

Lab Report No: 02

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

Name: Md. Moniruzzaman

ID: IT-17006

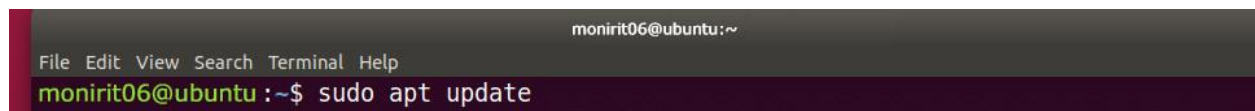
INSTALLING WIRESHARK:

It is a popular network analysis tool to capture network packets and display them at a granular level. Once these packets are broken down, we can use them for real-time or offline analysis. 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.

How to install Wireshark is given below step by step:

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

`$ sudo apt update`

A screenshot of a terminal window with a dark background. The title bar at the top reads 'monirit06@ubuntu:~'. Below the title bar is a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The main area of the terminal shows the prompt 'monirit06@ubuntu :~\$' followed by the 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`

A screenshot of a terminal window with a dark background. The title bar at the top reads 'monirit06@ubuntu:~'. Below the title bar is a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The main area of the terminal shows the prompt 'monirit06@ubuntu :~\$' followed by the command 'sudo apt-get install wireshark'.

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:

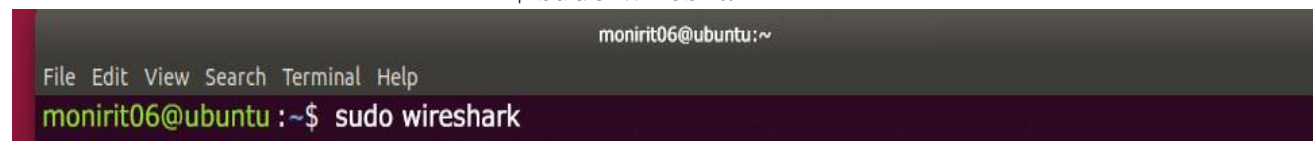
```
$ sudo usermod -aG wireshark $(whoami)
```

Now reboot your computer with the following command:

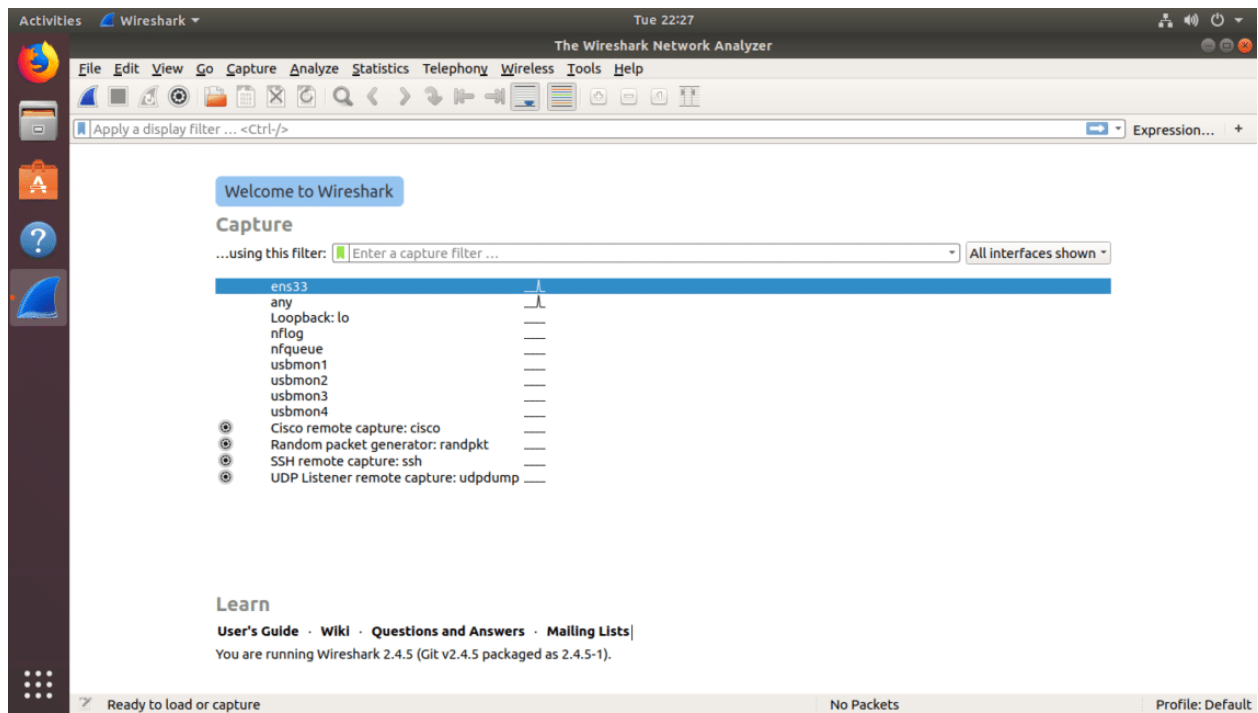
```
$ sudo reboot
```

Now run Wireshark using the following command:

```
$ sudo wireshark
```



Wireshark will start in your computer

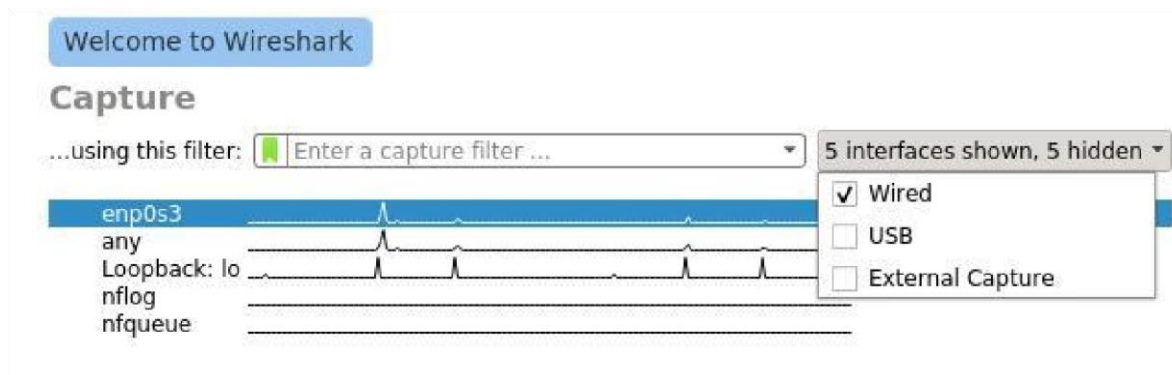


Now we will capture packages using Wireshark.

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



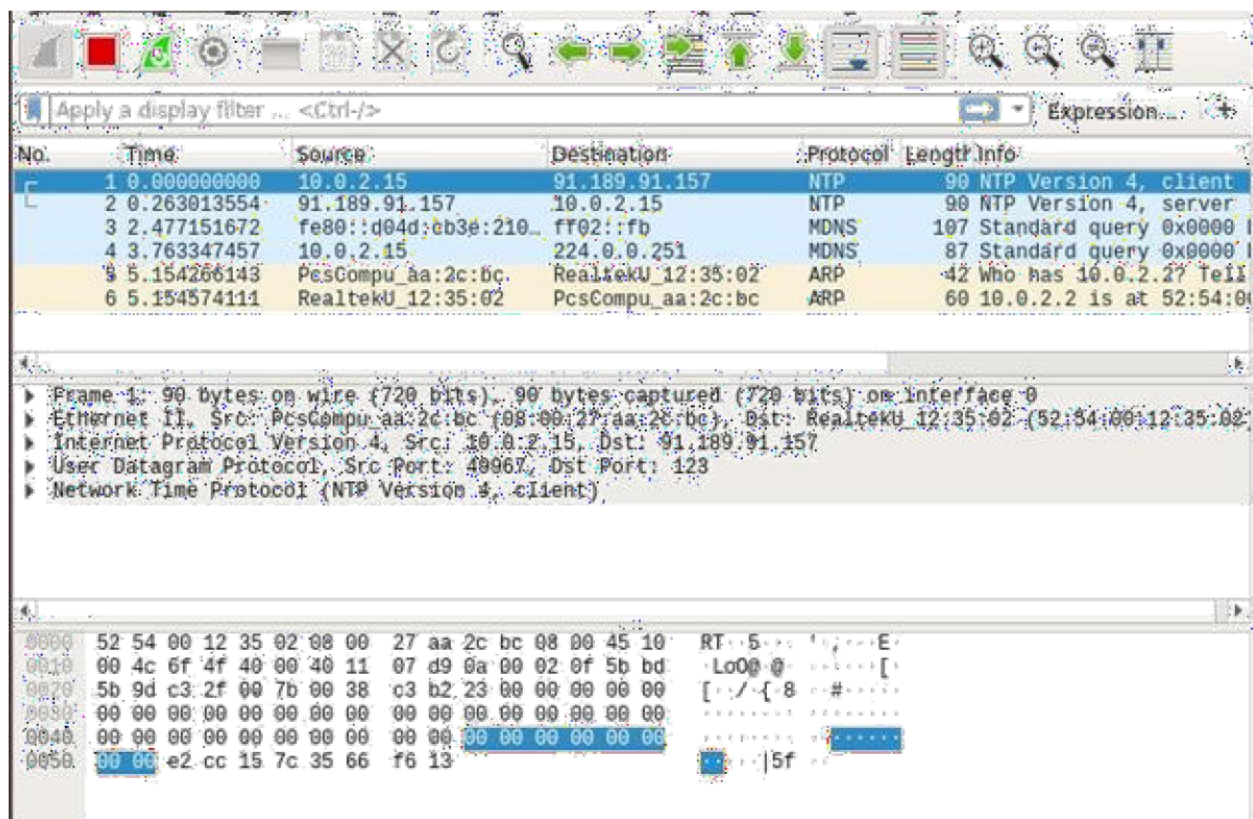
There are many types of interfaces you can monitor using Wireshark, for example, **Wired**, **Wireless**, USB and many external devices. You can choose to show specific types of interfaces in the welcome screen from the marked section of the screenshot below



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.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/> Expression... +						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	91.189.91.157	NTP	90	NTP Version 4, client
2	0.263013554	91.189.91.157	10.0.2.15	NTP	90	NTP Version 4, server
3	2.477151672	fe80::d04d:cb3e:210...	ff02::fb	MDNS	107	Standard query 0x0000 I
4	3.763347457	10.0.2.15	224.0.0.251	MDNS	87	Standard query 0x0000 I
5	5.154266143	PcsCompu_aa:2c:bc	RealtekU_12:35:02	ARP	42	Who has 10.0.2.2? Tell
6	5.154574111	RealtekU_12:35:02	PcsCompu_aa:2c:bc	ARP	60	10.0.2.2 is at 52:54:0

▶ Frame 2: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
▶ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_aa:2c:bc (08:00:27:aa:2c:bc)
▶ Internet Protocol Version 4, Src: 91.189.91.157, Dst: 10.0.2.15
▶ User Datagram Protocol, Src Port: 123, Dst Port: 49967
▶ Network Time Protocol (NTP Version 4, server)

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

0000	08 00 27 aa 2c bc 52 54 00 12 35 02 08 00 45 00	..',.RT..5...E..
0010	00 4c 01 06 00 00 40 11 b6 32 5b bd 5b 9d 0a 00	.L...@..2[...[...
0020	02 0f 00 7b c3 2f 00 38 8c e4 24 02 03 e8 00 00	...{/8...\$...[...
0030	0c 43 00 00 09 9d 84 a3 61 01 e2 cc 11 f7 45 fa	.C...a...E...[...
0040	1a d4 e2 cc 15 7c 35 66 f6 13 e2 cc 15 7d 08 ff	... 5f...}...[...
0050	0a 5d e2 cc 15 7d 09 00 41 d1	.]...}...A...

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

Protocol Layer.

The top screenshot shows a packet capture in Wireshark. The packet list table is as follows:

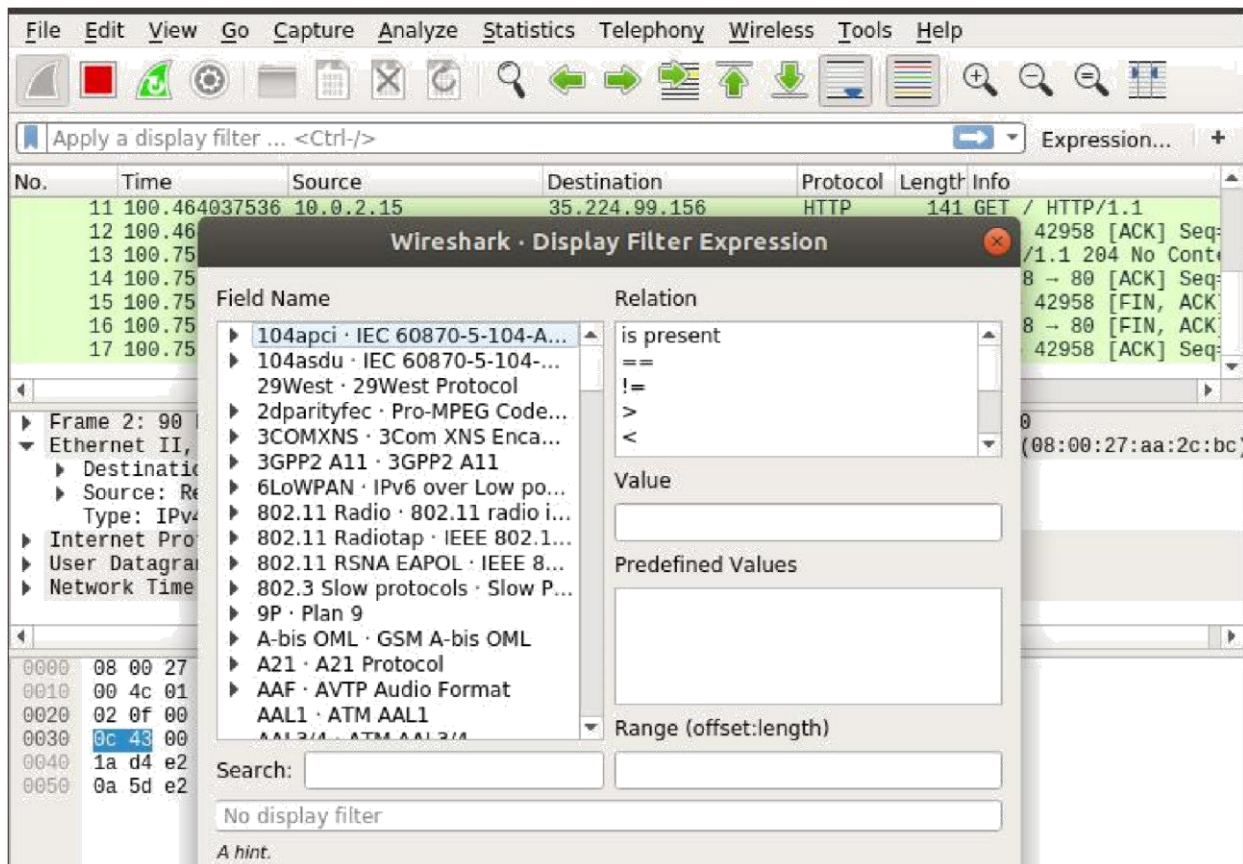
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	91.189.91.157	NTP	90	NTP Version 4, client
2	0.263013554	91.189.91.157	10.0.2.15	NTP	90	NTP Version 4, server
3	2.477151672	fe80::d04d:cb3e:210...	ff02::fb	MDNS	107	Standard query 0x0000
4	3.763347457	10.0.2.15	224.0.0.251	MDNS	87	Standard query 0x0000
5	5.154266143	PcsCompu_aa:2c:bc	RealtekU_12:35:02	ARP	42	Who has 10.0.2.2? Tell
6	5.154574111	RealtekU_12:35:02	PcsCompu_aa:2c:bc	ARP	60	10.0.2.2 is at 52:54:00

The bottom screenshot shows a detailed view of a packet (Frame 2). The packet details pane shows the following layers:

- Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_aa:2c:bc (08:00:27:aa:2c:bc)
- Internet Protocol Version 4, Src: 91.189.91.157, Dst: 10.0.2.15
- User Datagram Protocol, Src Port: 123, Dst Port: 49967
- Network Time Protocol (NTP Version 4, server)

The packet bytes pane shows the hex dump and ASCII representation of the packet data.

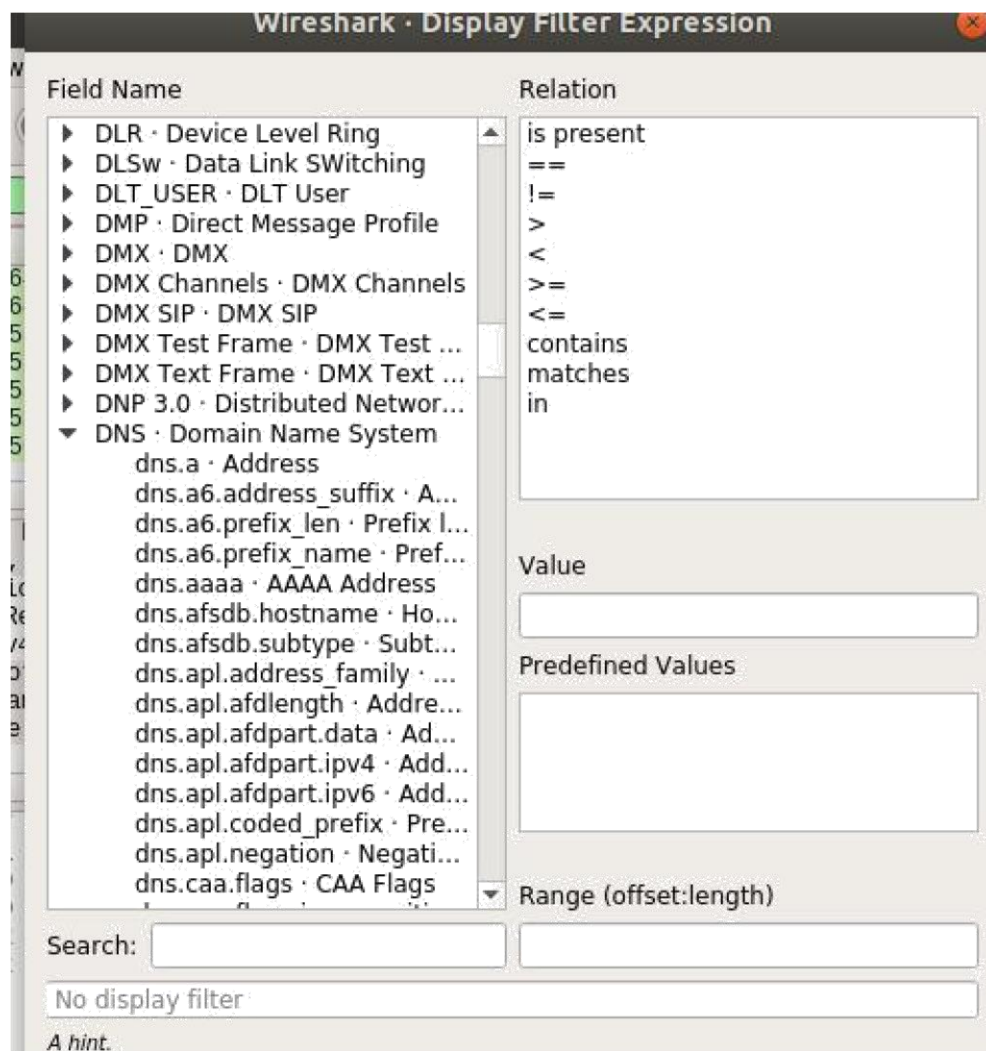
To filter packets, you can directly type in the filter expression in the textbox as marked in the screenshot below.



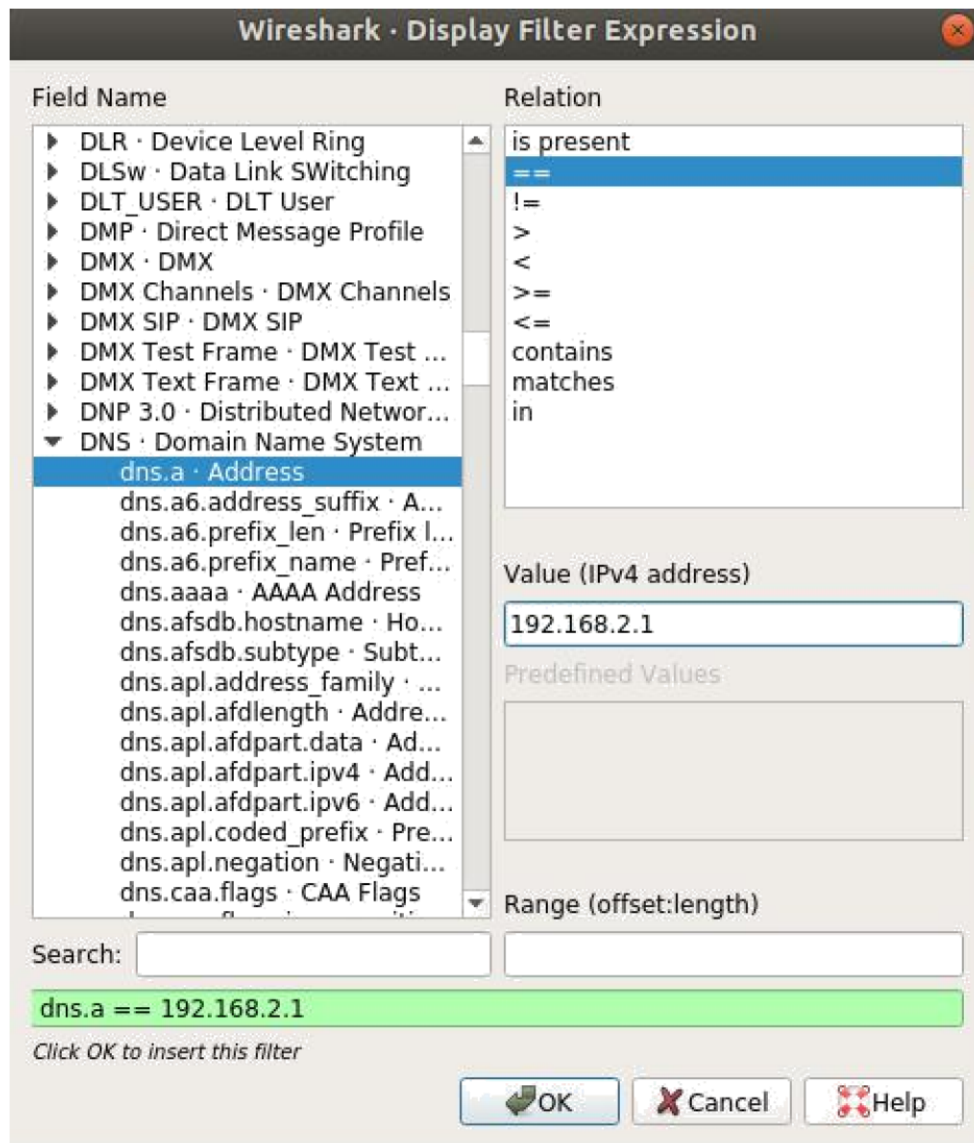
A new window should open as shown in the screenshot below. From here you can create filter expression to search packets very specifically.

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.

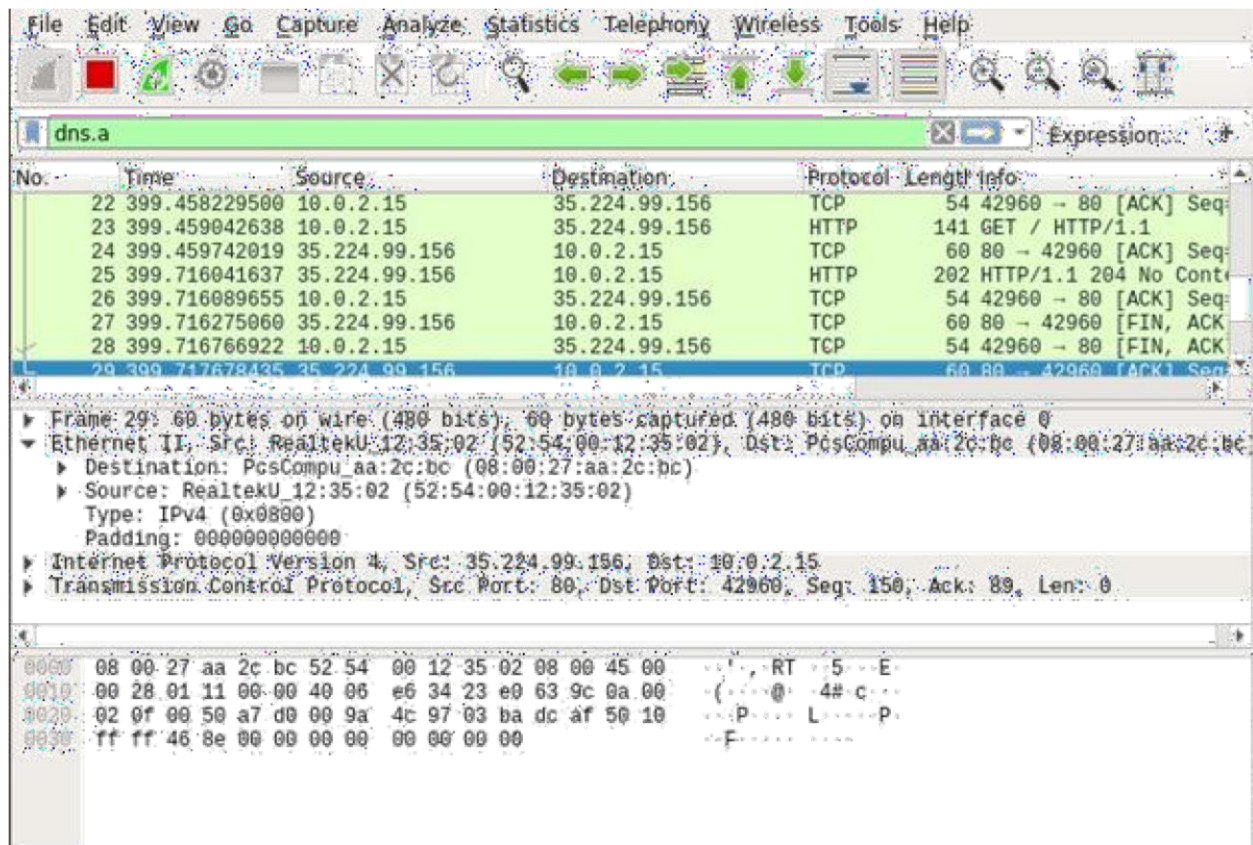
I am going to filter out all the DNS packets. So I selected **DNS Domain Name System** from the **Field Name** list. You can also click on the **arrow** on any protocol.



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

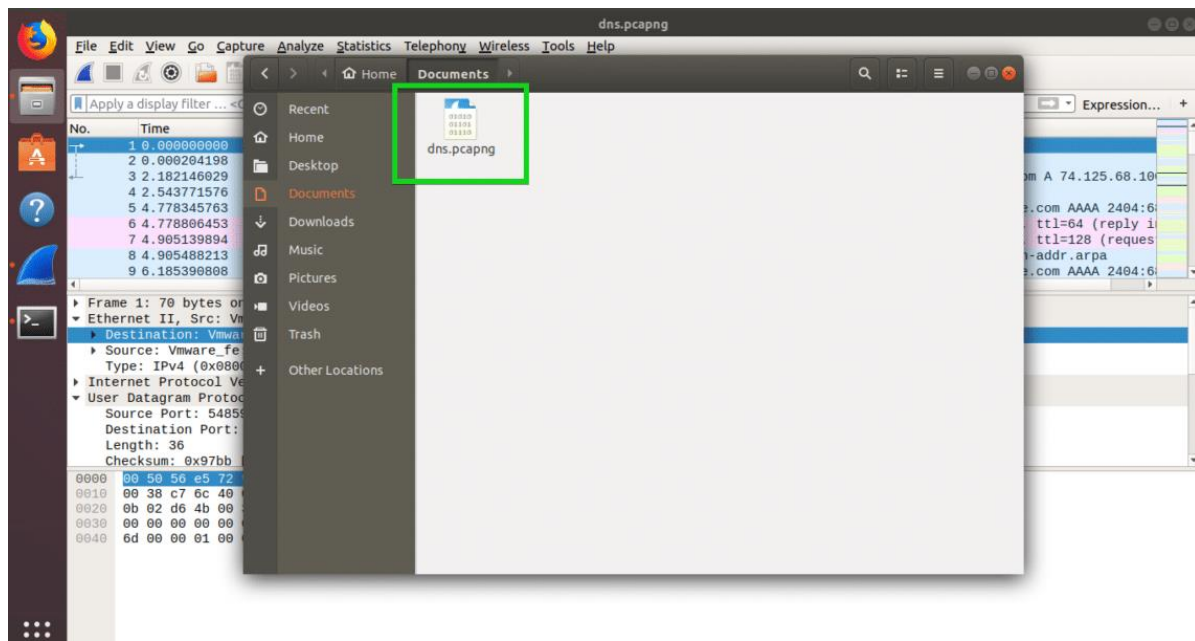


You can click on the red icon as red marked to stop capturing Wireshark packets.

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



That's how you install and use Wireshark in Linux.