Lab Report No.	02
Lab Report Name	Wireshark in Linux
ID	IT-17037

Objective:

- The main objective of Wireshark is to capture packets that are transmitted over a network. Wireshark can capture, decode and show various details of packets transmitted over a network.
- Observation of the functional difference between different packets and the analysis of the different headers and protocol.
- Writing a filtering options and choosing different analysis options.

Theory:

What is wireshark ?

Wireshark is a popular network analyser that uses pcap library to capture network packets at different layers of the OSI model. It is easy to install and possesses a nice GUI with many features.

Why use wireshark?

Wireshark is used in different sectors and different works . This is used for

- troubleshooting network problems
- examining security problems
- debugging protocol implementations
- learning network protocol internals
- used in industry and academia

what is the main features of the wireshark?

Wireshark has a rich feature set which includes the following:

•Deep inspection of hundreds of protocols, with more being added all the time

•Live capture and offline analysis

•Standard three-pane packet browser

•Multi-platform: Runs on Windows, Linux, OS X, FreeBSD, NetBSD, and many others

•Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility

•The most powerful display filters in the industry

•Rich VoIP analysis

•Capture files compressed with gzip can be decompressed on the fly

•Coloring rules can be applied to the packet list for quick, intuitive analysis

•Output can be exported to XML, PostScript®, CSV, or plain text

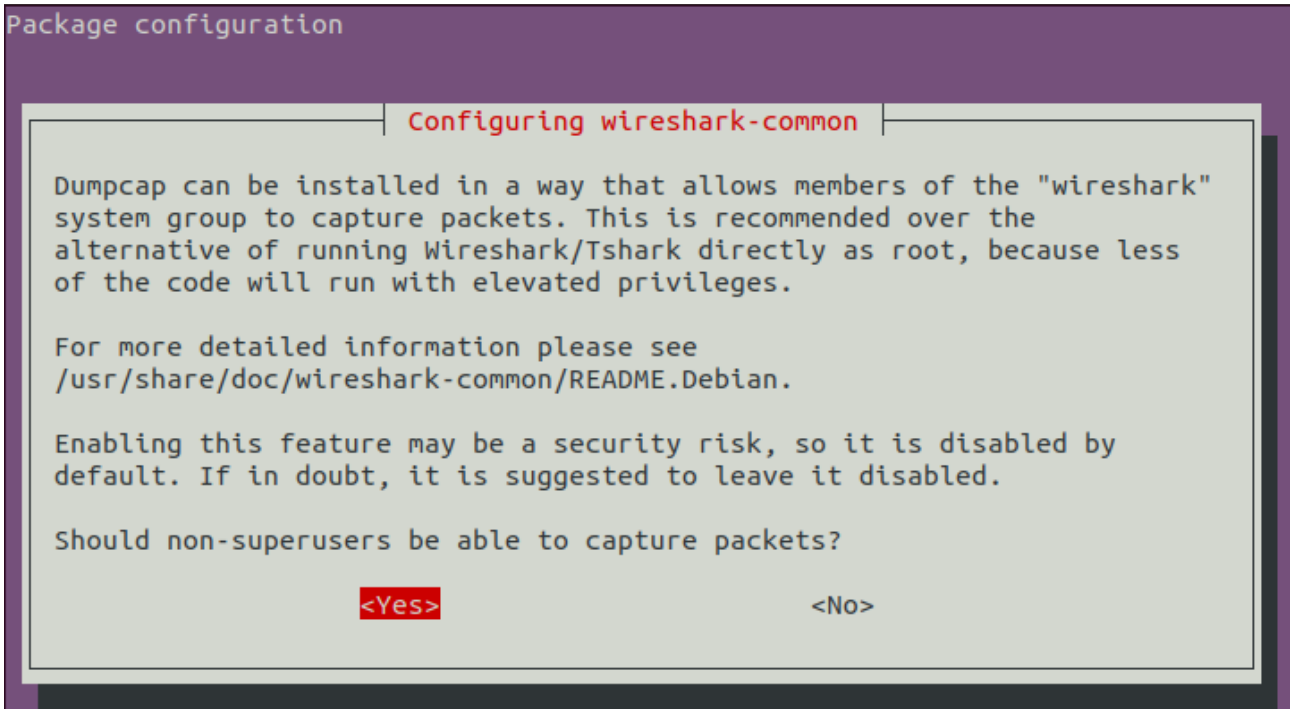
Wireshark Installation:

step-1: open the terminal. write this command:

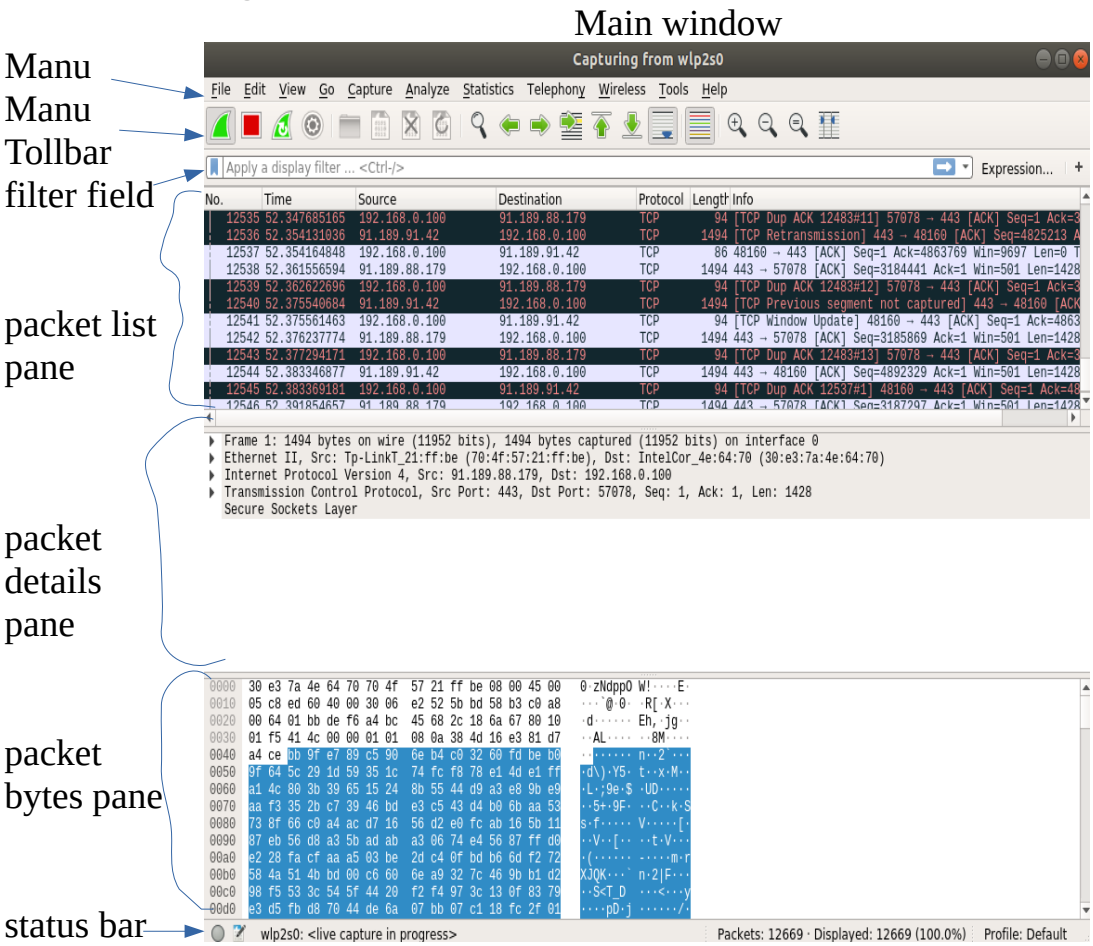
sudo apt-get install wireshark;

```
rafatul@rafatul-HP-Notebook:~$ sudo apt-get install wireshark;
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm7
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libc-ares2 libmaxminddb0 libnl-route-3-200 libqgsttools-p1 libqt5multimedia5
  libqt5multimedia5-plugins libqt5multimediawidgets5 libqt5opengl5
  libqt5printsupport5 libsmi2ldbl libspandsp2 libwireshark-data libwireshark11
  libwiretap8 libwscodecs2 libwsutil9 wireshark-common wireshark-qt
Suggested packages:
  mmdb-bin snmp-mibs-downloader wireshark-doc
The following NEW packages will be installed:
  libc-ares2 libmaxminddb0 libnl-route-3-200 libqgsttools-p1 libqt5multimedia5
  libqt5multimedia5-plugins libqt5multimediawidgets5 libqt5opengl5
  libqt5printsupport5 libsmi2ldbl libspandsp2 libwireshark-data libwireshark11
  libwiretap8 libwscodecs2 libwsutil9 wireshark wireshark-common wireshark-qt
0 upgraded, 19 newly installed, 0 to remove and 298 not upgraded.
Need to get 20.6 MB of archives.
After this operation, 107 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 libmaxminddb0 amd64 1.3.1-1 [25.6 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu bionic/main amd64 libnl-route-3-200 amd64 3.2.29-0ubuntu3 [146 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 libqt5multimedia5 amd64 5.9.5-0ubuntu1 [293 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libqt5opengl5 amd64 5.9.5+dfsg-0ubuntu2.5 [132 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 libqt5multimediawidgets5 amd64 5.9.5-0ubuntu1 [36.6 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 libqgsttools-p1 amd64 5.9.5-0ubuntu1 [72.4 kB]
Get:7 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 libqt5multimedia5-plugins amd64 5.9.5-0ubuntu1 [194 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libqt5printsupport5 amd64 5.9.5+dfsg-0ubuntu2.5 [178 kB]
Get:9 http://us.archive.ubuntu.com/ubuntu bionic/main amd64 libsmi2ldbl amd64 0.4.8+dfsg2-15 [100 kB]
Get:10 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 libspandsp2 amd64 0.0.6+dfsg-0.1 [273 kB]
Get:11 http://us.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 libwireshark-data all 2.6.10-1~ubuntu18.04.0 [1,425 kB]
Get:12 http://us.archive.ubuntu.com/ubuntu bionic/main amd64 libc-ares2 amd64 1.14.0-1 [37.1 kB]
```

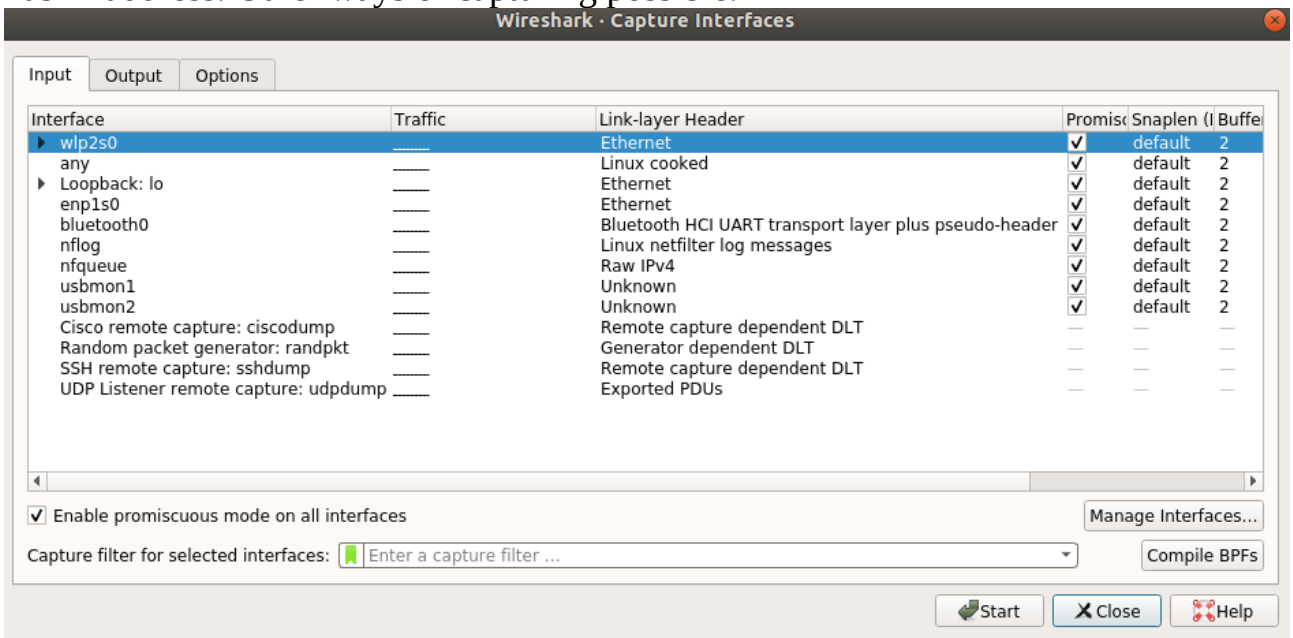
step-2: when show this enterface. Select yes and press enter.



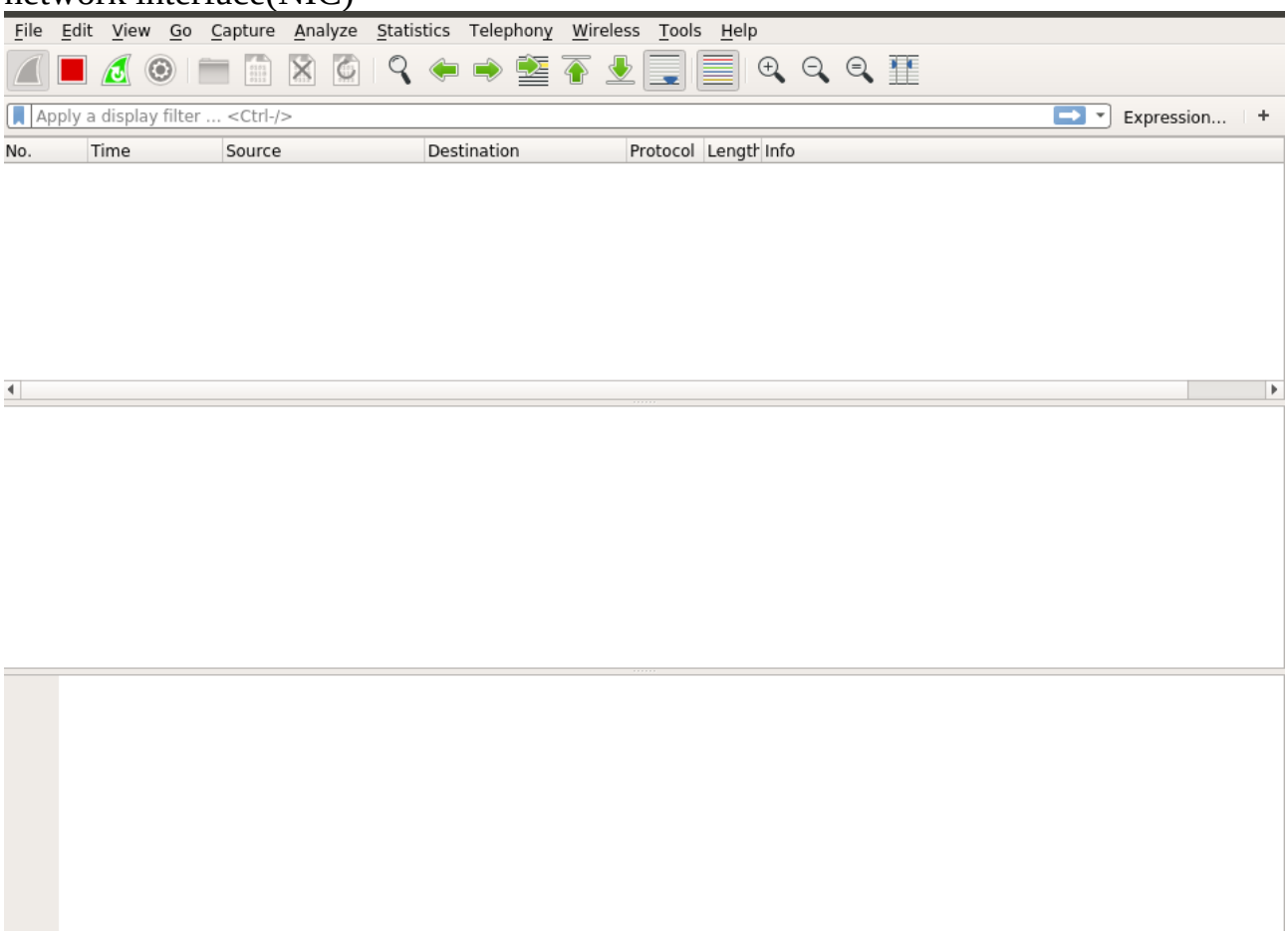
Wireshark usage:



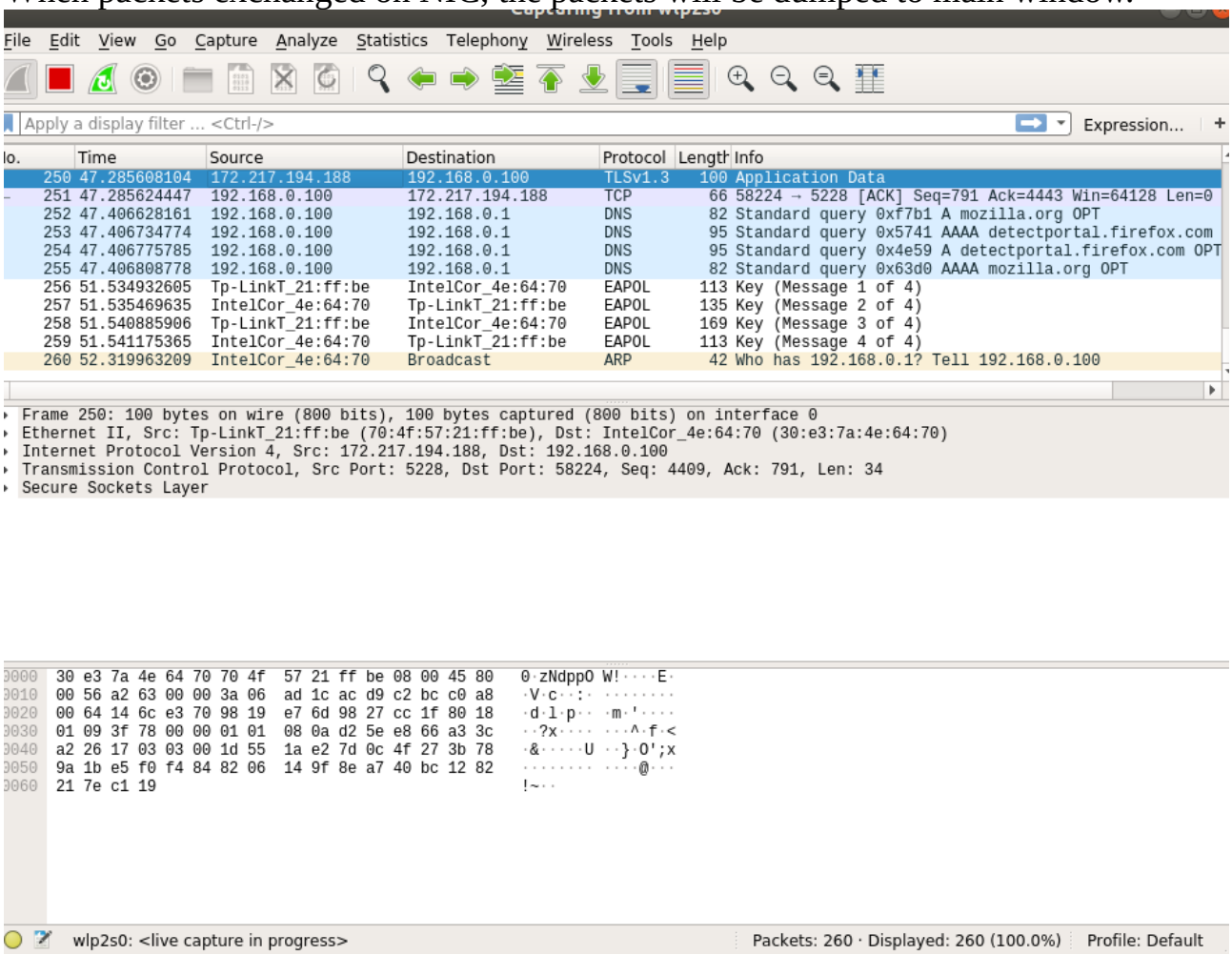
To capture: go to capture menu and select options. Start capturing on interface that has IP address. Other ways of capturing possible.



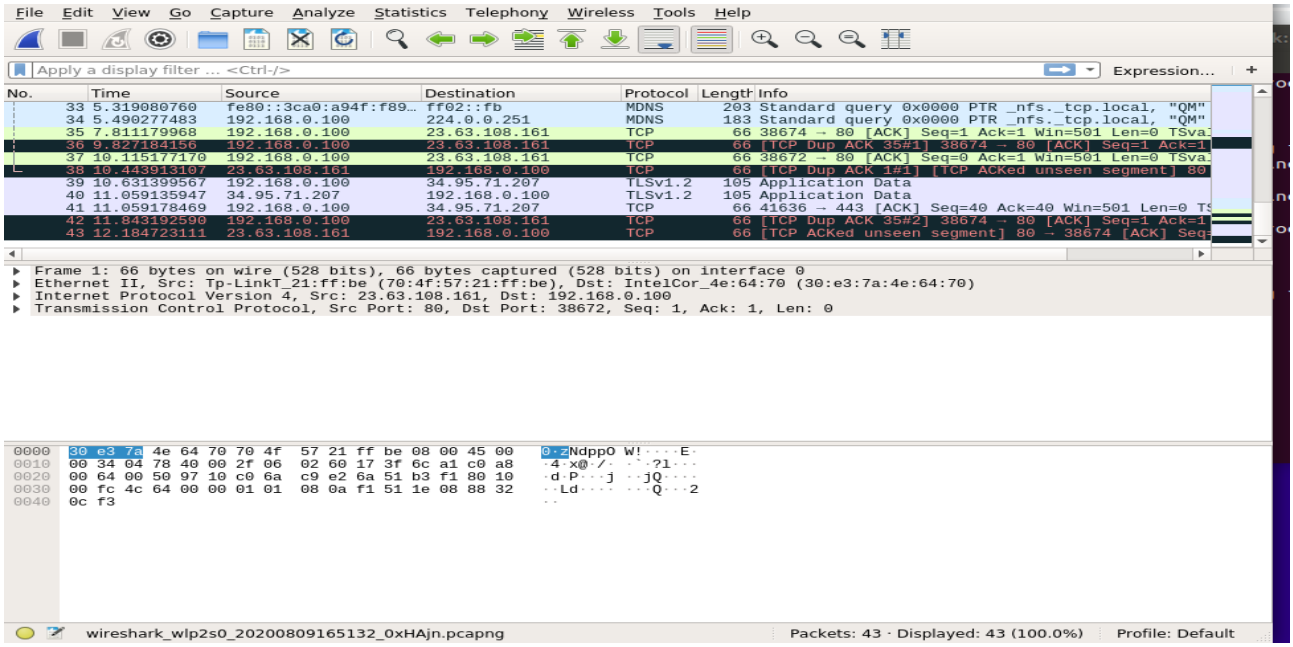
once the capturing starts, main window will be blank until the data is exchanged on network interface(NIC)



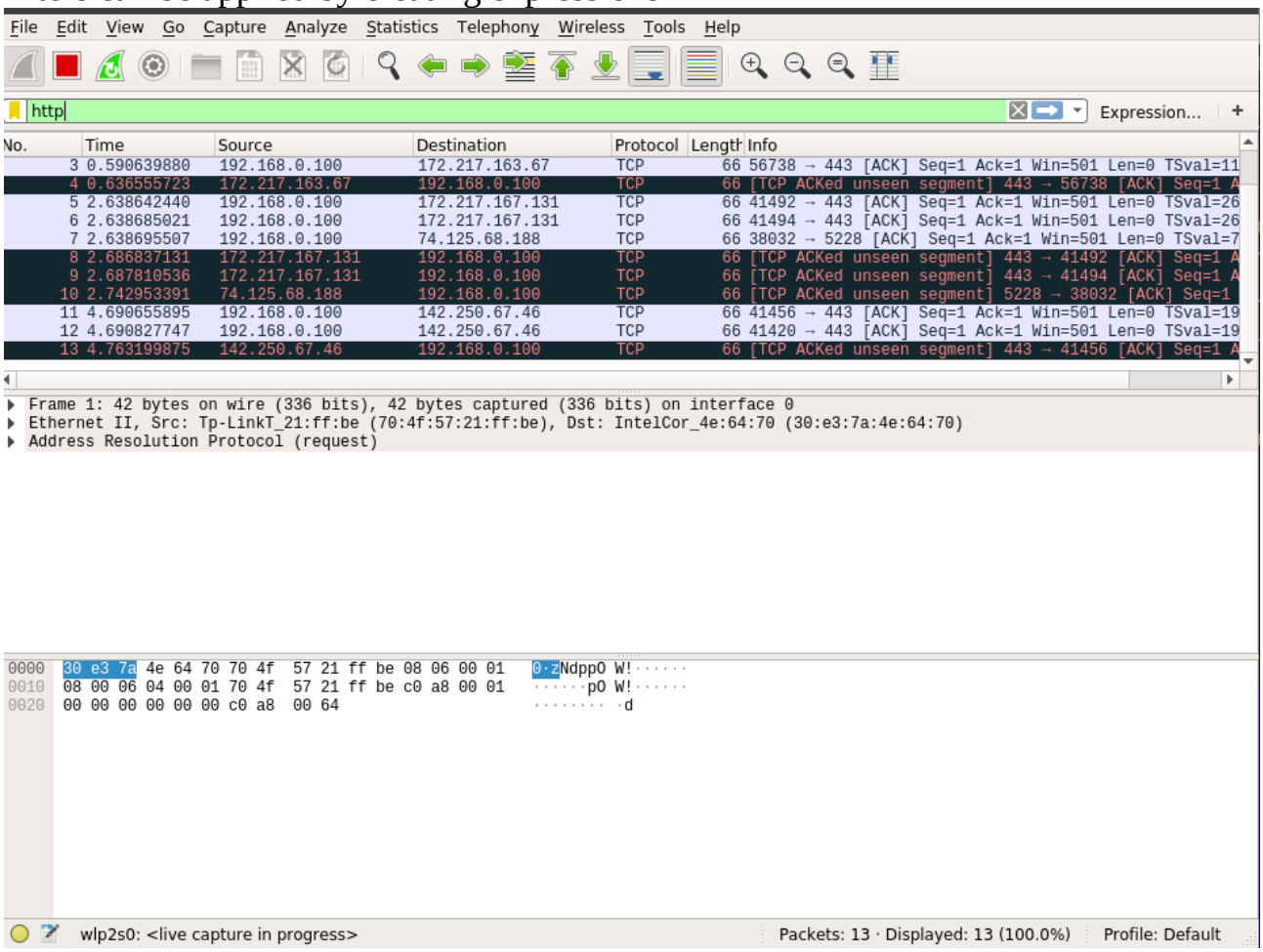
When packets exchanged on NIC, the packets will be dumped to main window.



Capturing can be stopped by clicking on stop the running capture button on the main toolbar.



Filter by entering the protocol or field name in apply a display and enter. Detailed filters can be applied by creating expressions

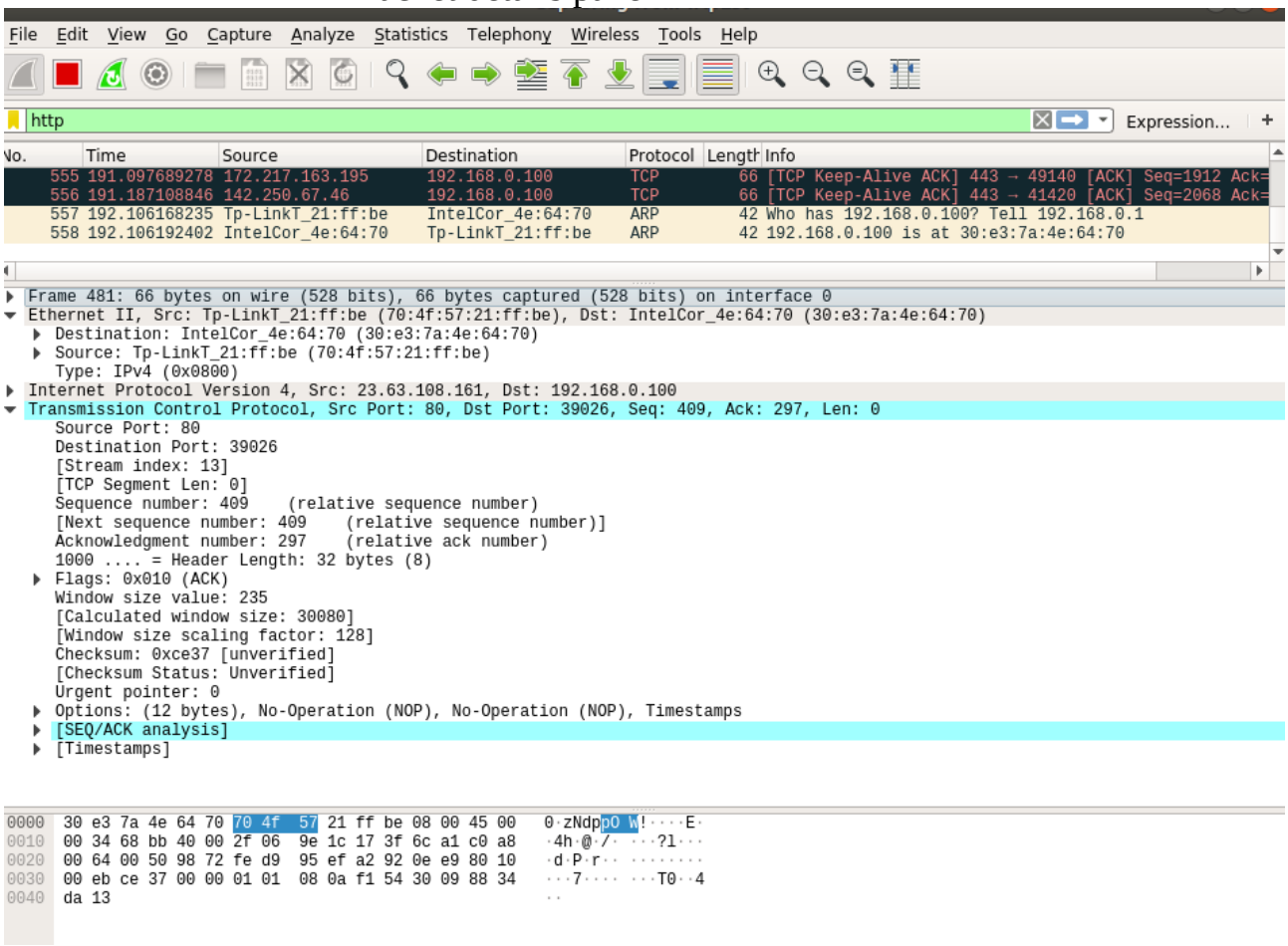


Protocol Analysis with wireshark:

- Packets and protocols can be analysed after capyure.
- Individual fields in protocols can be easily seen.
- Graphs and flow diagrams can be helpful in analysis

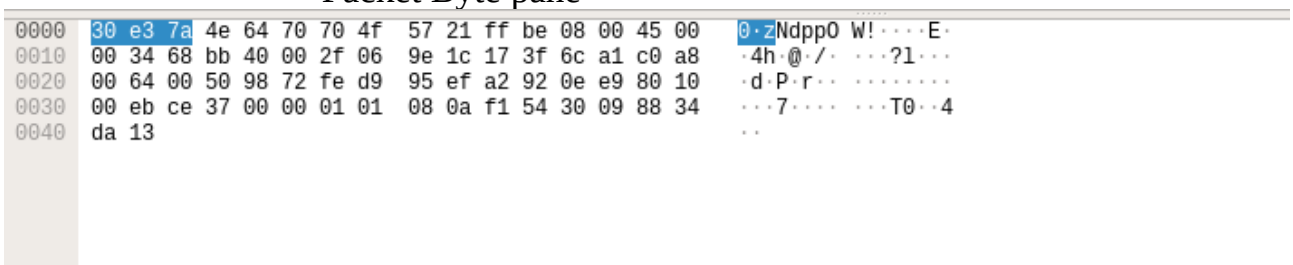
Analysis is performed manually

Packet details pane



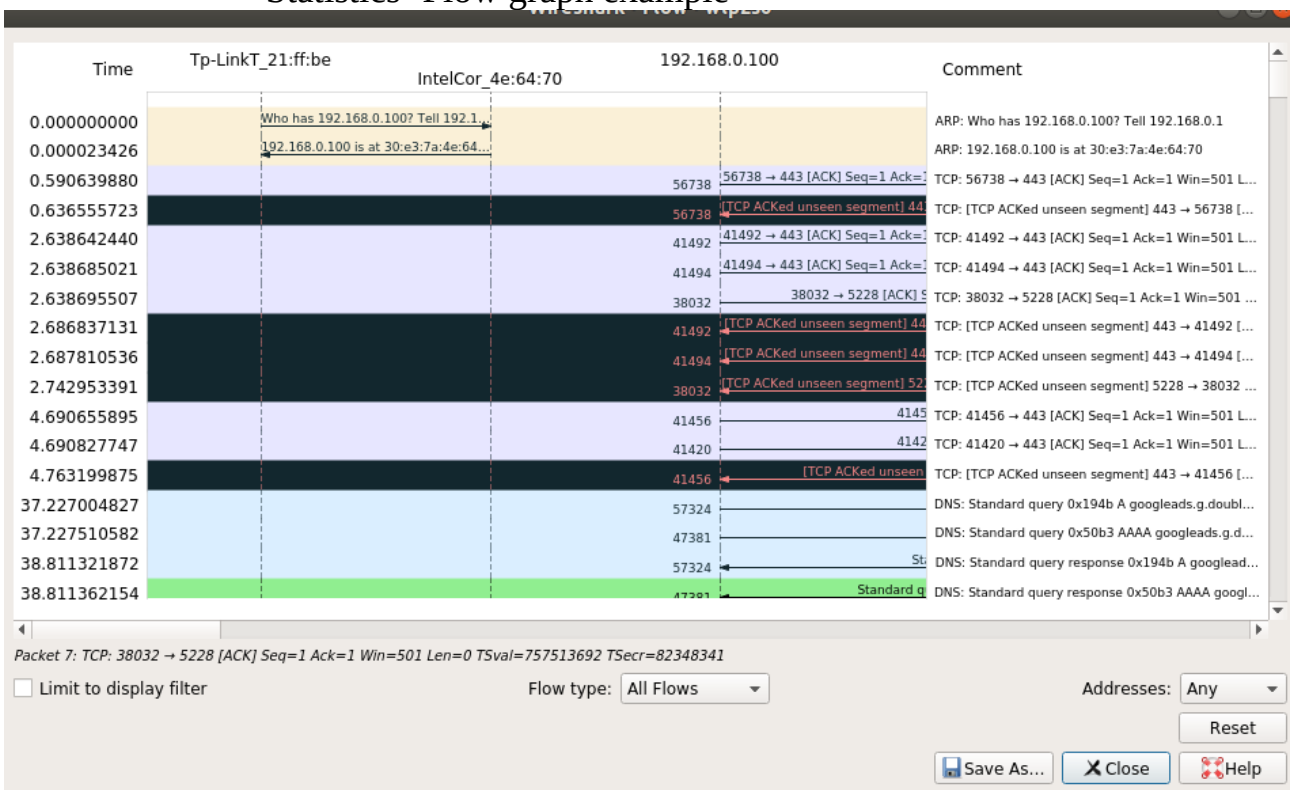
packet Byte pane consists of offset, Hex and ASCII fields.

Packet Byte pane



Tcp plots and flow graph are availabe in statistics menu.

Statistics- Flow graph example



Disscussion: In this lab we know about wireshark, how to install wireshark, how to use woreshark, and protocol and TCP analysis. I faced some problem butget help help internet for solve.