Mawlana Bhashani Science and Technology University

Lab-Report

Report No:08

Report Name:Installing Wireshark in Linux Operating System

Course title: Computer Network Lab

Date of Performance:21-04-21

Date of Submission:04-05-21

Submitted by

Name: Sabikun Nahar Piya

ID:IT-18020

3rd year 2nd semester

Session: 2017-2018

Dept. of ICT

MBSTU.

Submitted To

Nazrul Islam

Assistant Professor

Dept. of ICT

MBSTU.

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.

```
piya@piya-VirtualBox:~$ sudo apt update
[sudo] password for piya:
Get:1 http://security.ubuntu.com/ubuntu focal-security InRelease [109 kB]
Hit:2 http://bd.archive.ubuntu.com/ubuntu focal InRelease
Get:3 http://bd.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:4 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [627
 kB]
Get:5 http://bd.archive.ubuntu.com/ubuntu focal-backports InRelease [101 kB]
Get:6 http://security.ubuntu.com/ubuntu focal-security/main i386 Packages [224
kB]
Get:7 http://security.ubuntu.com/ubuntu focal-security/main Translation-en [127
 kB]
Get:8 http://security.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Metada
ta [24.4 kB]
Get:9 http://security.ubuntu.com/ubuntu focal-security/main DEP-11 48x48 Icons
[11.0 kB]
Get:10 http://security.ubuntu.com/ubuntu focal-security/main DEP-11 64x64 Icons
 [16.5 kB]
Get:11 http://security.ubuntu.com/ubuntu focal-security/main amd64 c-n-f Metada
ta [7,460 B]
Get:12 http://security.ubuntu.com/ubuntu focal-security/universe amd64 Packages
 [557 kB]
Get:13 http://bd.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages [46
5 kB]
```

Now, 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

```
                    Ssudaaptnsta\1wlreshark<
Read1ng pacKage 1Tsl:s.    Dane
eu11dlngdependencytree
Read1ngs1ale1nlanma1lan...Done
The following additional packages will be installed :
  libc-ares2 libdouble-conversions liblua'5.2-0 libpcre2-16-0 libqtBcore5a
  libqtsdbuss libqt5Qui5 libqtSmultimedia5 libqt5multimediaS - plugins
  libqt5multimedidgsttools6 libqtSmultimedidwidgets5 libqtSnetwork9
  libqtsopengls libqtsprintsupports libqtssvgs libqtswidgetss libsmizldbl
  libsnappylvs tibspandsp2 tibssh-gcrypt-4 tibwireshark-ddtd tibwireshdrkl3
  libwiretapio libwsutilil libxcb-xineramao libxcb-xinputo
  qt5-gtk- platformtheme qttranslationsB-ll0n wireshark - common wireshark - qt
Suggested packages :
  qt5-imaQe-formats-plugins qtwayland5 snmp-mibs-downloader geoipupdate
  gealp-dacabasegealp—dacabase-extra\lbs-1eal'1ec
  libjs -leaflet. markercluster wireshark-doc
The following new packages will be installed :
  libc-ares2 libdouble-conversions libtua'5.2-0 libpcre2-16-0 libqt5core5a
  libqt5dbusS libqts9ui5 libqt5multimedias libqtSmuttimedia5- plugins
  tibqt5muttimedidgsttoots5 tibqt5multimediawidgets5 libqt5network5
  libqtsopengls libqt5printsupport5 libqtssvgs libqt5widgetsS libsmi2ldbl
  libsnappylv5 libspandsp2 libssh-gcrypt-d libwireshark-Oata libwiresharkl3
  libwiretaplo libwsutilll libxcb-xineramaO libxcb-xinput0
  qts gtk-platformtheme qttranslations5 l10n wireshark wireshark-common wireshark—
  qt                                                              y g. g
O- upgnade•d, 31 new1y 1nsl:a11ed, O- l:a  nemoveand22nat:upgnaded
Needtogec0B/32.9MBo7anchlves.
A11ent:hTsapenat:Tan,163MBa7addT1lana1d1skspacew111be•u•
DoyOuwant1ocontInUey§v/n§
```

Conf'6gur Eng w6resha z-k - common

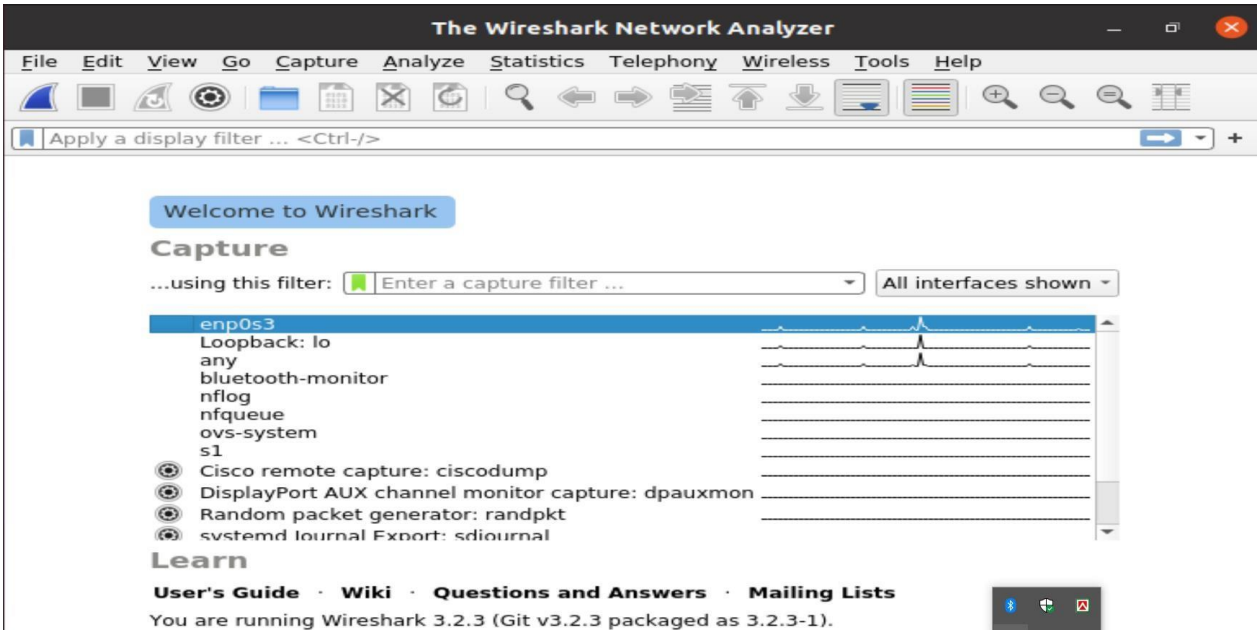
Dunpcap can be ins falled in a ¥vay that allows esenbez-s of' I-he "w1resha k" sys€en group No cap€uz-e packets . This is recoe'u•¥ended Over the aft-er-native off-unn1ng Nez-eshaz-k/Tshaz-k dv rec€ly as root- . because less of' the code with run with eleva' ed privileges

/ usw/sha we/doc/w6 mesha wk- soe•uson/READ 'IE. Debtan. gz once the package is

```
Enabling this feature may be a security risk, so it is disabled by
default. If in doubt, it is suggested to leave it disabled.

Should non-superusers be able to capture packets?
```

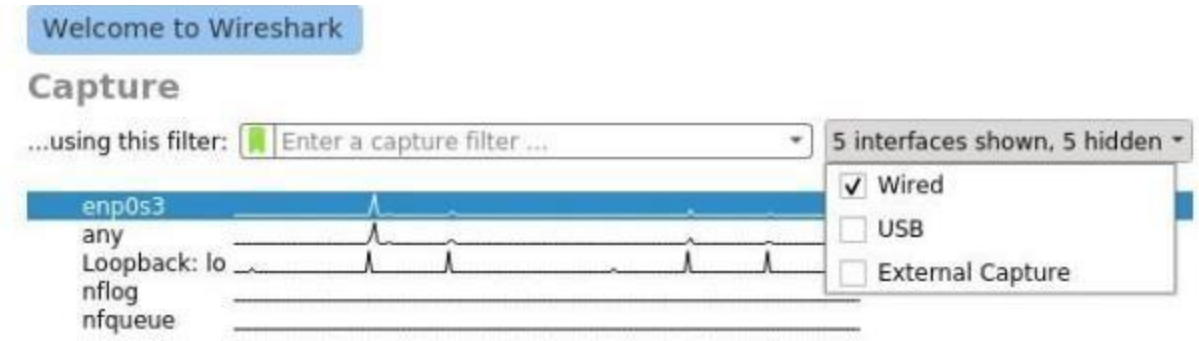
```
                    Ssudawlreshar
QStandar dPaths: XDG RUNTIME DIRtot sel,delau1tIngto'/tmp/nuntIme-root'
                    S #
```



Now we will capture packages using Wireshark.

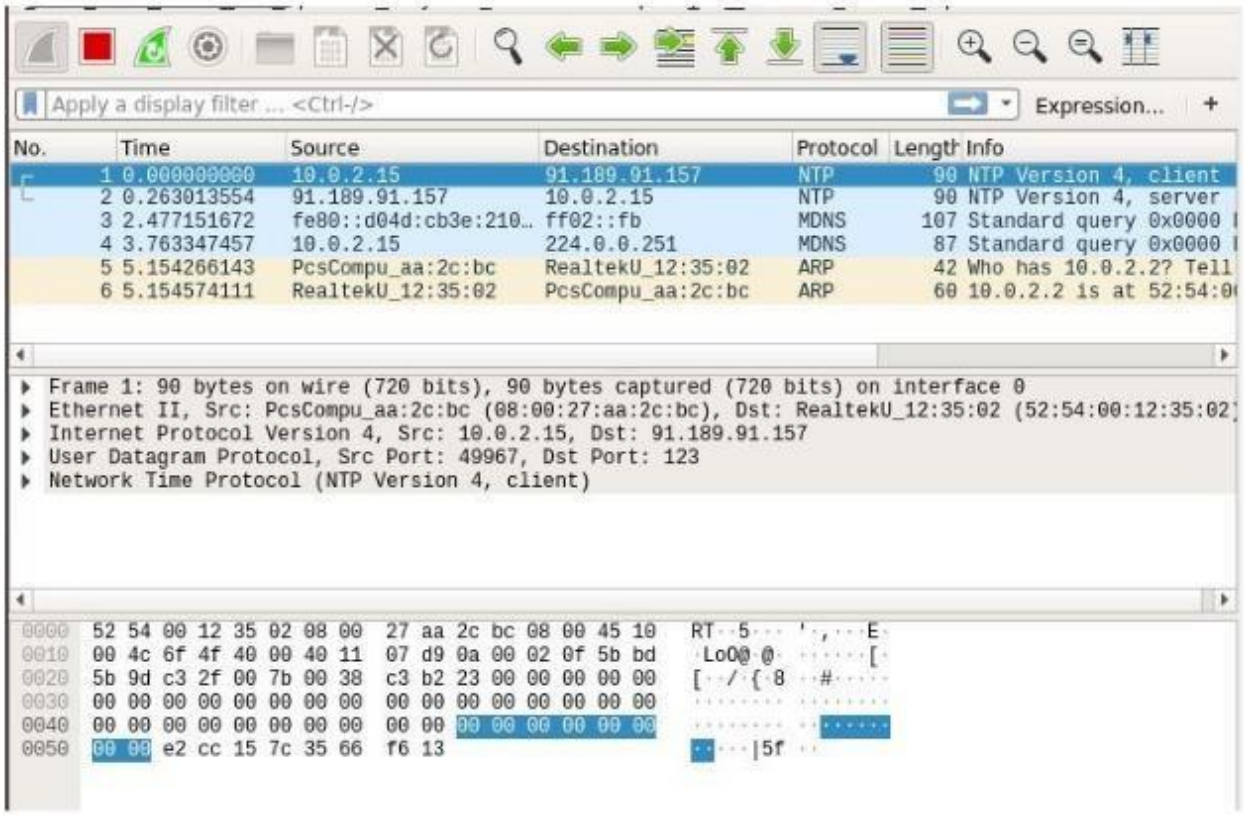
When you start Wireshark, you will see a list of interfaces that you can capture packets to and
from.

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.

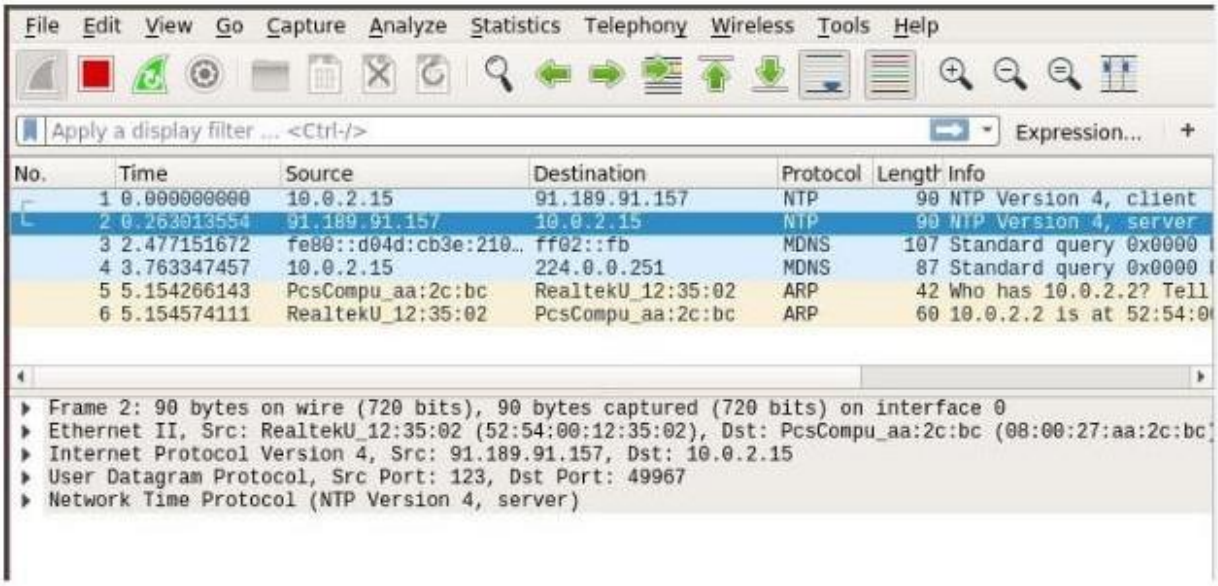


Now to start capturing packets, just select the interface (in my case interface ens33) and click on the **Start capturing packets** icon as marked in the screenshot below.
You can also capture packets to and from multiple interfaces at the same time. Just press and hold **<Ctrl>** and click on the interfaces that you want to capture packets to and from and then click on the **Start capturing packets** icon as marked in the screenshot below.

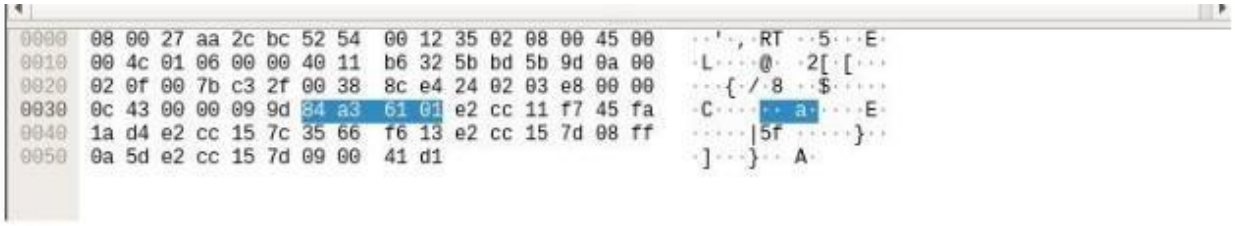
I pinged google.com from the terminal and many packets were captured.



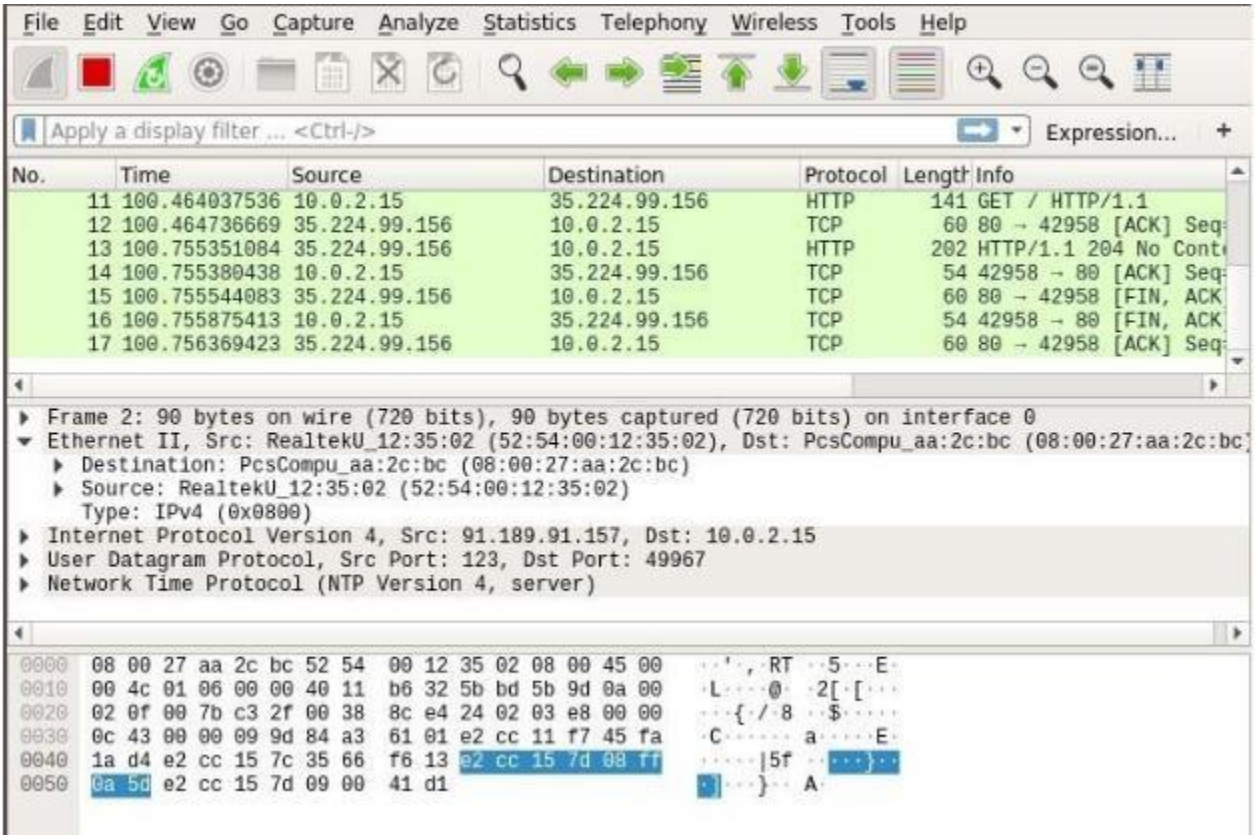
Now you can click on a packet to select it. Selecting a packet would show many information about that packet. As you can see, information about different layers of TCP/IP Protocol is listed.



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



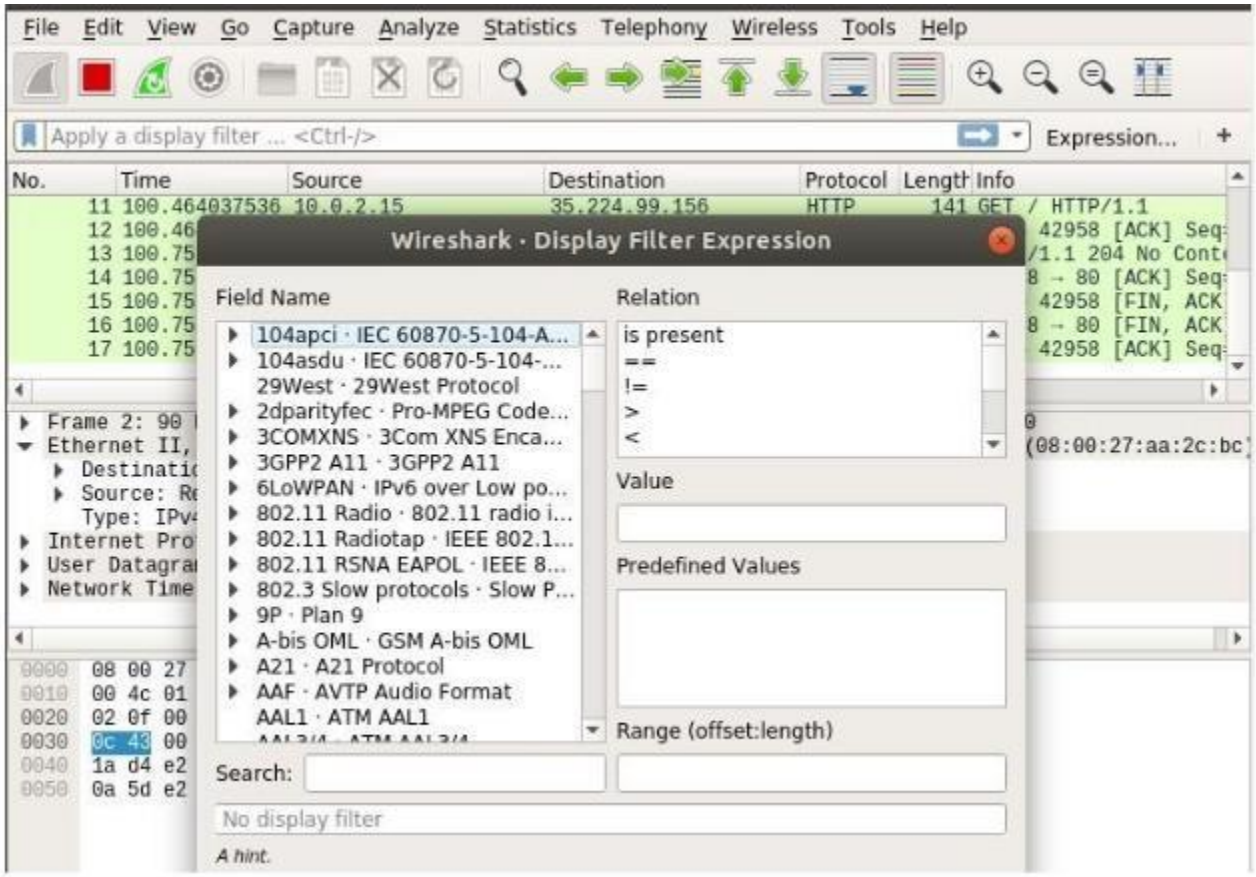
You can also click on the arrows to expand packet data for a particular TCP/IP Protocol Layer.



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

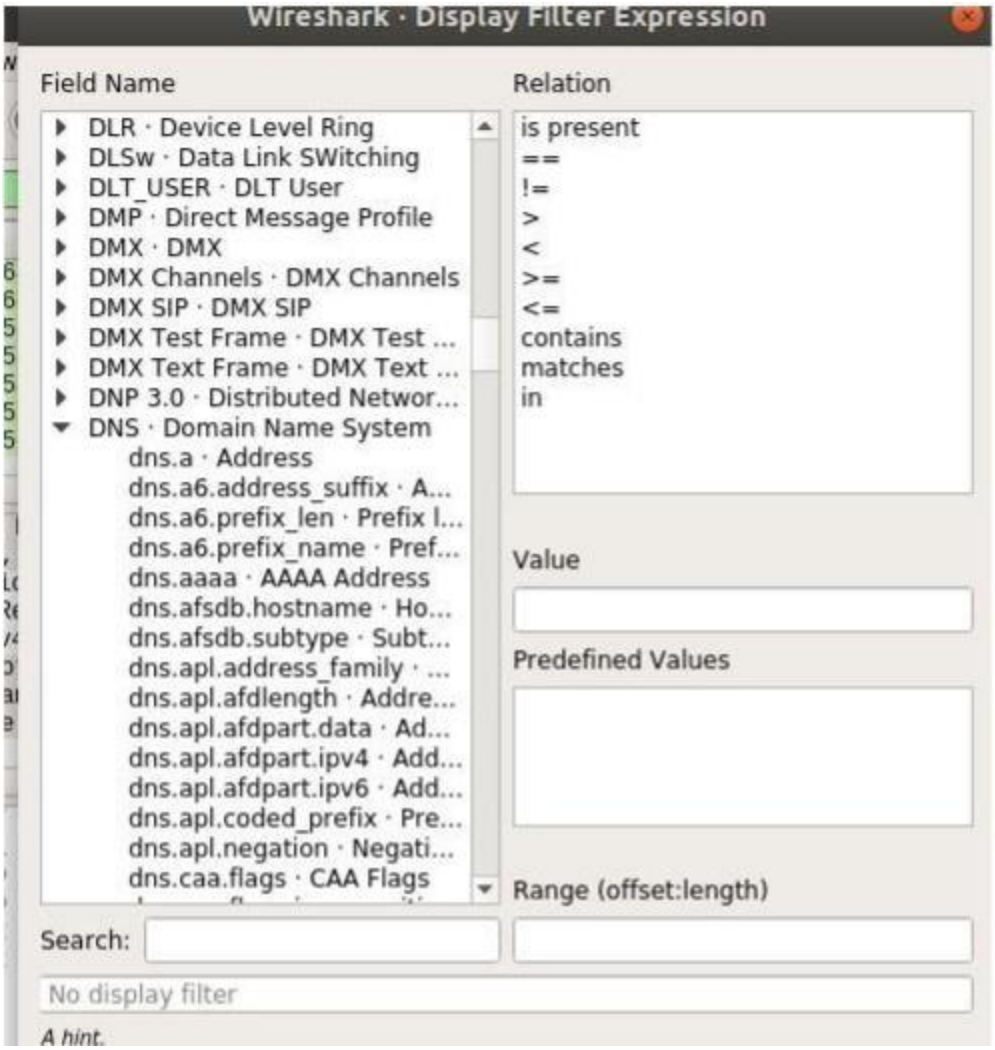
A new window should open as shown in the screenshot below. From here you can create filter expression to search packets very specifically.

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.

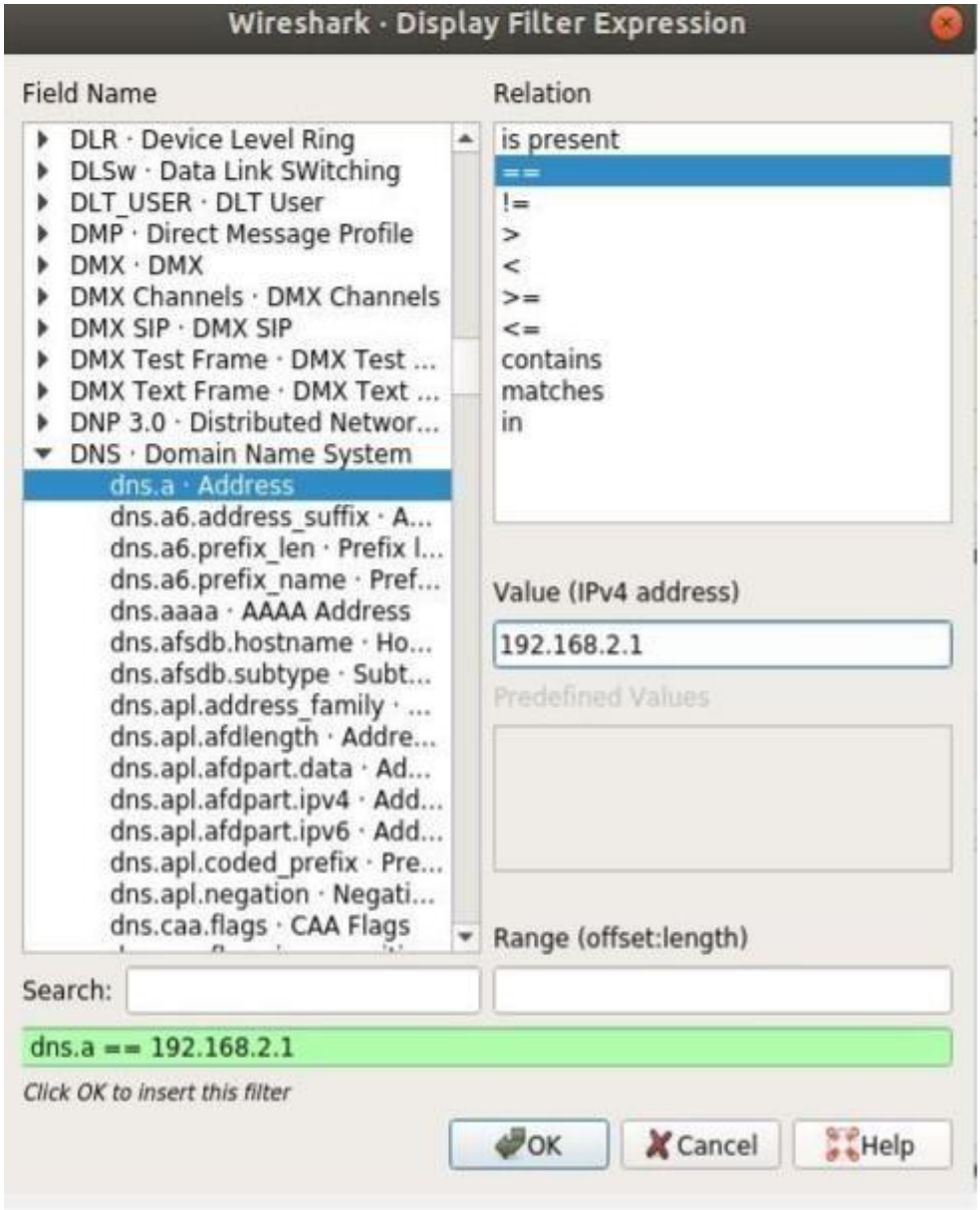


I am going to filter out all the DNS packets. So I selected **DNS Domain Name System** from the **Field Name** list. You can also click on the arrow on any protocol.

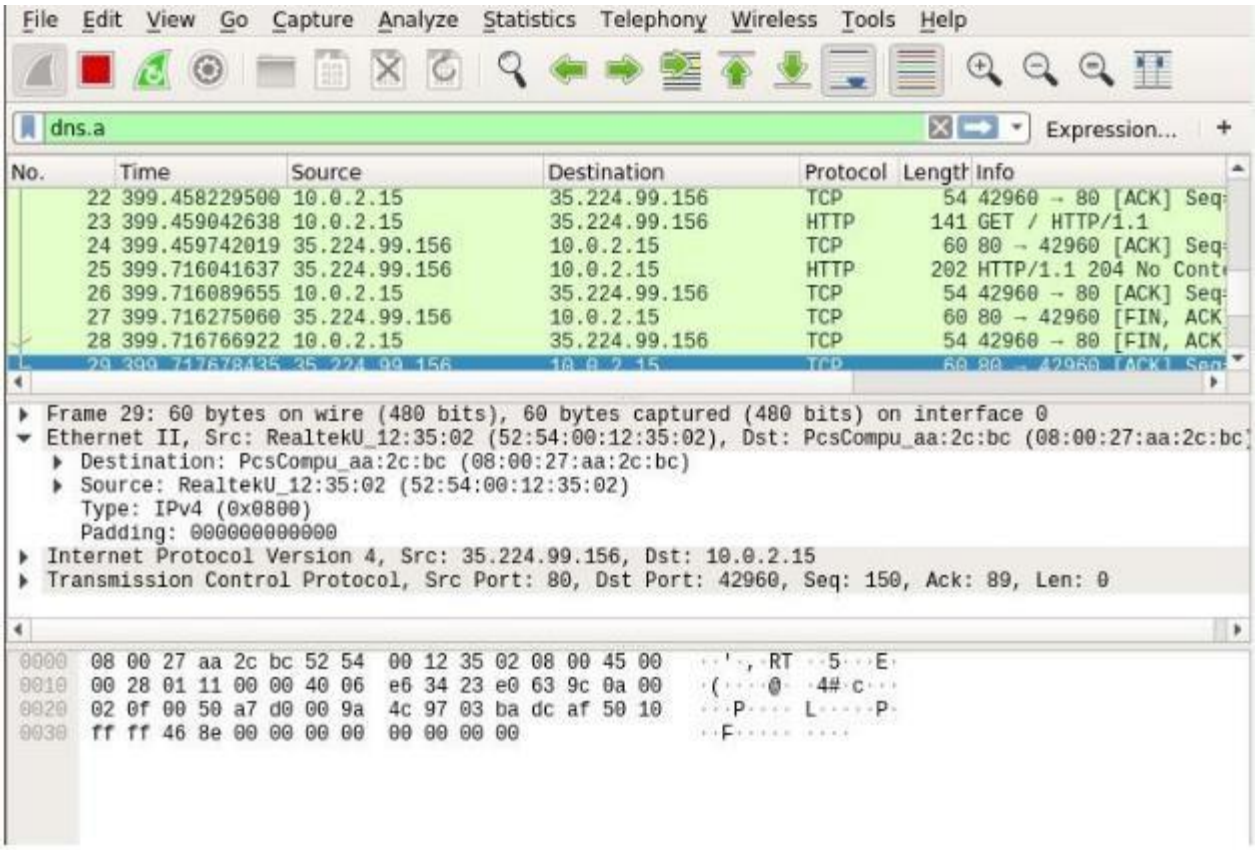
You also can use



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.



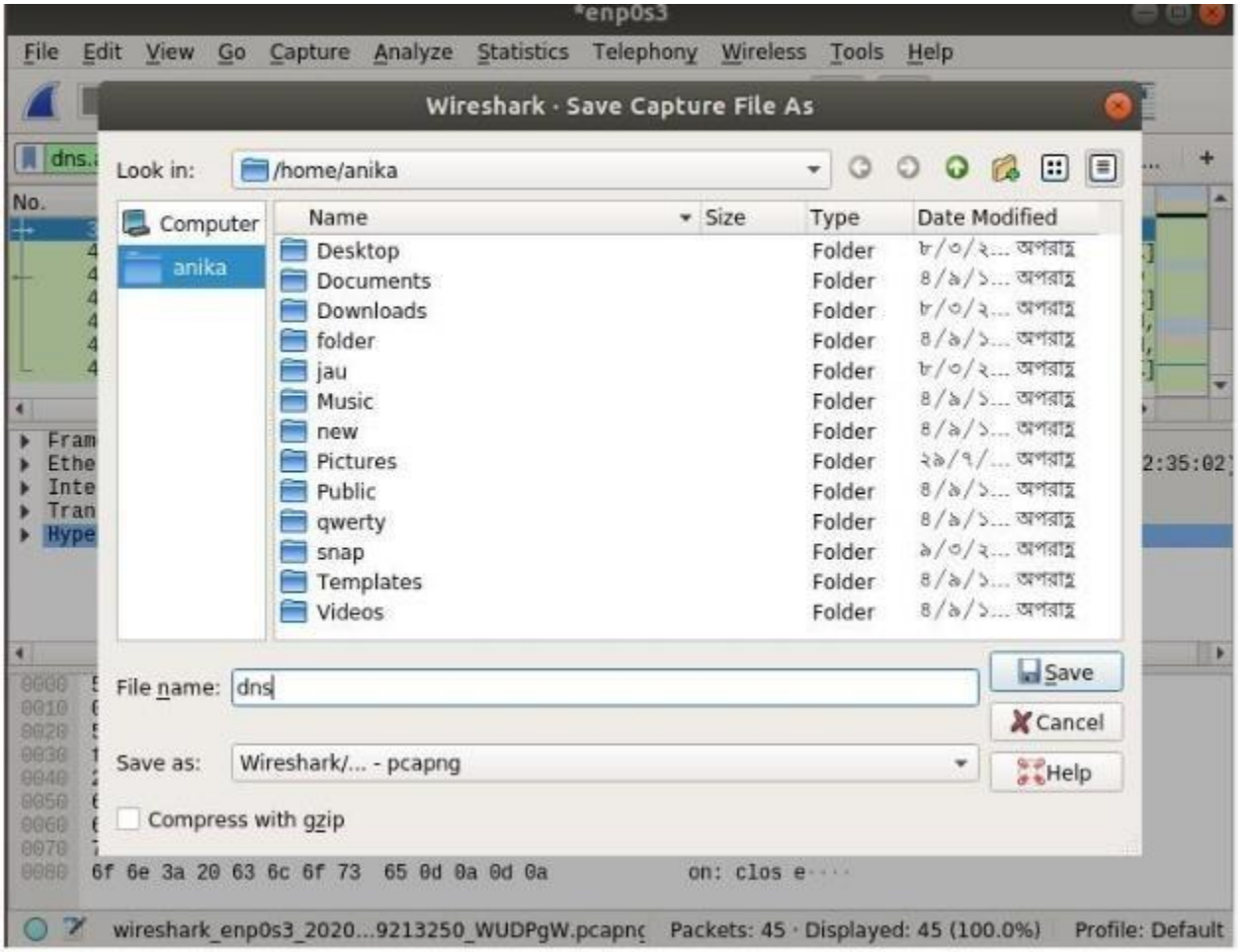
As you can see, only the DNS protocol packets are shown.



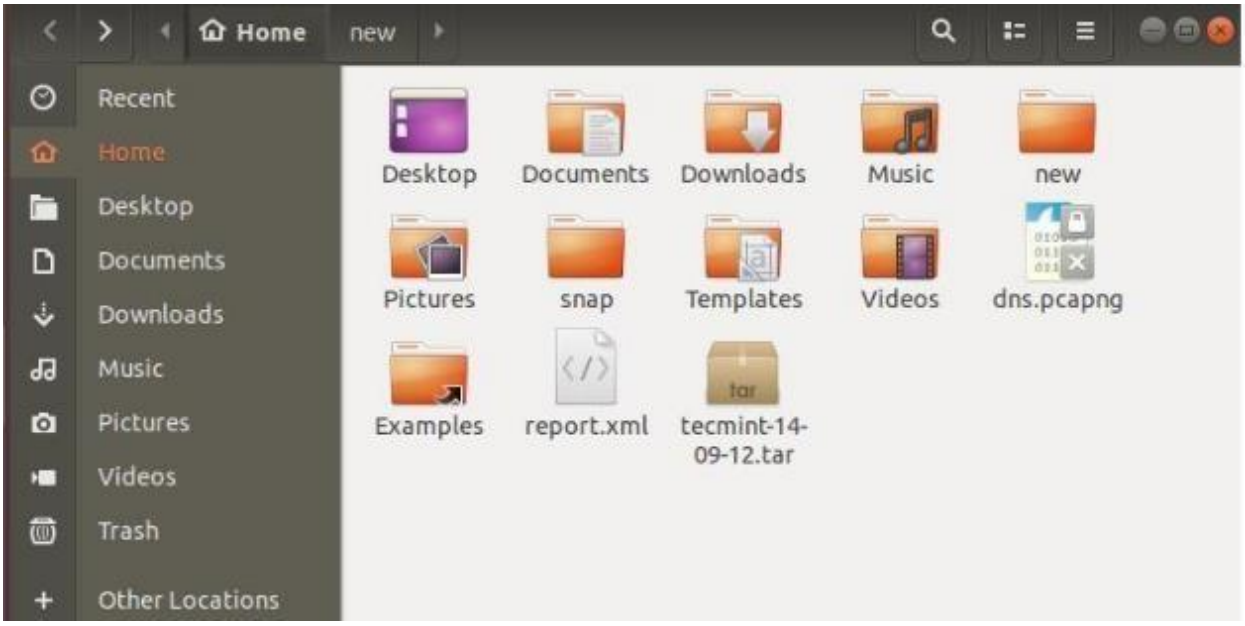
You can click on the red icon as red marked in the screenshot below to stop capturing Wireshark packets.

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.

Conclusion: Wireshark is a must-have (and free) network protocol analyzer for any security professional or systems administrator. It's like Jaws, only for packets.

Wireshark is the world's leading network traffic analyzer, and an essential tool for any security professional or systems administrator. This free software lets you analyze network traffic in real time, and is often the best tool for troubleshooting issues on your network.

Common problems that Wireshark can help troubleshoot include dropped packets, latency issues, and malicious activity on your network. It lets you put your network traffic under a microscope, and provides tools to filter and drill down into that traffic, zooming in on the root cause of the problem. Administrators use it to identify faulty network appliances that are dropping packets, latency issues caused by machines routing traffic halfway around the world, and data exfiltration or even hacking attempts against your organization.