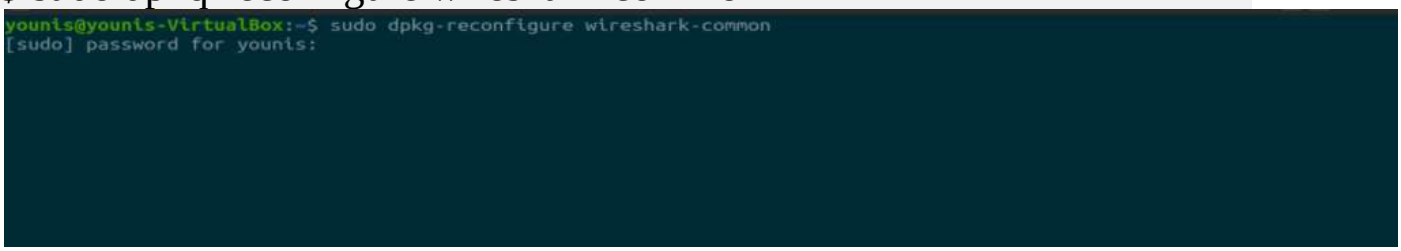
When Wireshark installs on your system, you will be prompted by the following window. As Wireshark requires super user/root privileges to operate, this option asks to enable or disable permissions for all every user on the system. Press the “Yes” button to allow other users, or press the “No” button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

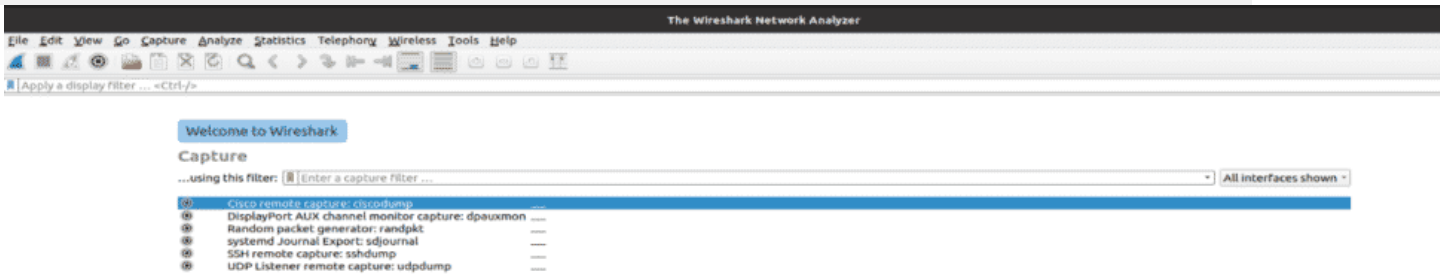
```
$ sudo dpkq-reconfigure wireshark-common
```



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