



Mawlana Bhashani Science and Technology University

Santosh, Tangail-1902.

Lab Report

Department of Information and Communication Technology

Report No: 08

Report Name: Install and use Wireshark on Linux Operating System.

Course Title: Network Planning and designing Lab.

Course Code: ICT-3208

Submitted By	Submitted To
Name: Zafrul Hasan Khan & Hasibul Islam Imon ID: IT-18003 & IT-18047 Session: 2017-18 3rd Year 2nd Semester Dept. of Information & Communication Technology, MBSTU.	Nazrul Islam Assistant Professor, Dept. of Information & Communication Technology, MBSTU.

Objectives: The main objectives of this lab how to install wireshark on linux ,to know how to wireshark captures every packet getting in or out of a network interface and shows them in a nicely formatted text .

Theory : 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.

Methodology :

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

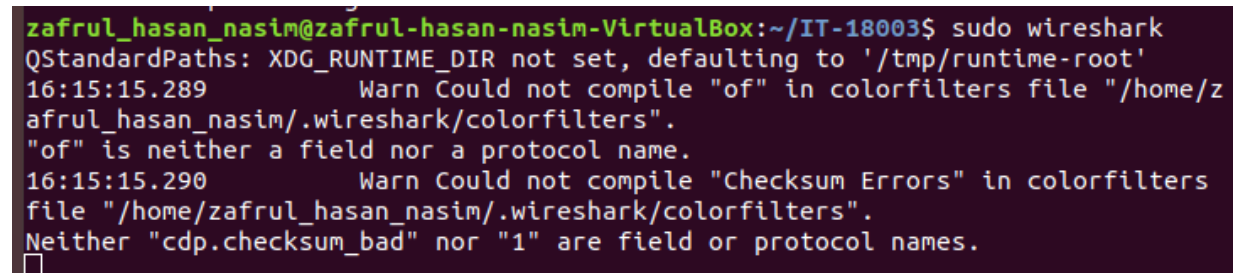
```
$ sudo apt get install wireshark
```

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



```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ sudo wireshark
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
16:15:15.289      Warn Could not compile "of" in colorfilters file "/home/zafrul_hasan_nasim/.wireshark/colorfilters".
"of" is neither a field nor a protocol name.
16:15:15.290      Warn Could not compile "Checksum Errors" in colorfilters
file "/home/zafrul_hasan_nasim/.wireshark/colorfilters".
Neither "cdp.checksum_bad" nor "1" are field or protocol names.
```

After run this above command then show like as below screenshot:

Capturing from enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

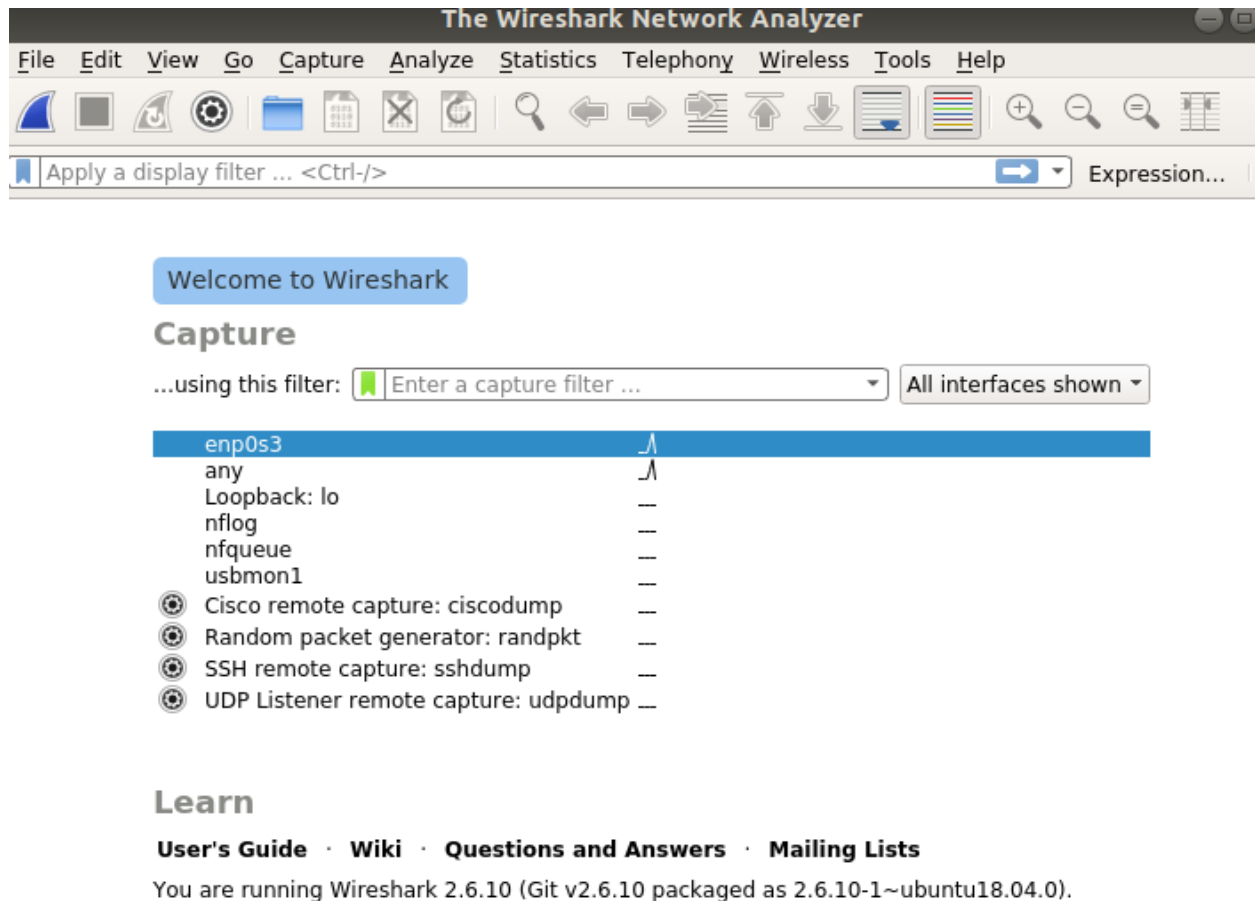
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	91.189.89.198	NTP	90	NTP Version 4, client
2	5.196719549	PcsCompu_44:19:2e	RealtekU_12:35:02	ARP	42	Who has 10.0.2.2? Tell
3	5.196994702	RealtekU_12:35:02	PcsCompu_44:19:2e	ARP	60	10.0.2.2 is at 52:54:00

▶ Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
▶ Ethernet II, Src: PcsCompu_44:19:2e (08:00:27:44:19:2e), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 91.189.89.198
▶ User Datagram Protocol, Src Port: 43156, Dst Port: 123
▶ Network Time Protocol (NTP Version 4, client)

0000	52 54 00 12 35 02 08 00 27 44 19 2e 08 00 45 10	RT..5... 'D'..E.
0010	00 4c 62 c0 40 00 40 11 16 3f 0a 00 02 0f 5b bd	..Lb..@..?....[.
0020	59 c6 a8 94 00 7b 00 38 c1 db 23 00 00 00 00 00	Y....{.8 ..#.....
0030	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
0050	00 00 e3 ef 27 54 1e 17 c1 27'T.. .'.

enp0s3: <live capture in progress>
Packets: 3 · Displayed: 3 (100.0%)
Profile: Default

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:

Welcome to Wireshark

Capture

...using this filter: 5 interfaces shown, 5 hidden ▾



Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 2.6.10 (Git v2.6.10 packaged as 2.6.10-1~ubuntu18.04.0).

Now to start capturing packets, Just press and hold 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:

Capturing from enp0s3

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	91.189.89.198	NTP	90	NTP Version 4, client
2	5.196719549	PcsCompu_44:19:2e	RealtekU_12:35:02	ARP	42	Who has 10.0.2.2? Tell
3	5.196994702	RealtekU_12:35:02	PcsCompu_44:19:2e	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_44:19:2e (08:00:27:44:19:2e), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 91.189.89.198
- User Datagram Protocol, Src Port: 43156, Dst Port: 123
- Network Time Protocol (NTP Version 4, client)

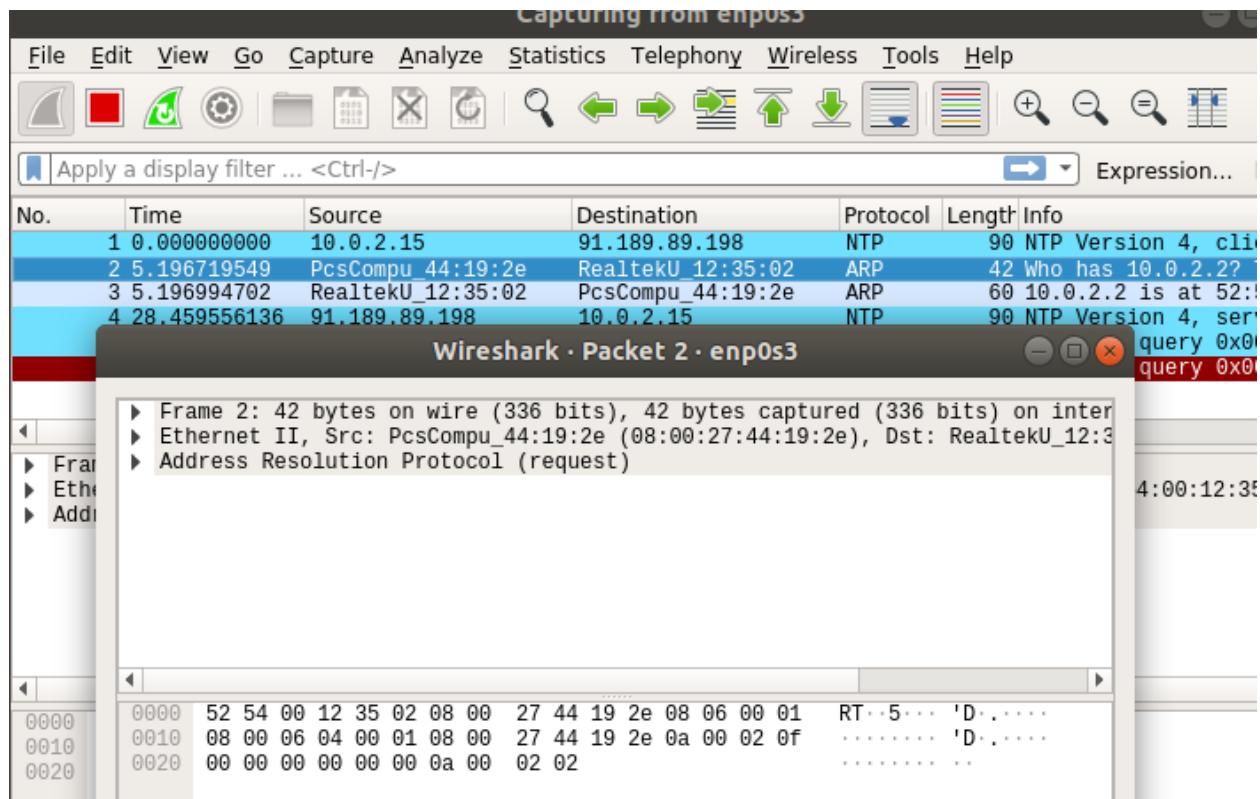
```

0000  52 54 00 12 35 02 08 00 27 44 19 2e 08 00 45 10  RT...5...D...E
0010  00 4c 62 c0 40 00 40 11 16 3f 0a 00 02 0f 5b bd  Lb...@...?...[
0020  59 c6 a8 94 00 7b 00 38 c1 db 23 00 00 00 00 00  Y...{8...#...
0030  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  .....
0050  00 00 e3 ef 27 54 1e 17 c1 27  ....T...

```

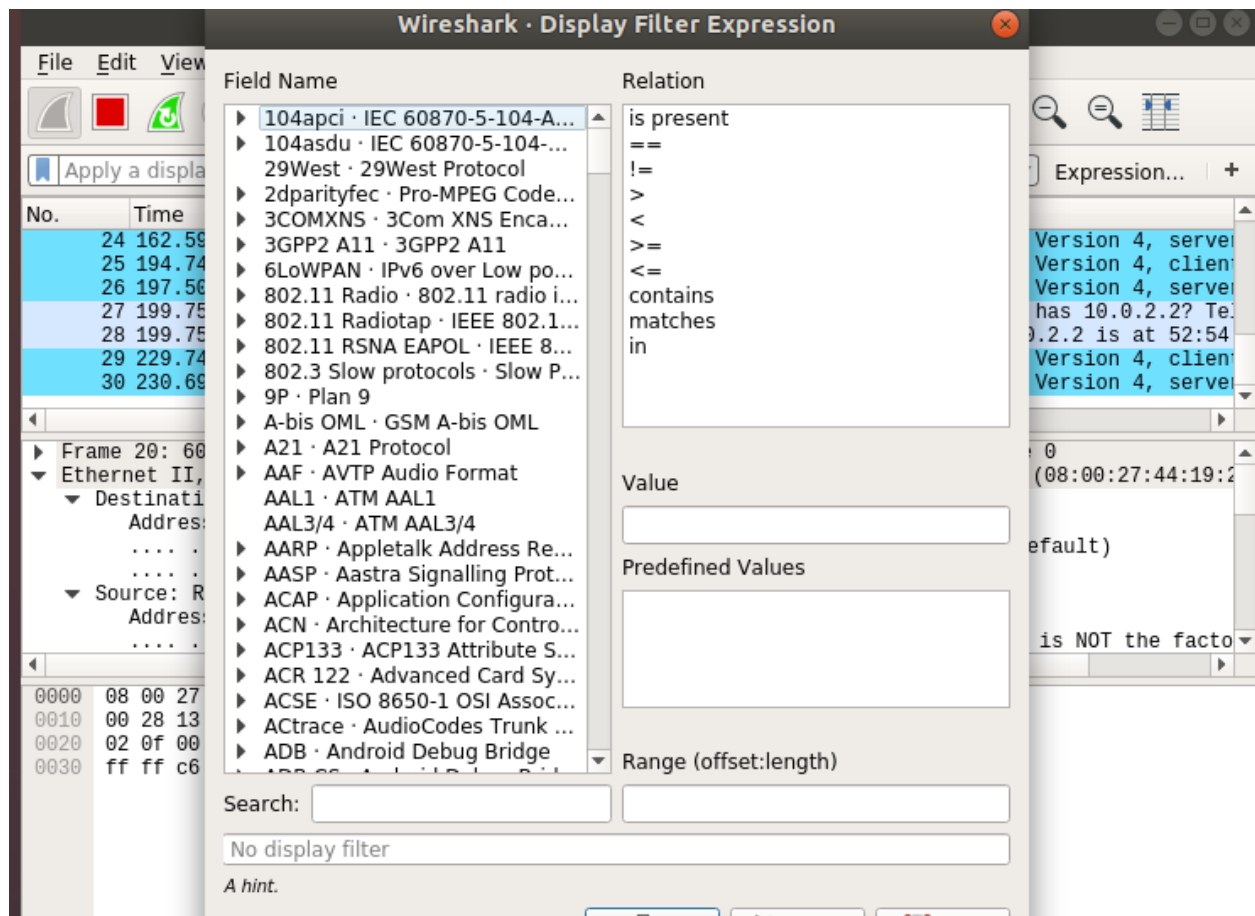
enp0s3: <live capture in progress> Packets: 3 · Displayed: 3 (100.0%) Profile: Default

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.

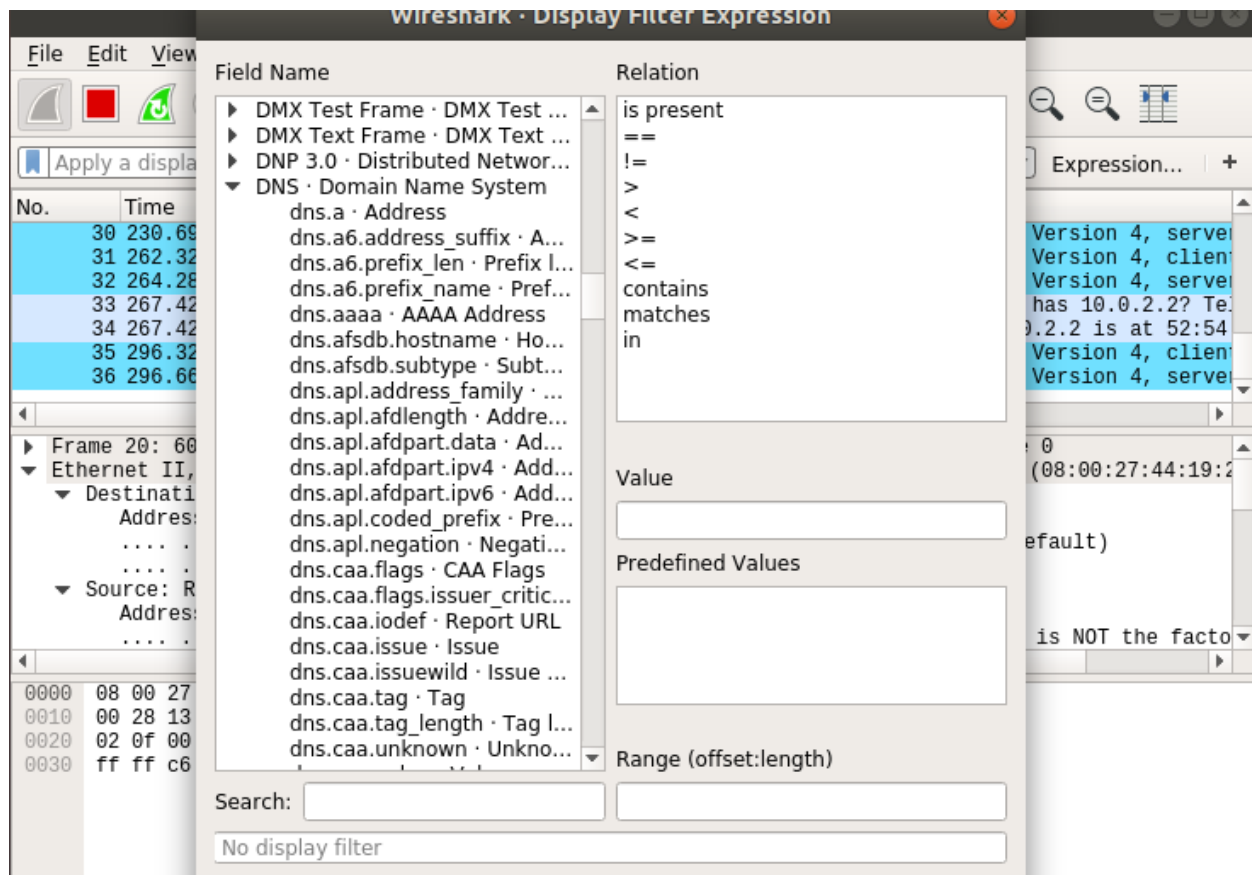


A new window should open as shown in the screenshot below. From here you can create filter expression to search packets very specifically.

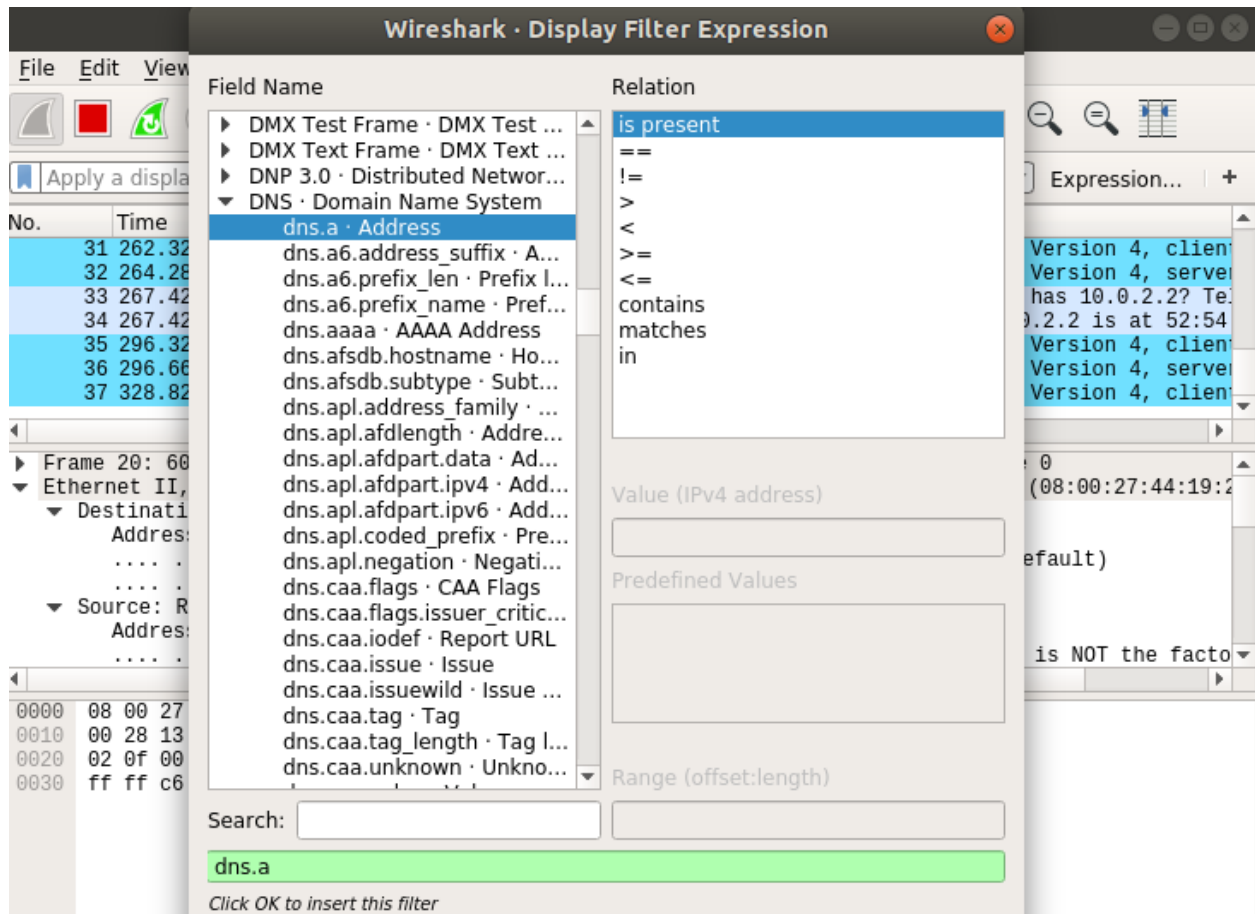
In the Field Name section almost all the networking protocols are listed. The list is huge. You can type in what protocol you're looking for in the Search textbox and the Field Name section would show the ones that matched.



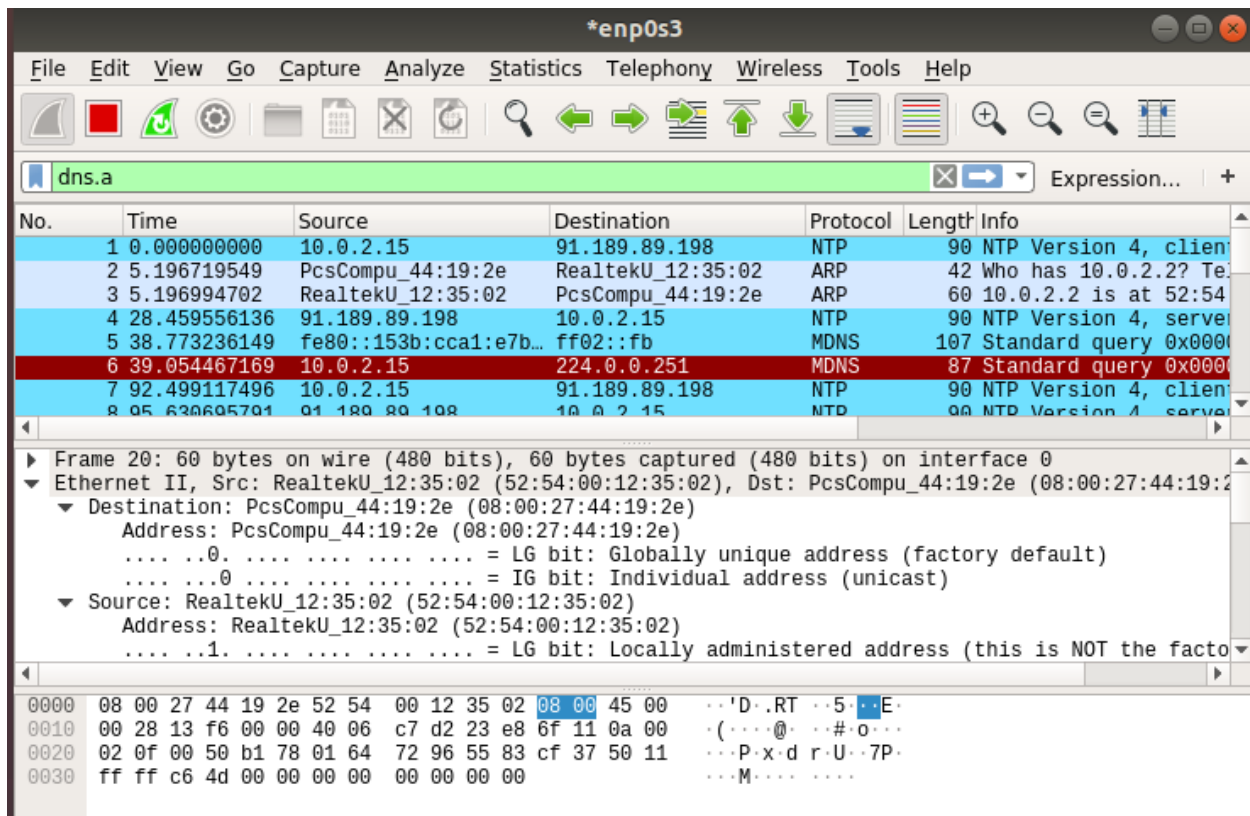
I am going to filter out all the DNS packets. So I selected DNS Domain Name System from the Field Name list. I can also click on the arrow on DNS protocol .



I 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.

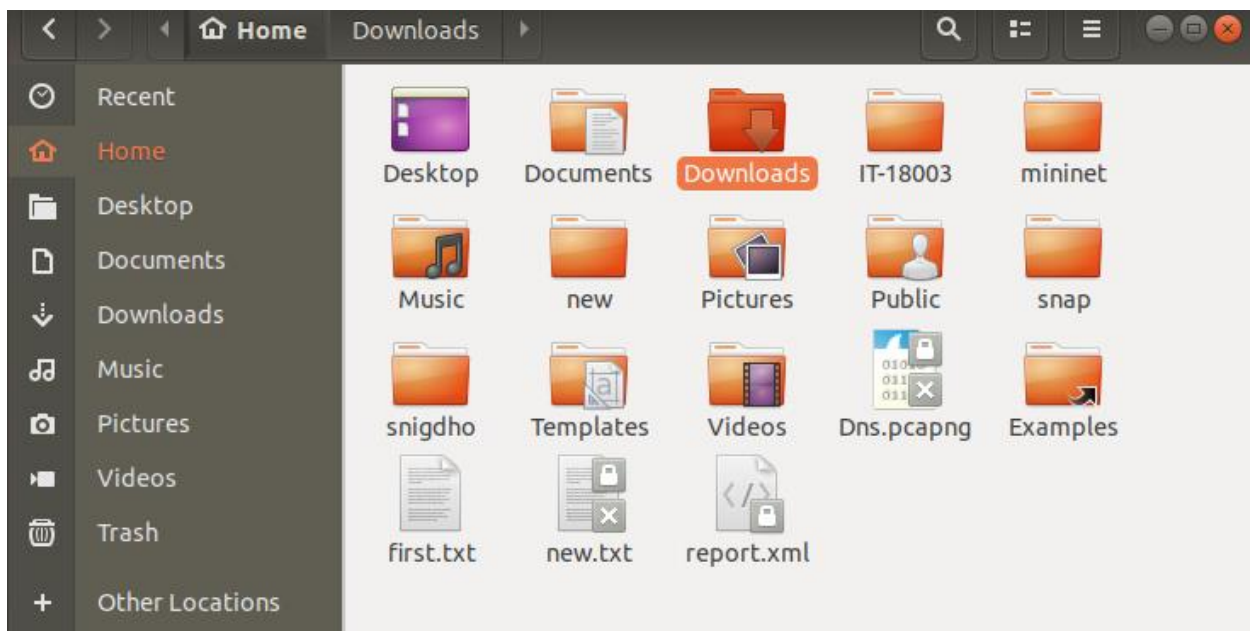


As I can see, only the DNS protocol packets are shown.



Now select a destination folder, type in the file name and click on Save:

I save this file as ' Dns.pcapng ' and store in home .



Conclusion: From this lab , I have learnt that how to install and use wireshark on Linux . Wireshark is a really interesting tool to have installed - both for developers and curious minds. It have some might potentially benefit such as : Web debugging, Capture interesting stuff, Making sure that the right applications access the right resources. I want to make sure that every application I use, that has access to the Internet, only accesses resources it should, WireShark pretty much covers every transfer layer. I have also known that it is not that big and doesn't consume enormous quantities of resources, so it runs pretty well in the background while other processes are running.