

## Lab Report No: 02

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

**Name: Mahade Hasan**

**ID: IT-17040**

### INSTALLING WIRESHARK:

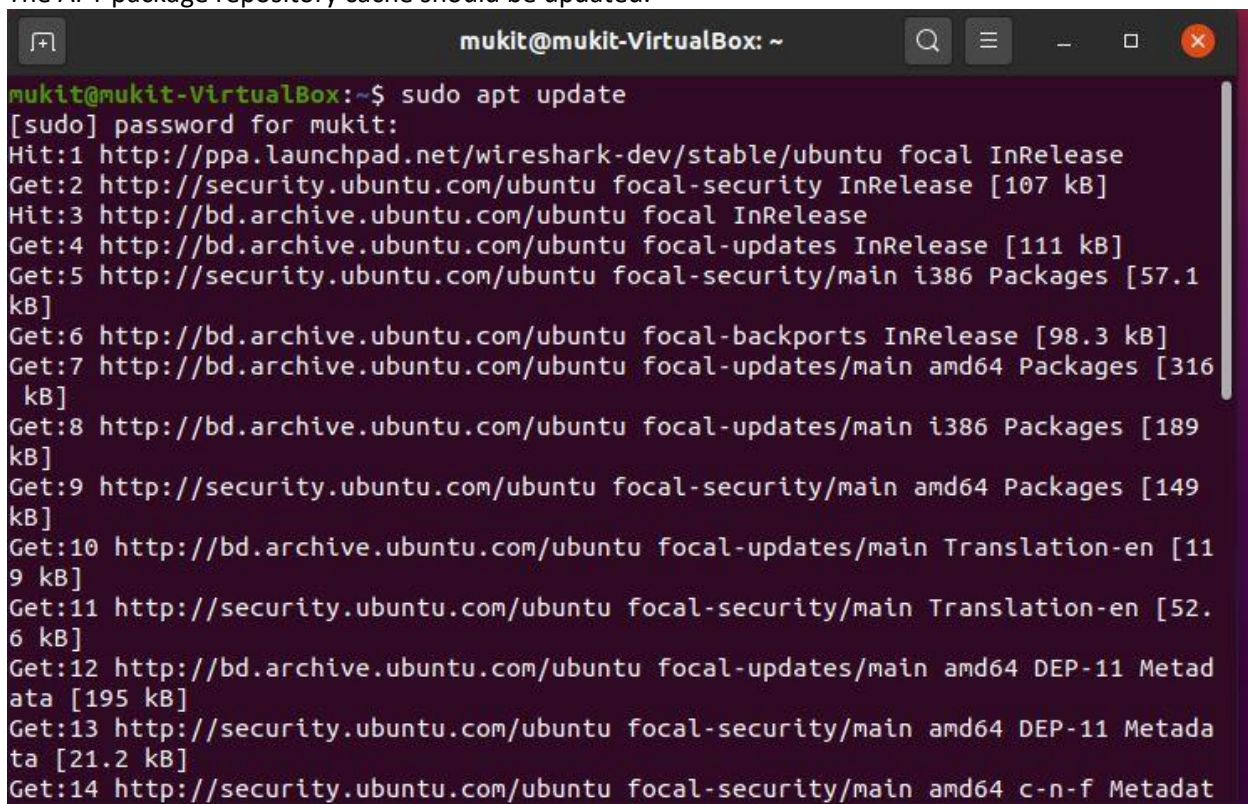
Wireshark is a network packet analyzer. It captures every packet getting in or out of a network interface and shows them in a nicely formatted text. It is used by Network Engineers all over the world.

How to install Wireshark is given below step by step:

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

```
$ sudo apt update
```

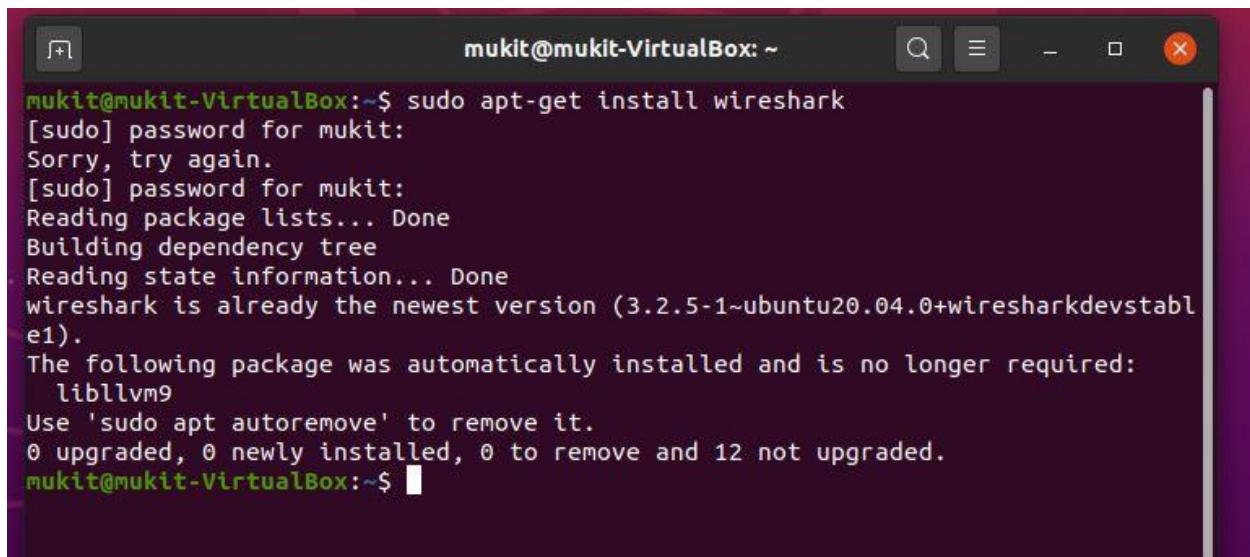
The APT package repository cache should be updated.



```
mukit@mukit-VirtualBox: ~$ sudo apt update
[sudo] password for mukit:
Hit:1 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu focal InRelease
Get:2 http://security.ubuntu.com/ubuntu focal-security InRelease [107 kB]
Hit:3 http://bd.archive.ubuntu.com/ubuntu focal InRelease
Get:4 http://bd.archive.ubuntu.com/ubuntu focal-updates InRelease [111 kB]
Get:5 http://security.ubuntu.com/ubuntu focal-security/main i386 Packages [57.1 kB]
Get:6 http://bd.archive.ubuntu.com/ubuntu focal-backports InRelease [98.3 kB]
Get:7 http://bd.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [316 kB]
Get:8 http://bd.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages [189 kB]
Get:9 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [149 kB]
Get:10 http://bd.archive.ubuntu.com/ubuntu focal-updates/main Translation-en [119 kB]
Get:11 http://security.ubuntu.com/ubuntu focal-security/main Translation-en [52.6 kB]
Get:12 http://bd.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metadata [195 kB]
Get:13 http://security.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Metadata [21.2 kB]
Get:14 http://security.ubuntu.com/ubuntu focal-security/main amd64 c-n-f Metadata
```

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

```
$ sudo apt get install wireshark
```

A terminal window titled 'mukit@mukit-VirtualBox: ~' with standard window controls. The terminal shows the command 'sudo apt-get install wireshark' being executed. It prompts for a password twice, then shows the progress of installing the package, including reading package lists, building a dependency tree, and reading state information. It reports that Wireshark is already the newest version (3.2.5-1~ubuntu20.04.0+wiresharkdevstable1) and that the package 'libllvm9' was automatically installed and is no longer required. It suggests using 'sudo apt autoremove' to remove it. The final summary shows 0 upgraded, 0 newly installed, 0 to remove, and 12 not upgraded. The prompt returns to 'mukit@mukit-VirtualBox:~\$' with a cursor.

```
mukit@mukit-VirtualBox:~$ sudo apt-get install wireshark
[sudo] password for mukit:
Sorry, try again.
[sudo] password for mukit:
Reading package lists... Done
Building dependency tree
Reading state information... Done
wireshark is already the newest version (3.2.5-1~ubuntu20.04.0+wiresharkdevstable1).
The following package was automatically installed and is no longer required:
  libllvm9
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 12 not upgraded.
mukit@mukit-VirtualBox:~$
```

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:

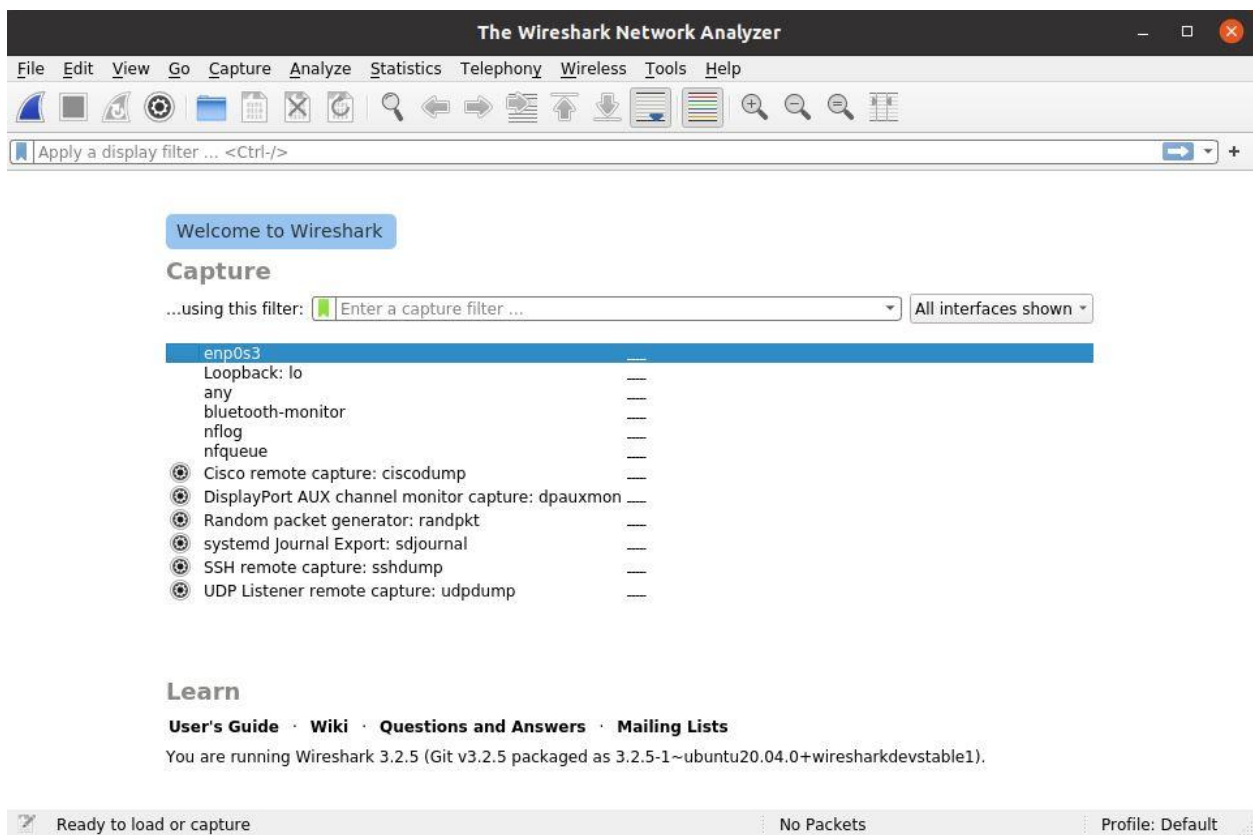
```
$ sudo reboot
```

Now run Wireshark using the following command:

```
$ sudo wireshark
```

```
mukit@mukit-VirtualBox:~$ sudo wireshark
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

Wireshark will start in your computer

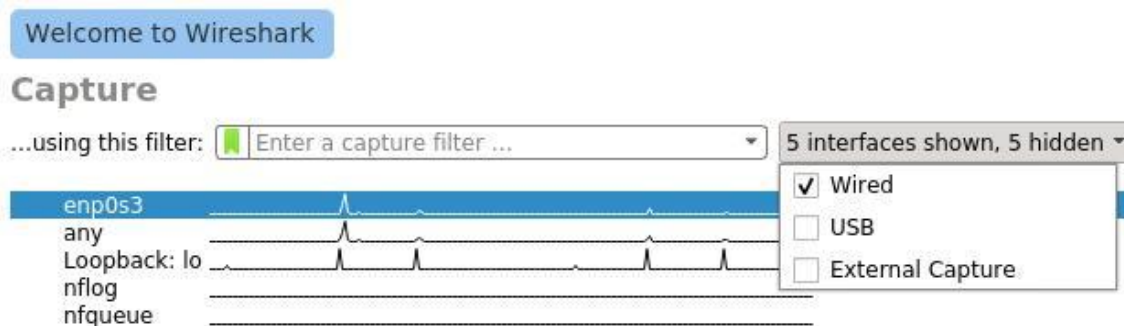


Now we will capture packages using Wireshark.

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.

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

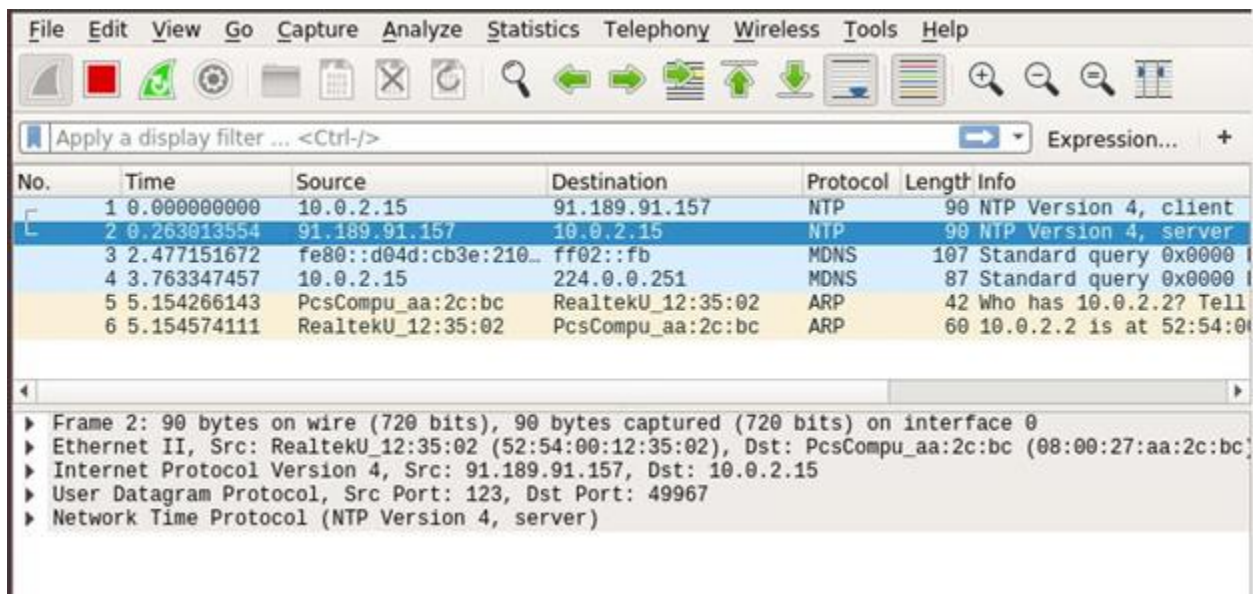
▶	Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
▶	Ethernet II, Src: PcsCompu_aa:2c:bc (08:00:27:aa:2c:bc), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▶	Internet Protocol Version 4, Src: 10.0.2.15, Dst: 91.189.91.157
▶	User Datagram Protocol, Src Port: 49967, Dst Port: 123
▶	Network Time Protocol (NTP Version 4, client)

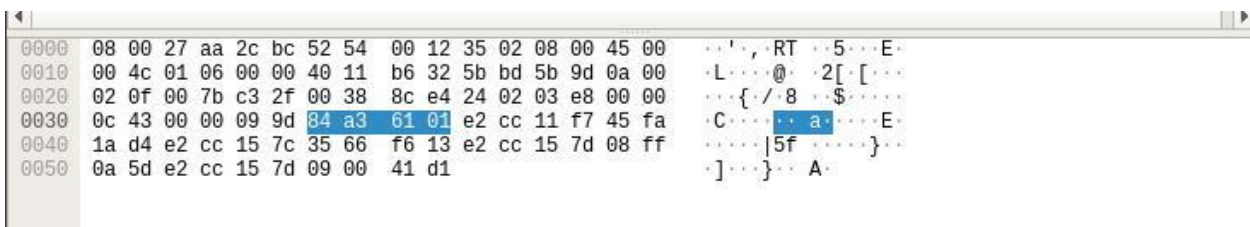
0000	52 54 00 12 35 02 08 00	27 aa 2c bc 08 00 45 10	RT..5...	'...E.
0010	00 4c 6f 4f 40 00 40 11	07 d9 0a 00 02 0f 5b bd	Lo00-@	.....[.
0020	5b 9d c3 2f 00 7b 00 38	c3 b2 23 00 00 00 00 00	[.../{ 8	...#.....
0030	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....	.....
0040	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....	.....
0050	00 00 e2 cc 15 7c 35 66	f6 13	... 5f	...

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.

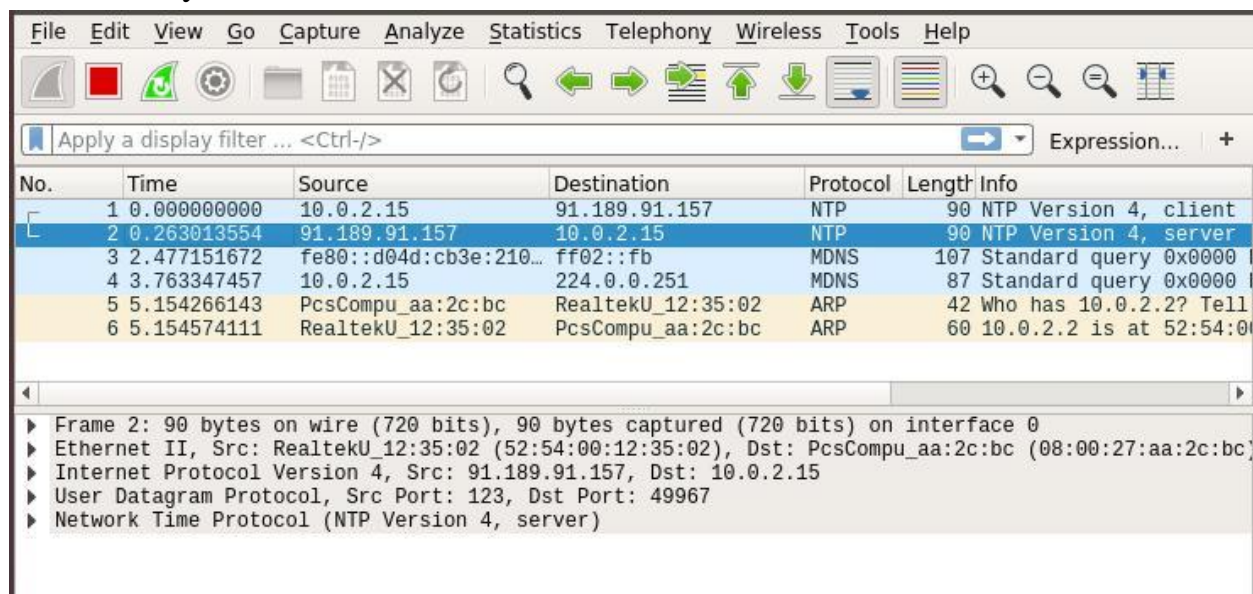


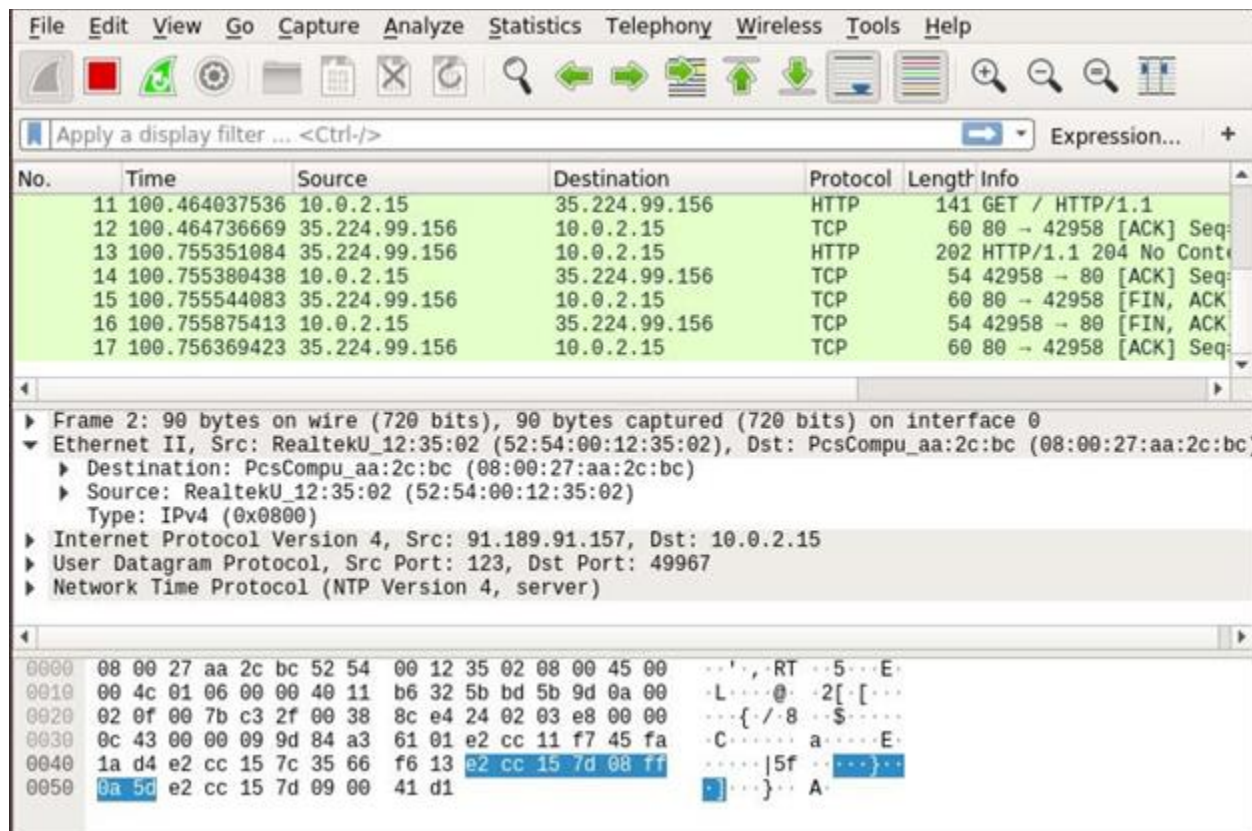


You can also see the RAW data of that particular packet.



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

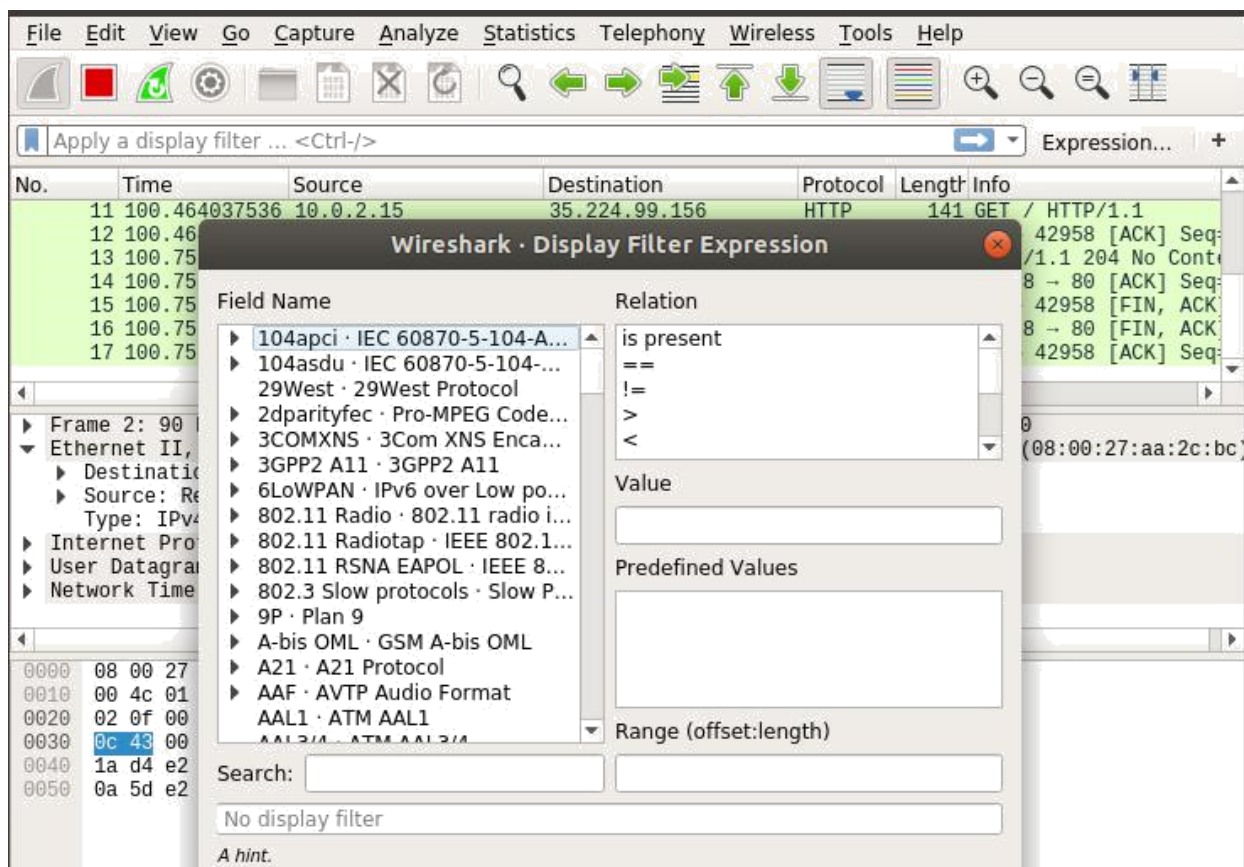




To filter packets, you can directly type in the filter expression in the textbox as marked in the screenshot below.

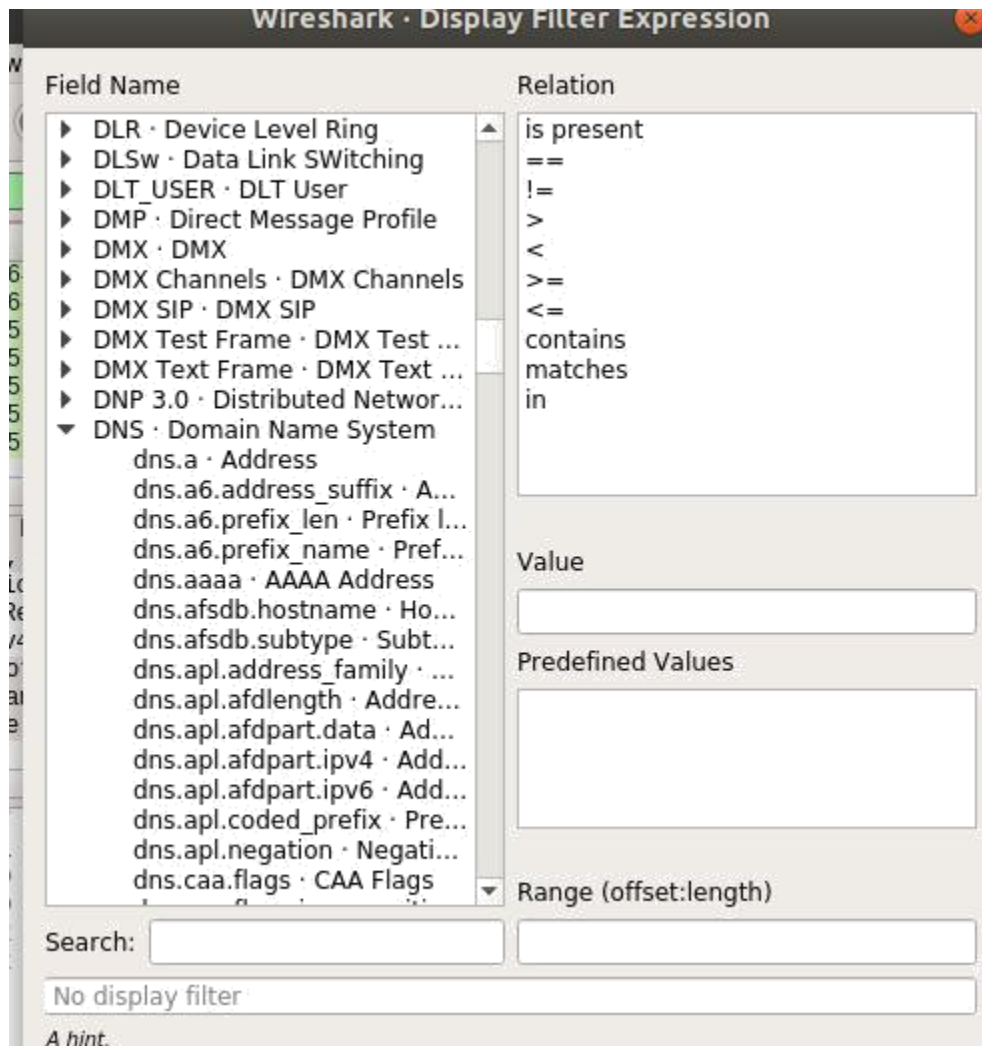
A new window should open as shown in the screenshot below. From here you can create filter expression to search packets very specifically.

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.

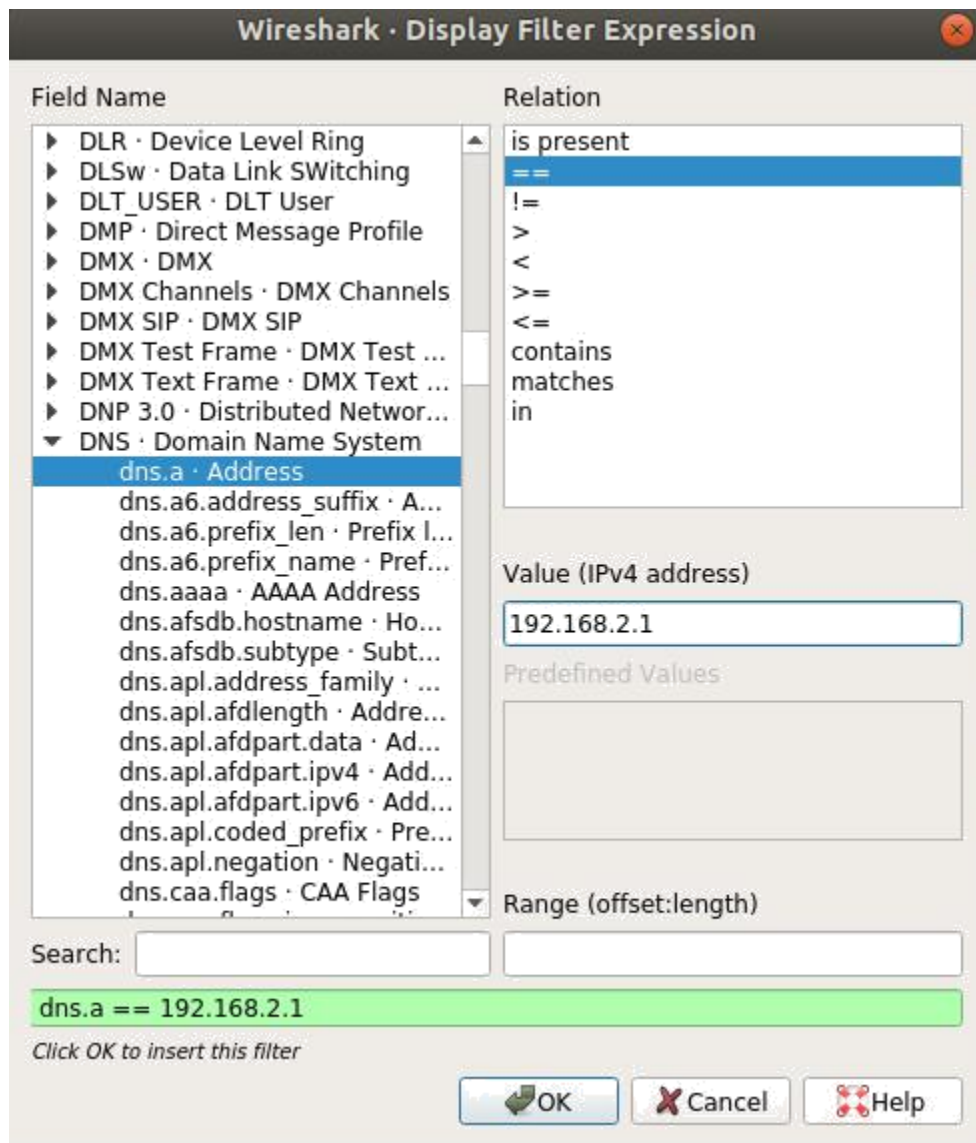


I am going to filter out all the DNS packets. So I selected **DNS Domain Name System** from the **Field Name** list. You can also click on the **arrow** on any protocol.

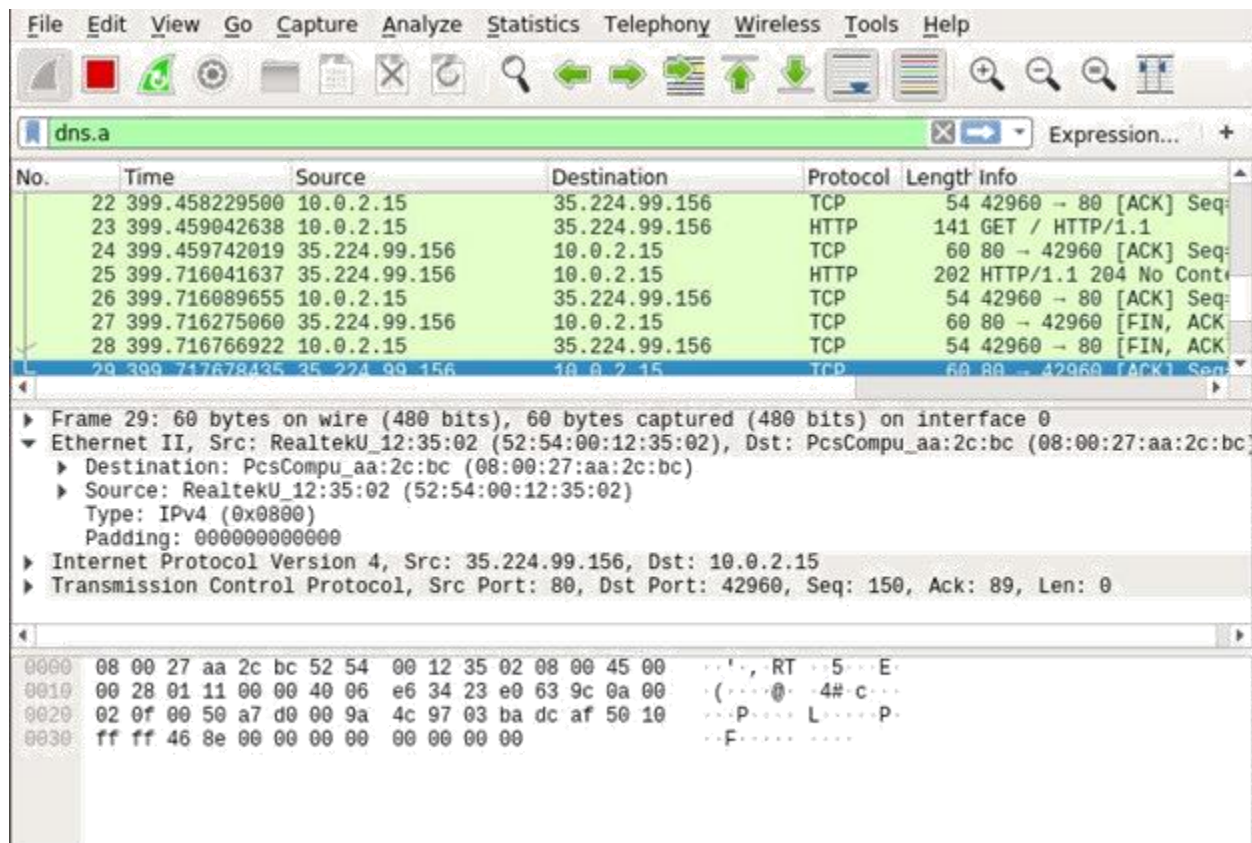




You can also use relational operators to test whether some field is equal to, not equal to, great than or less than some value. I searched for all the DNS IPv4 address which is equal to 192.168.2.1 as you can see in the screenshot below.



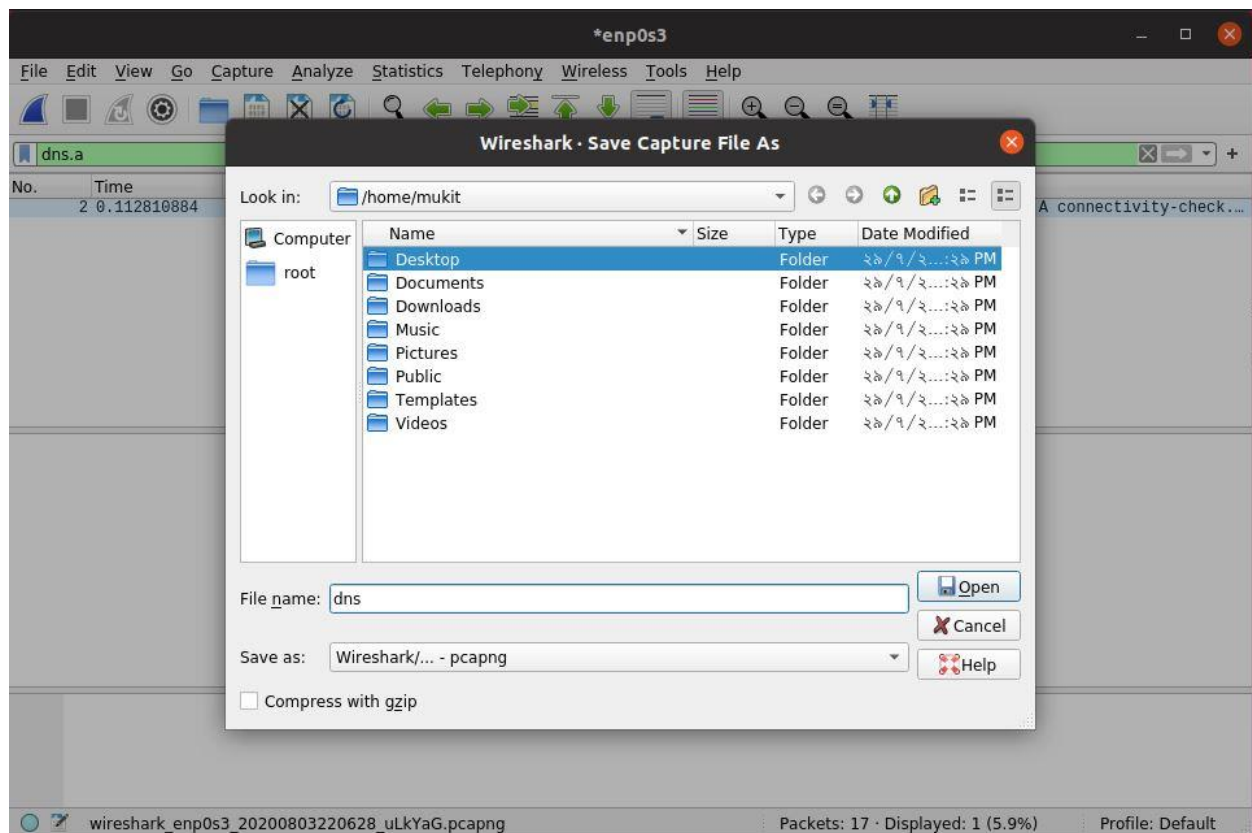
As you can see, only the DNS protocol packets are shown



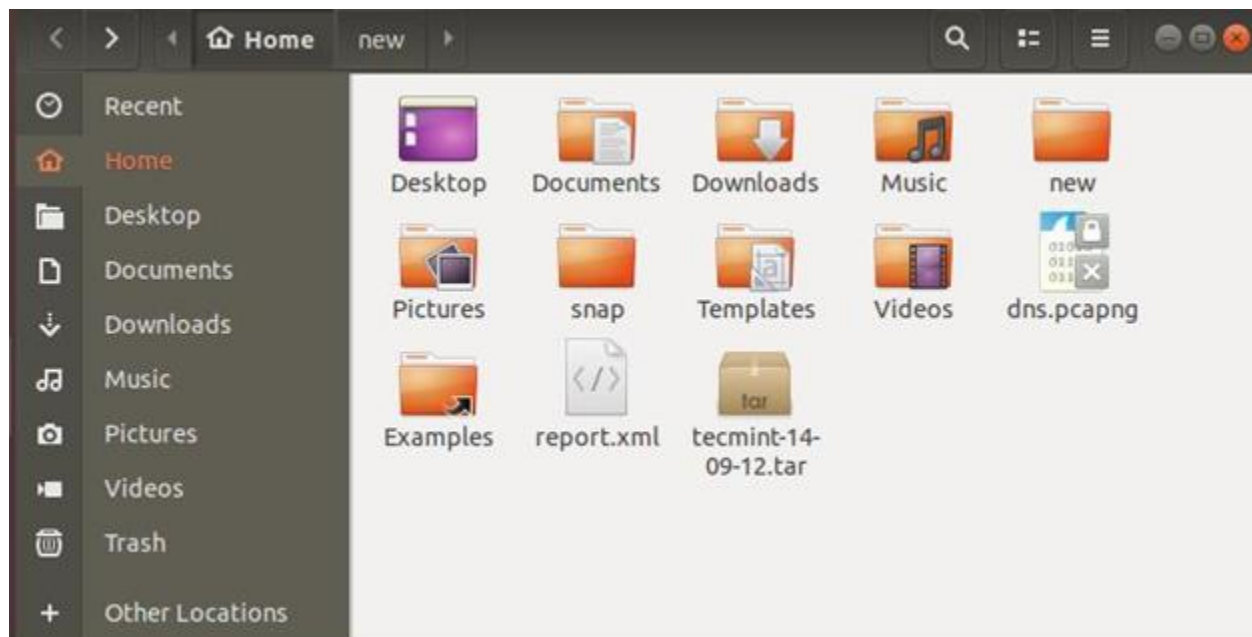
You can click on the red icon as red marked in the screenshot below to stop capturing Wireshark packets.

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 and click on **Save**.



The file should be saved



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