Lab Report No: 02

Lab Report Name: How to install and use Wireshark in Linux operating system.

Name:Tahmina Afroze

ID: IT-17014

INSTALLING WIRESHARK:

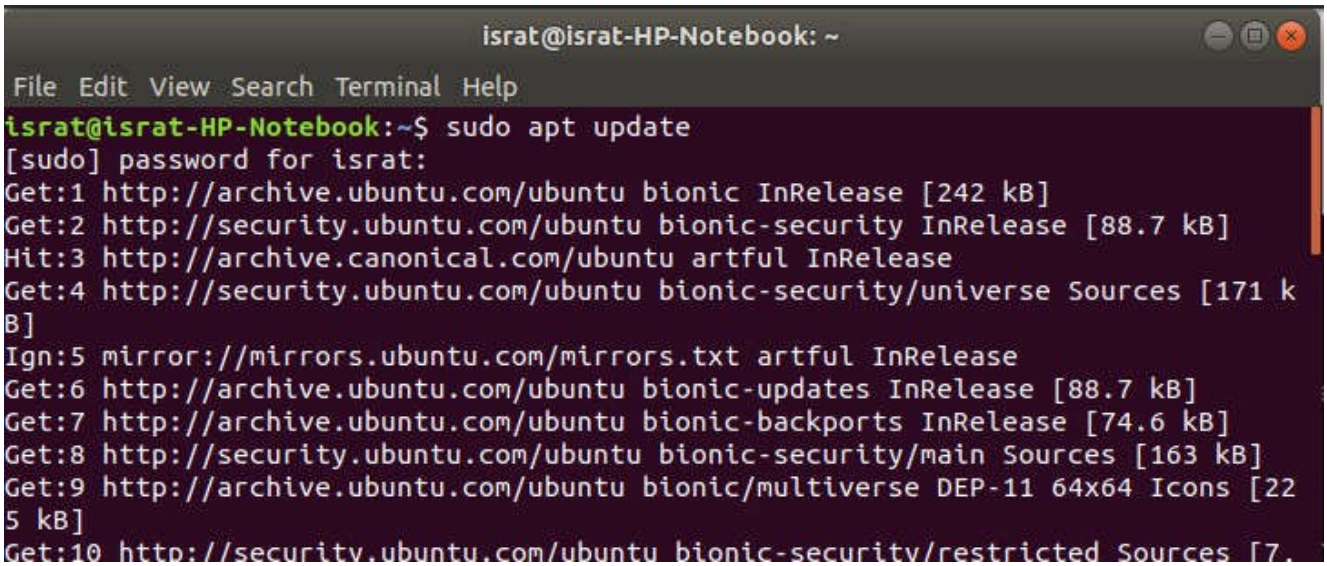
Wireshark is a network packet analyzer. It captures every packet getting in or out of a network interface and shows them in a nicely formatted text. It is used by Network Engineers all over the world. Wireshark is cross platform and it is available for Linux, Windows and Mac OS. You get the same user experience in any operating system you use.

.

How to install Wireshark is given below step by step:

First update the APT package repository cache with the following command:

$ sudo apt update



The APT package repository cache should be updated.

Now, Run the following command to install Wireshark on your Ubuntu machine:

$ sudo apt get install wireshark

```
israt@israt-HP-Notebook: ~
File  Edit  View  Search  Terminal  Help
israt@israt-HP-Notebook:~$ sudo apt-get install wireshark
[sudo] password for israt:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  fontconfig-config libc-ares2 libdouble-conversion1 libegl-mesa0 libegl1
  libegl1-mesa libfontconfig1 libgbm1 libglvnd0 libicu60 liblua5.2-0
  libmaxminddb0 libnl-route-3-200 libqgsttools-p1 libqt5core5a libqt5dbus5
  libqt5gui5 libqt5multimedia5 libqt5multimedia5-plugins
  libqt5multimediawidgets5 libqt5network5 libqt5opengl5 libqt5printsupport5
  libqt5svg5 libqt5widgets5 libsmi2ldbl libsnappy1v5 libspandsp2
  libssh-gcrypt-4 libwayland-egl1-mesa libwireshark-data libwireshark11
  libwiretap8 libwscodecs2 libwsutil9 libxcb-xinerama0 qt5-gtk-platformtheme
```

Now press y and then press <Enter>.

```
The following NEW packages will be installed:
  geoip-database-extra javascript-common libc-ares2 libdouble-conversion1 libjs-openlayers
  liblua5.2-0 libnl-route-3-200 libqt5core5a libqt5dbus5 libqt5gui5 libqt5multimedia5
  libqt5network5 libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl libsnappy1v5
  libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark10 libwiretap7 libwscodecs1 libwsutil8
  libxcb-xinerama0 qt5-gtk-platformtheme qttranslations5-l10n wireshark wireshark-common
  wireshark-qt
0 upgraded, 30 newly installed, 0 to remove and 325 not upgraded.
Need to get 41.0 MB of archives.
After this operation, 181 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Wireshark should be installed.

Run the following command to add your user to the **Wireshark** group:

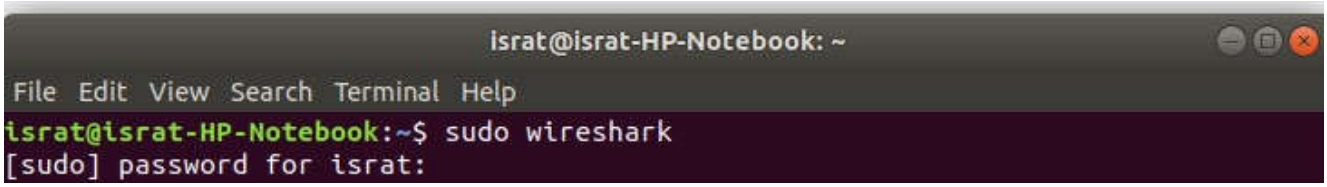
$ sudo usermod -aG wireshark $(whoami)

Now reboot your computer with the following command:

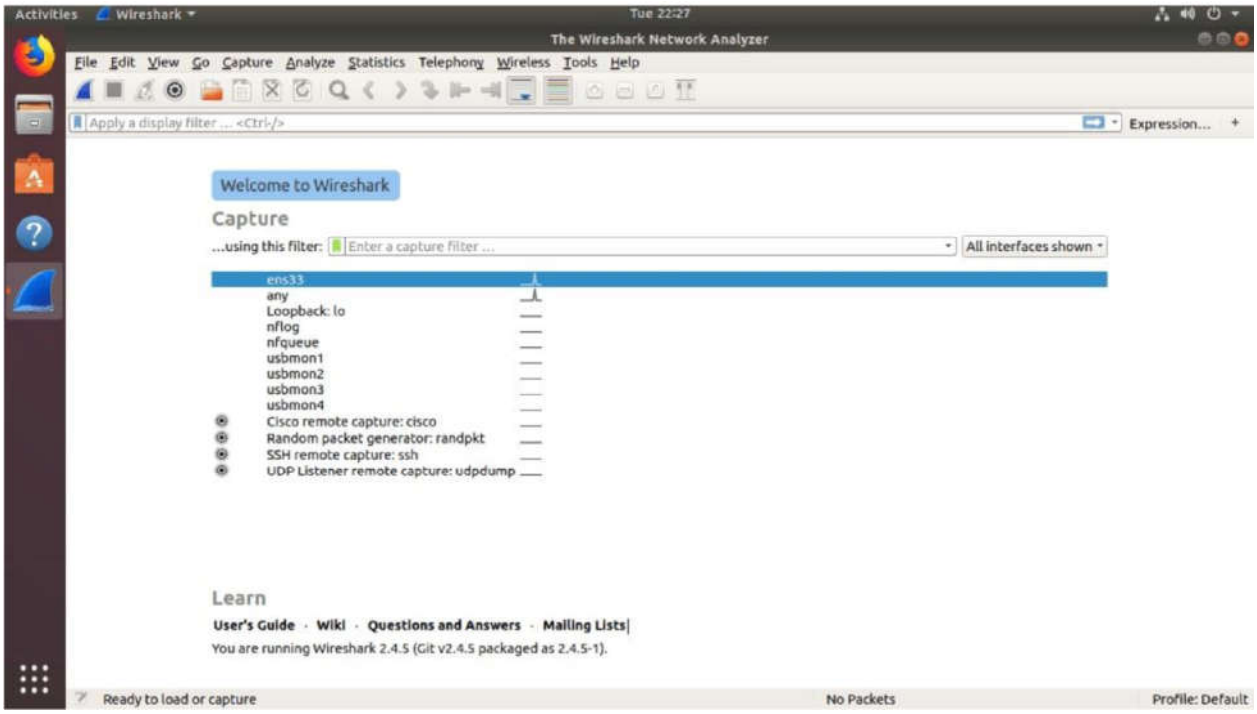
$ sudo reboot

Now run Wireshark using the following command:

$ sudo wireshark

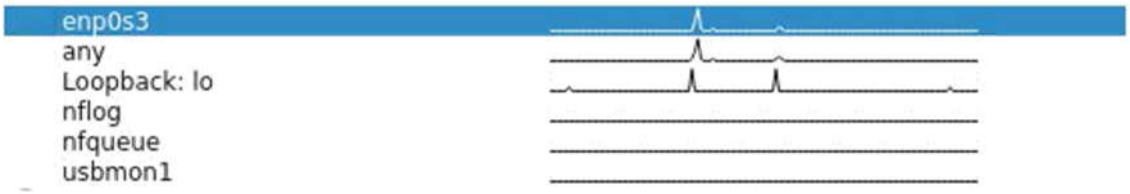


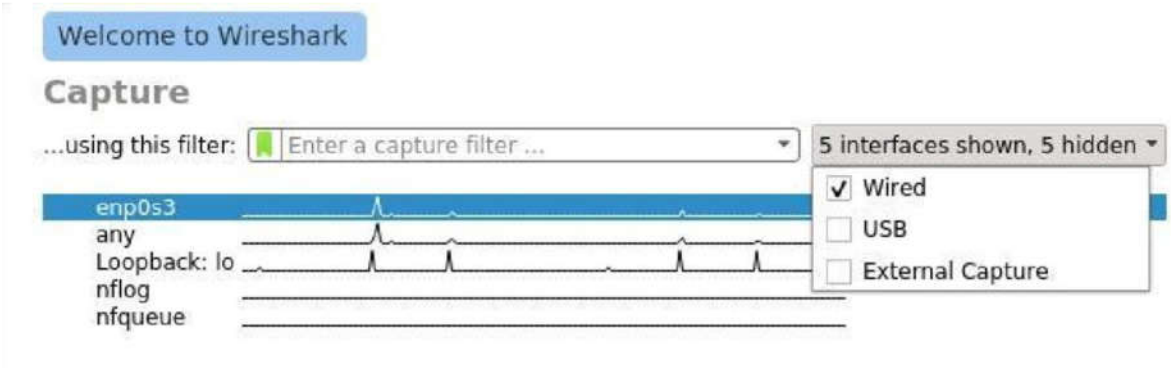
Wireshark will start in your computer



Now we will capture packages using Wireshark.

When you start Wireshark, you will see a list of interfaces that you can capture packets to and from.



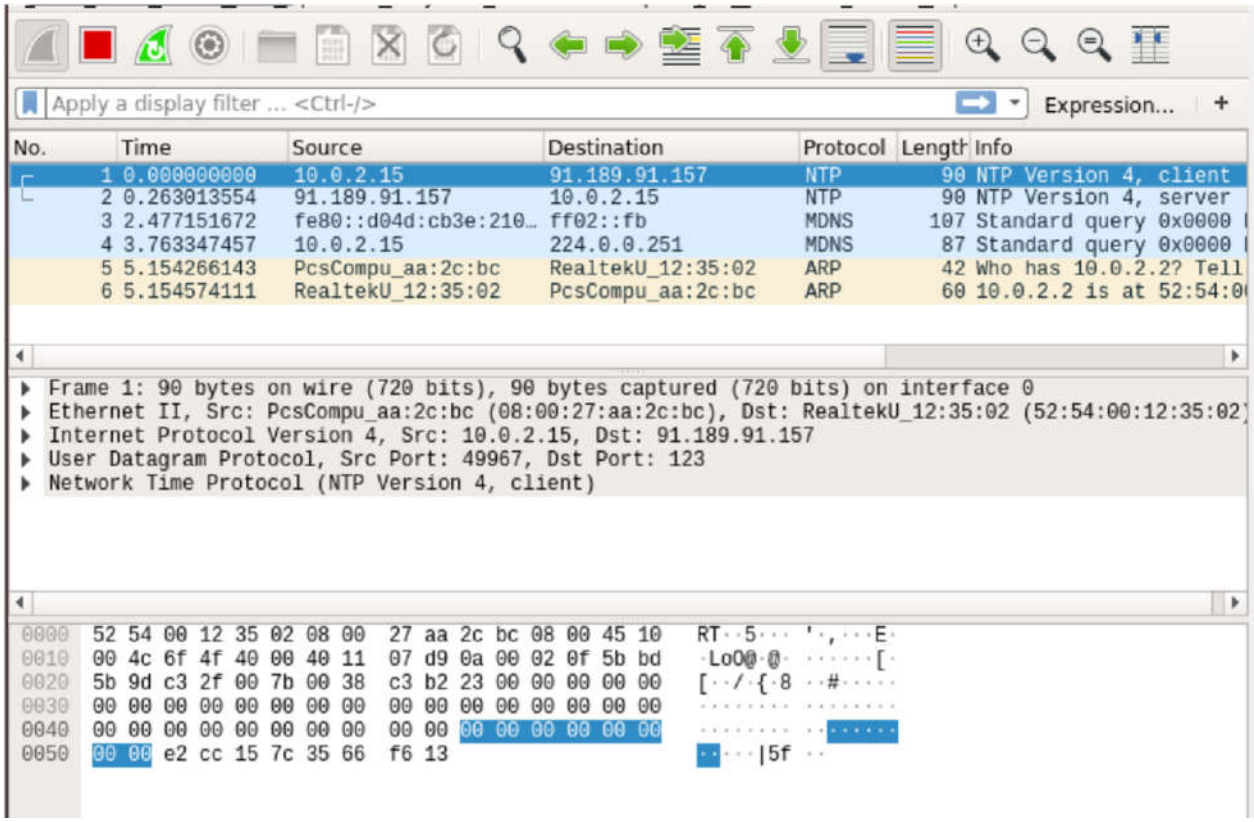


There are many types of interfaces you can monitor using Wireshark, for example, **Wired**, **Wireless**, USB and many external devices. You can choose to show specific types of interfaces in the welcome screen from the marked section of the screenshot below

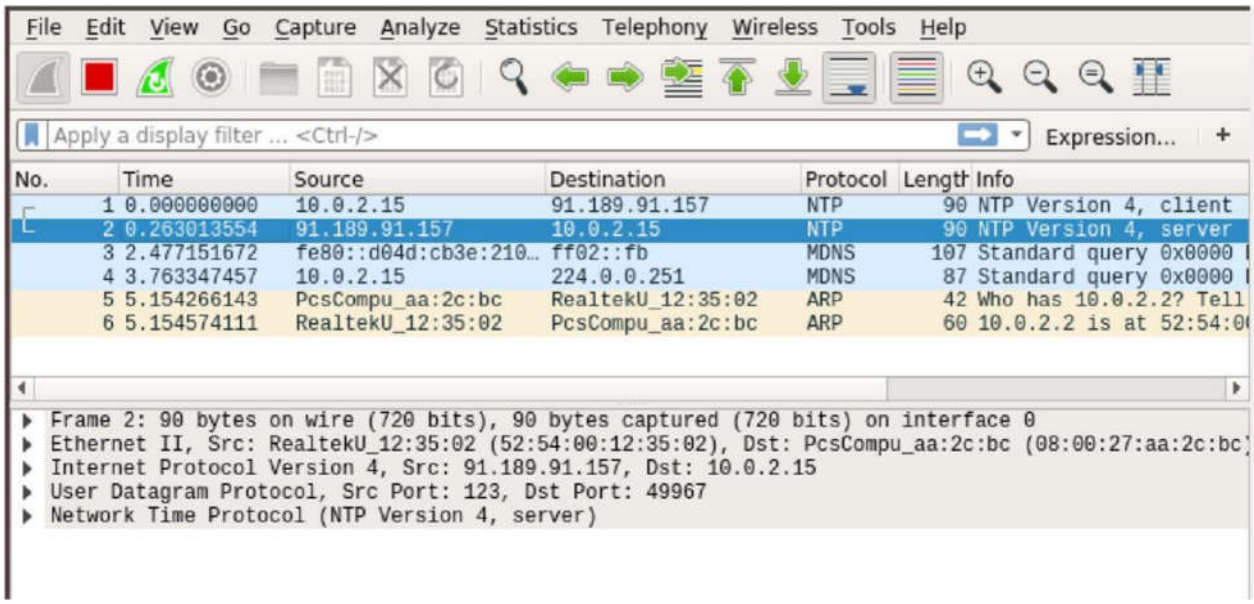
Now to start capturing packets, just select the interface (in my case interface **ens33**) and click on the **Start capturing packets** icon as marked in the screenshot below.

You can also capture packets to and from multiple interfaces at the same time. Just press and hold **<Ctrl>** and click on the interfaces that you want to capture packets to and from and then click on the **Start capturing packets** icon as marked in the screenshot below.

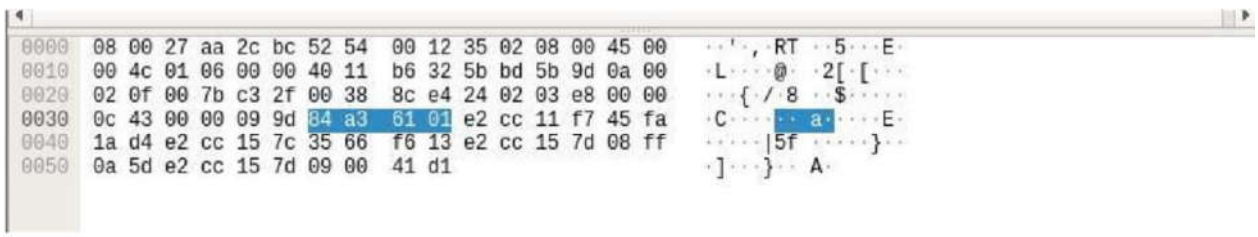
I pinged google.com from the terminal and many packets were captured.



Now you can click on a packet to select it. Selecting a packet would show many information about that packet. As you can see, information about different layers of TCP/IP Protocol is listed.

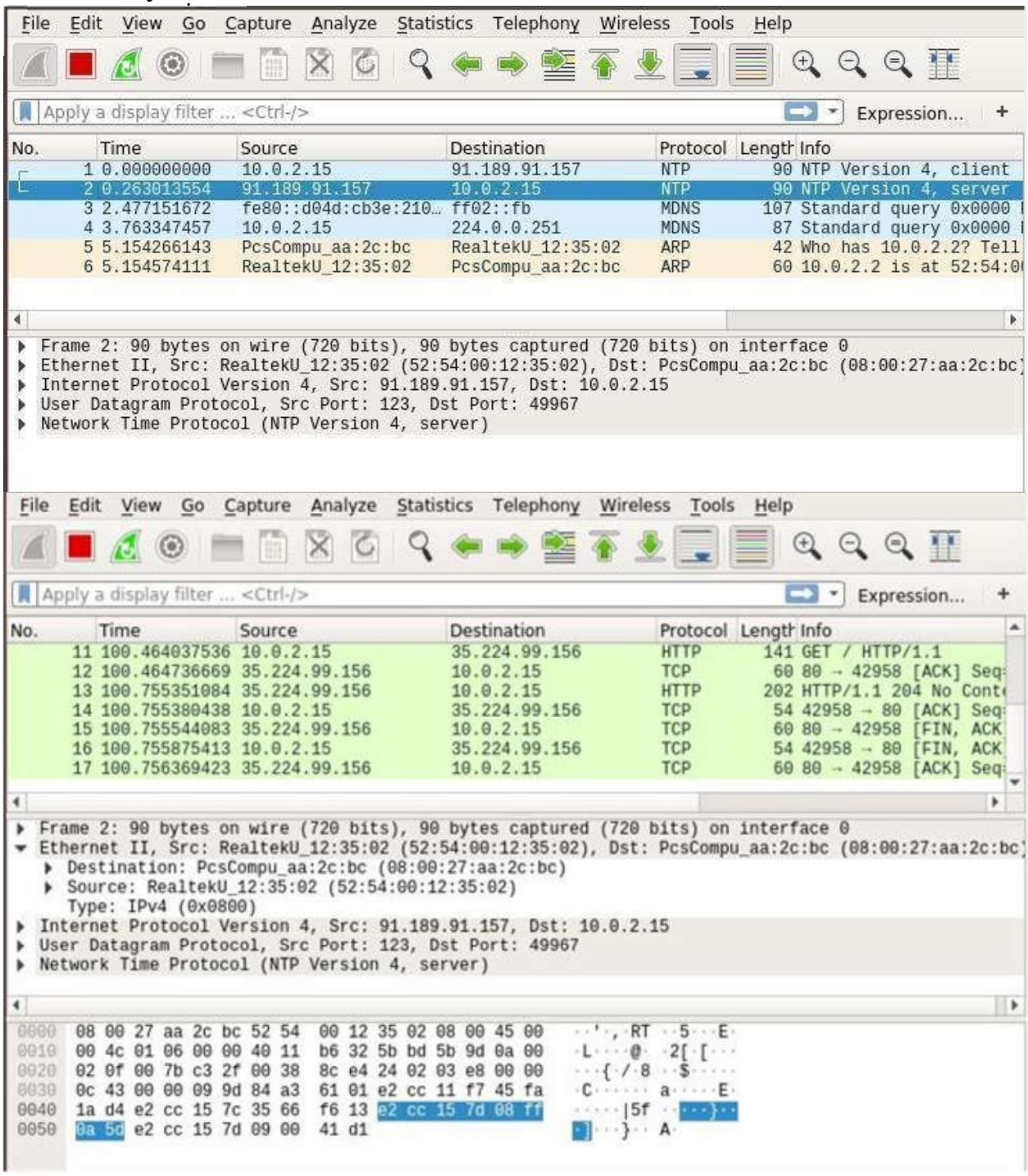


You can also see the RAW data of that particular packet.

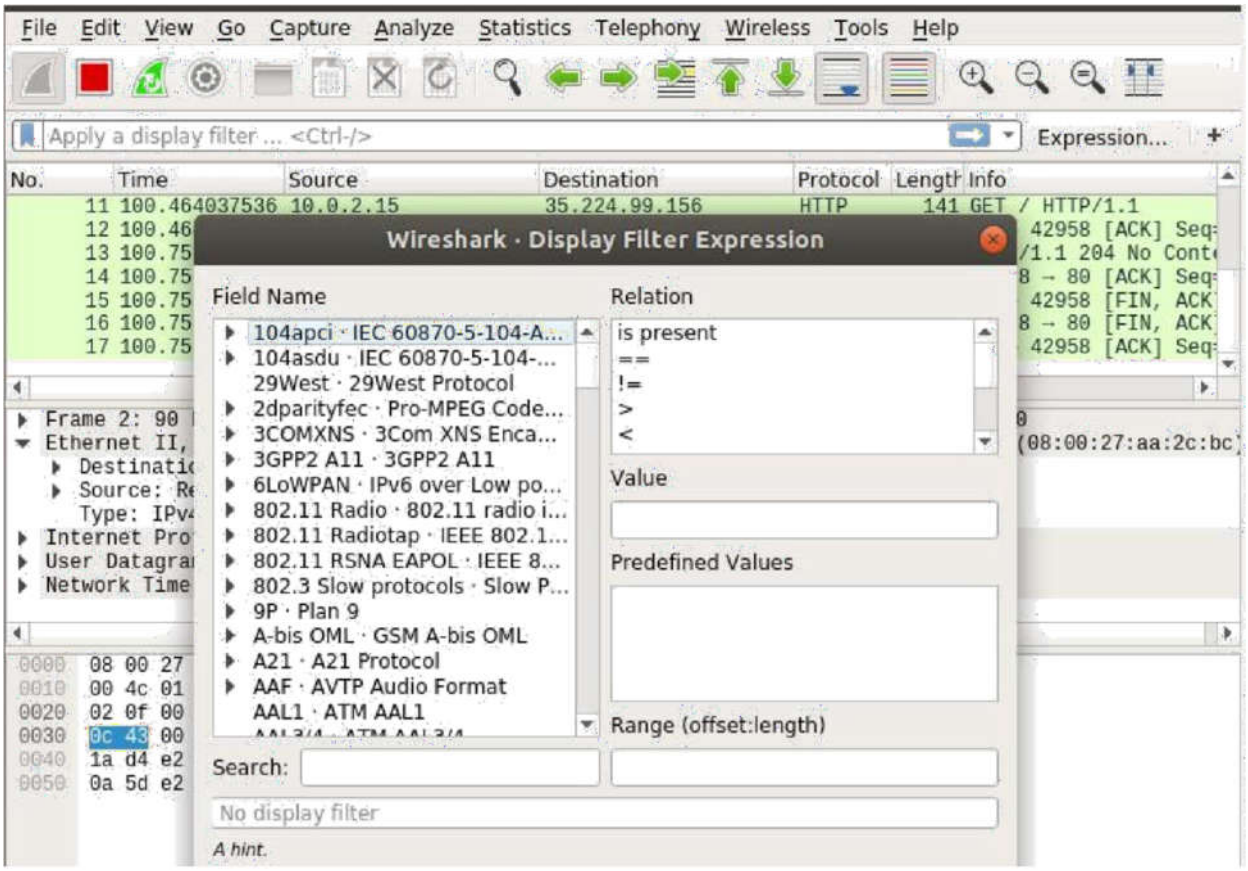


You can also click on the arrows to expand packet data for a particular TCP/IP

Protocol Layer



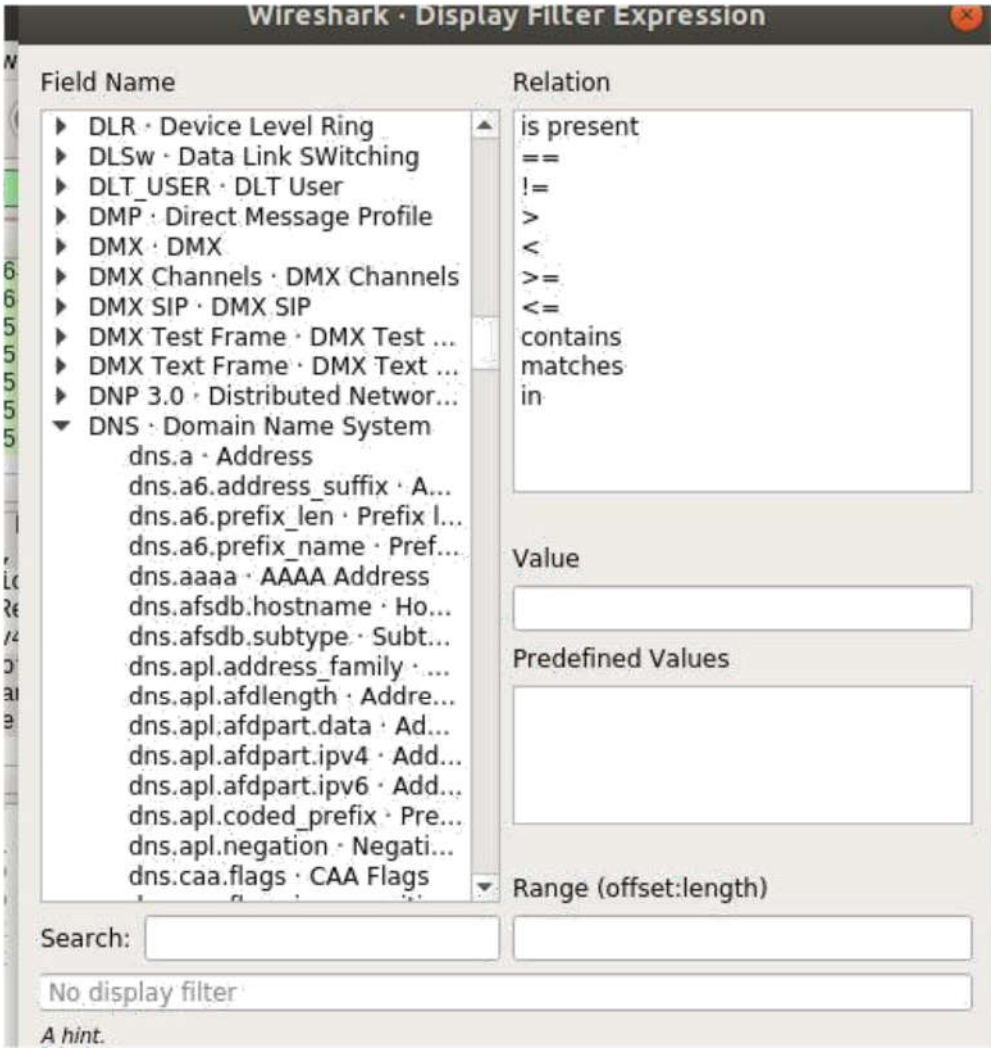
To filter packets, you can directly type in the filter expression in the textbox as marked in the screenshot below.



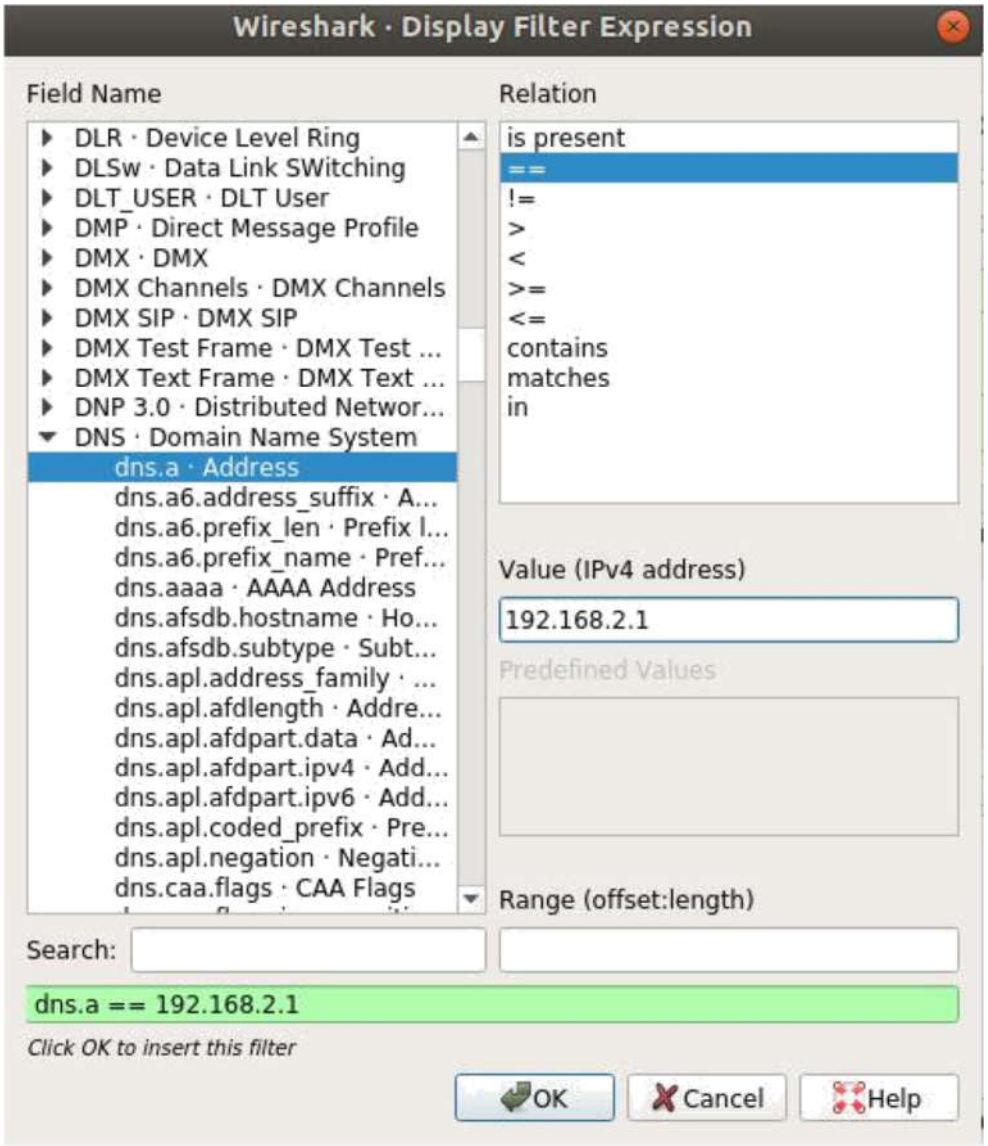
A new window should open as shown in the screenshot below. From here you can create filter expression to search packets very specifically.

In the Field Name section almost all the networking protocols are listed. The list is huge. You can type in what protocol you're looking for in the Search textbox and the Field Name section would show the ones that matched.

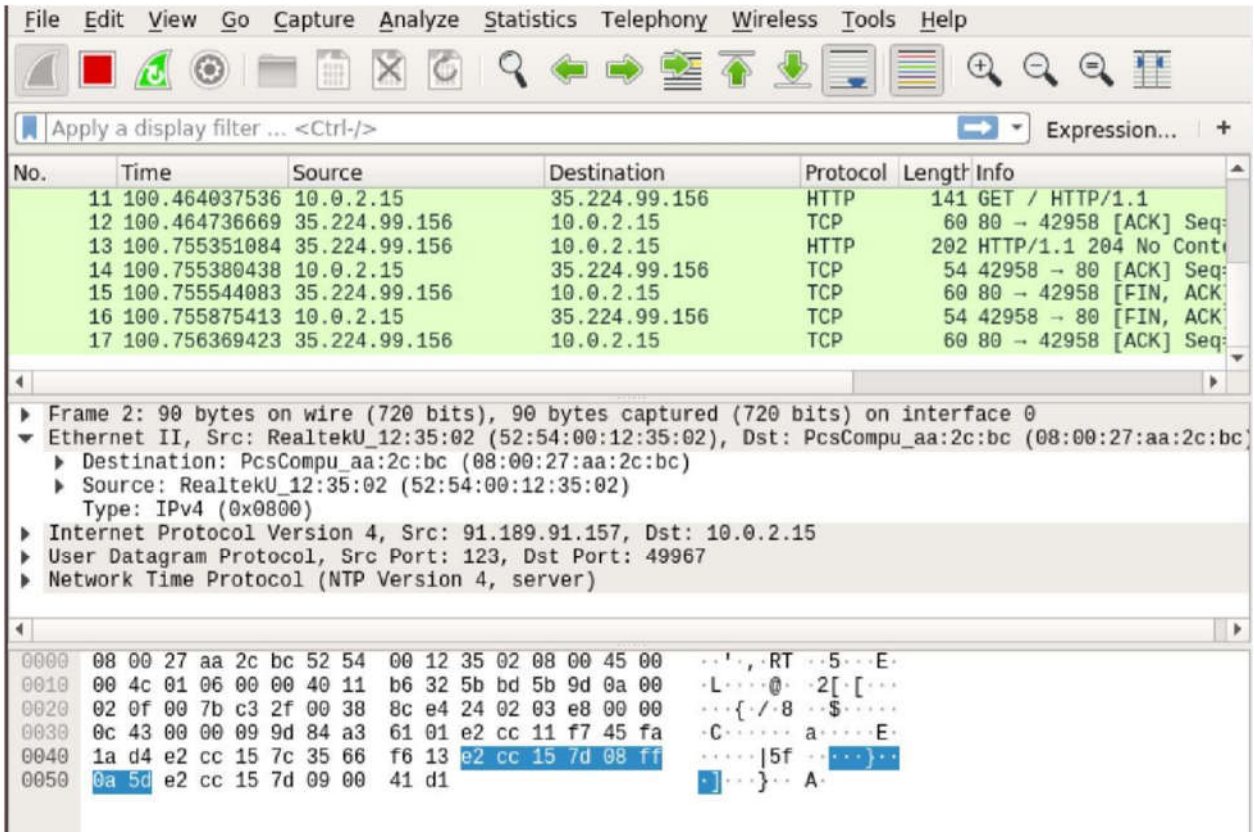
I am going to filter out all the DNS packets. So I selected **DNS Domain Name System** from the **Field Name** list. You can also click on the **arrow** on any protocol.



You can also use relational operators to test whether some field is equal to, not equal to, great than or less than some value. I searched for all the DNS IPv4 address which is equal to 192.168.2.1 as you can see in the screenshot below.



As you can see, only the DNS protocol packets are shown

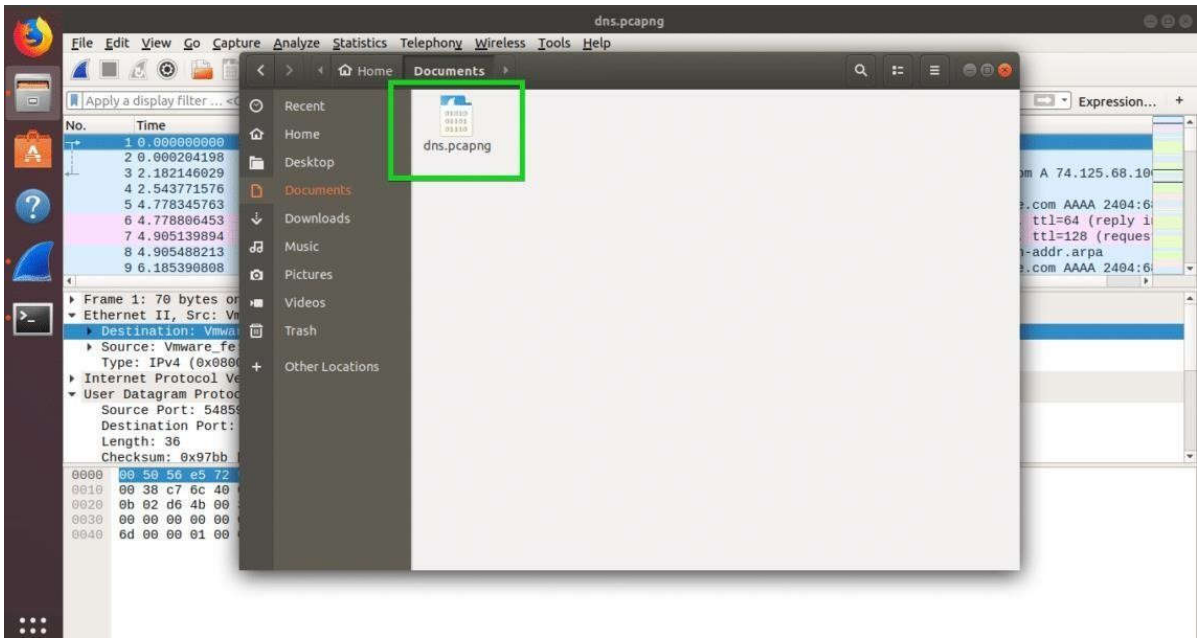


You can click on the red icon as red marked to stop capturing Wireshark packets.

You can click on the saved marked icon to save captured packets to a file for future use.

Now select a destination folder, type in the file name i.e “dns” and click on **Save**.

The file should be saved



Conclusion:This lab is about install and use wireshark in linux operating system.Wireshark is a popular open source graphical user interface(GUI) tool for analyzing packets.However it also provides a powerful command line utility called Tshark for people who prefer to work on the linux command line.