MAWLANA BHASHANI SCIENCE AND TECHNOLOGY UNIVERSITY

DEPARTMENT OF ICT

Lab Report No : 02

Course Code : ICT-3208

Course Title : Network Planning and Designing Lab

Lab Report Name : Wireshark Lab

Submitted by
Md. Faruk Hosen
ID : IT-17035
Session : 2016-2017
Year : 3rd Semester : 2nd

Submitted to
Nazrul Islam
Assistant Professor,
Department of ICT,MBSTU
Santosh,Tangail-1902

Date of Submission : 15 July 2020

Objective : 1. Wireshark basic and it's features.

2. How to work with wireshark.

3. Protocol Analysis with wireshark

Wireshark Lab

1. What is Wireshark? Why we use wireshark ?

Ans: Wireshark :

- Wireshark is a network protocol analyzer.
  - Captures network packets
  - displays packet data in details
- First released in 1998 by Geralds Combs as Ethereal
  - many contributors around the world.
- Open source and free software.
- Graphical alternative to tcpdump.

Why use wireshark : We use wireshark because -
Wireshark is a powerful tool for -

i. Troubleshooting network problems
ii. examining security problems
iii. debugging protocol implementations
iv. learning network protocols internals.

2. What are the main features of wireshark ?

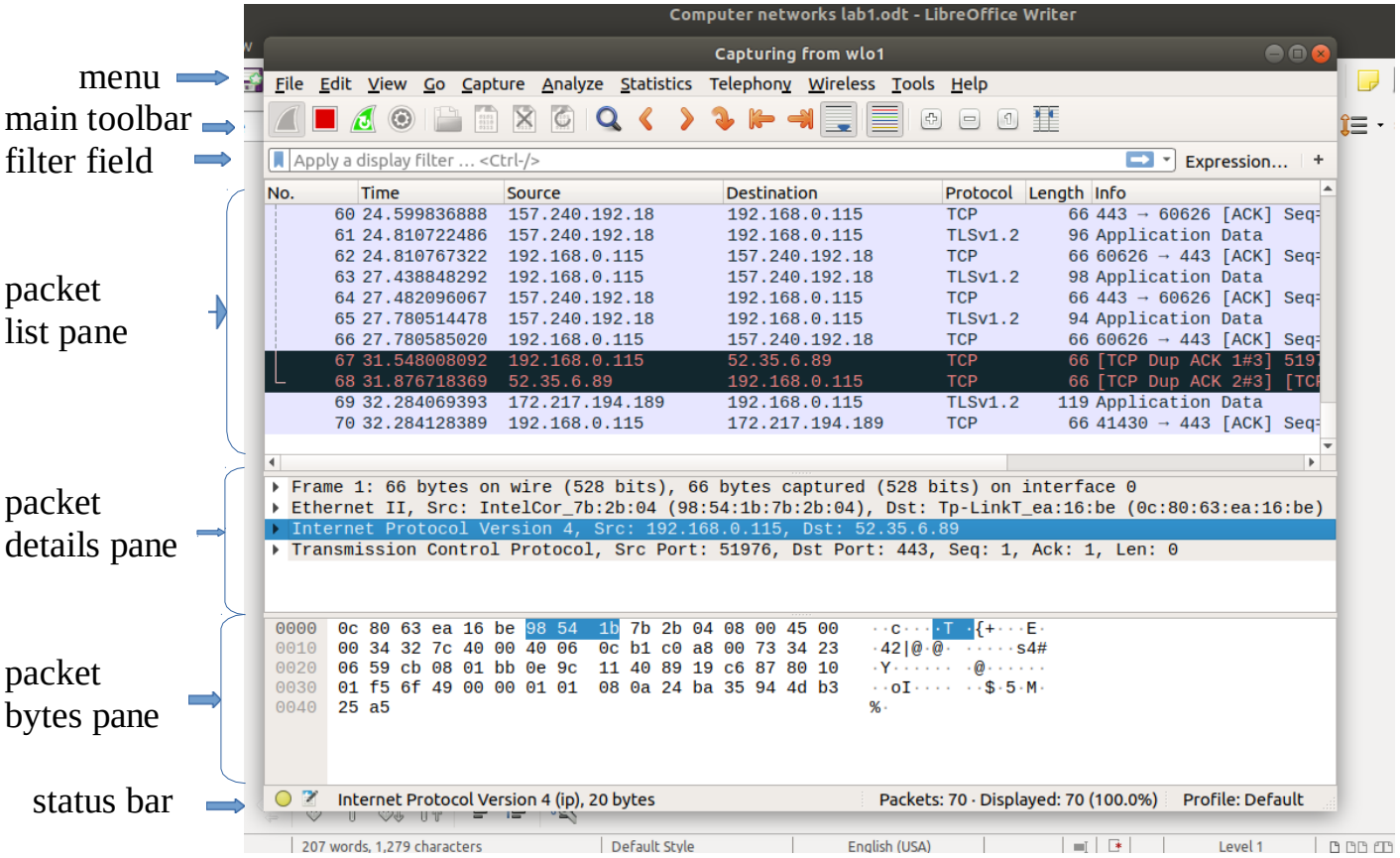
Ans : The main features of wireshark is :

i. Capture live traffic
   -data can be captured on wired or wireless medium.
   -numerous protocols can be captured and analyzed.

ii. Display packet in details
iii. Open files containing packet data captured.
-from other programs(tcpdump/winDump).
iv. Filtering is essential when dealing with lots of packets.
-filters can be applied on protocols,fields,values etc.
-filtering while capturing packets is possible.

3. Describe each field of Wireshark GUI window ?

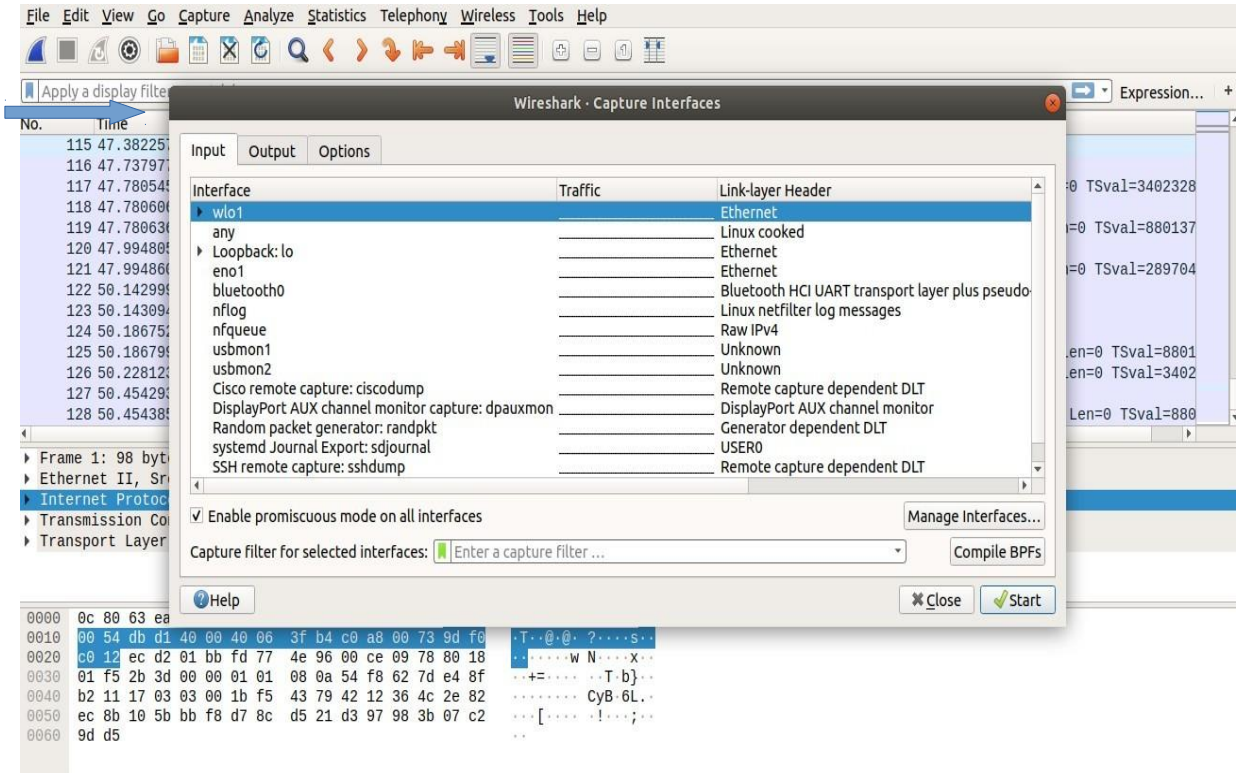
Ans : The each field of wireshark GUI main window is described below :



4. How to start capture in wireshark ?

Ans : To start capture, one can go to capture menu and select options . Now start capturing on interface that has an IP address. The capturing is also possible in another way .

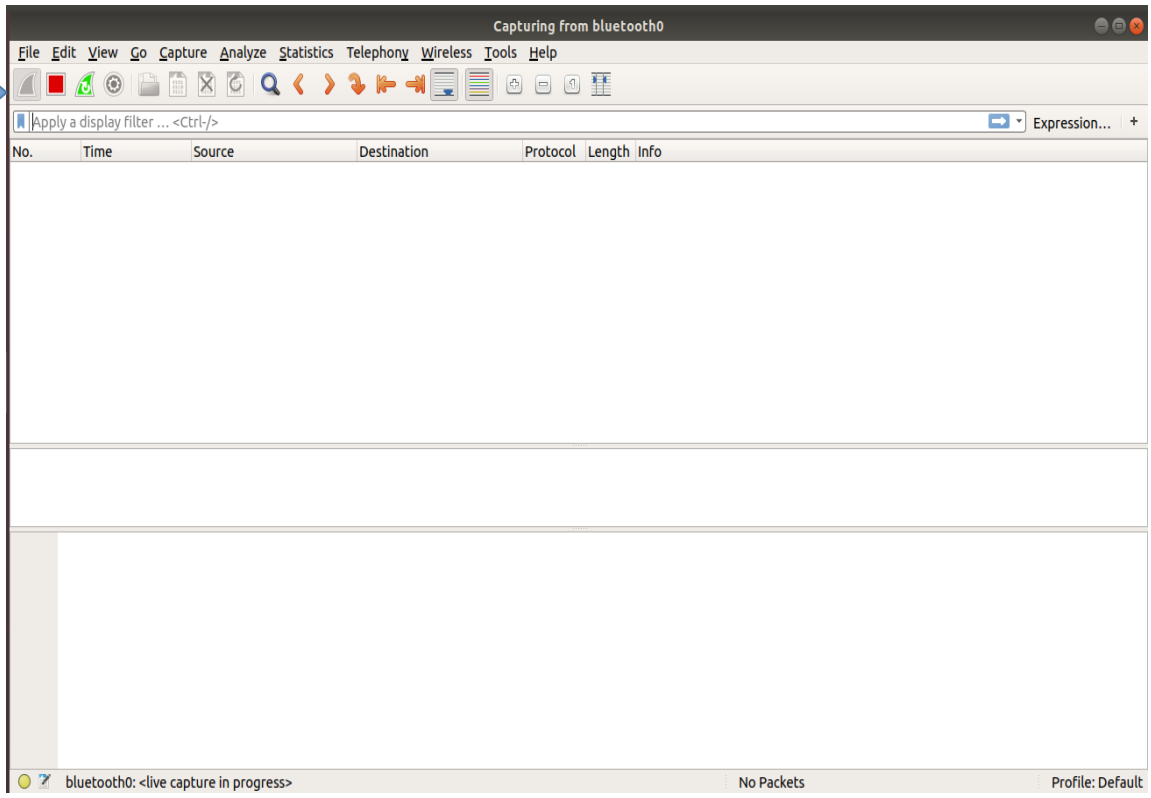
capture interfaces



5. When capturing starts, what is the situation of the wireshark main window ?

Ans: Once the capturing starts, the main window will be blank until the data is exchanged on Network Interface Card (NIC).

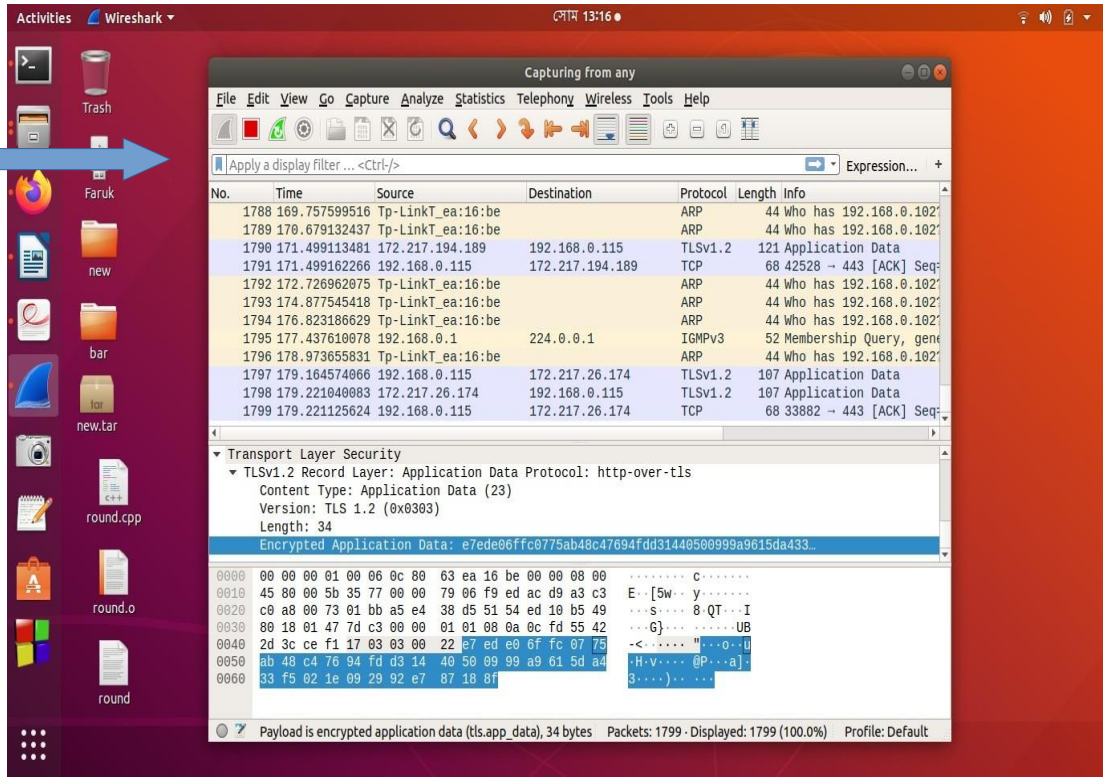
Capturing starts, so the icon is hide



6. When packets exchanged on NIC, what will be condition of wireshark GUI ?

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

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

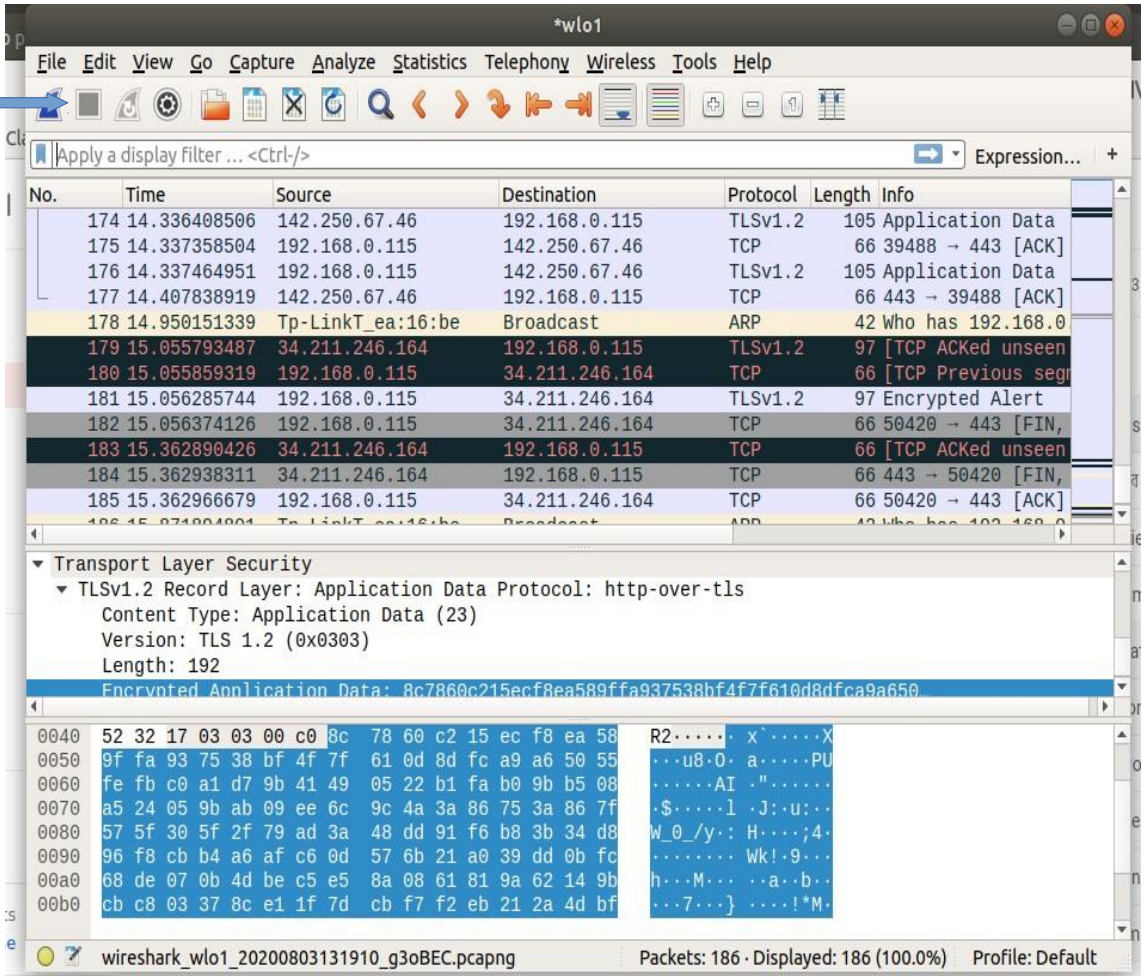


7. How to stop capturing packets on wireshark ?

Ans:

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

Stop capturing buttons on the main toolbar

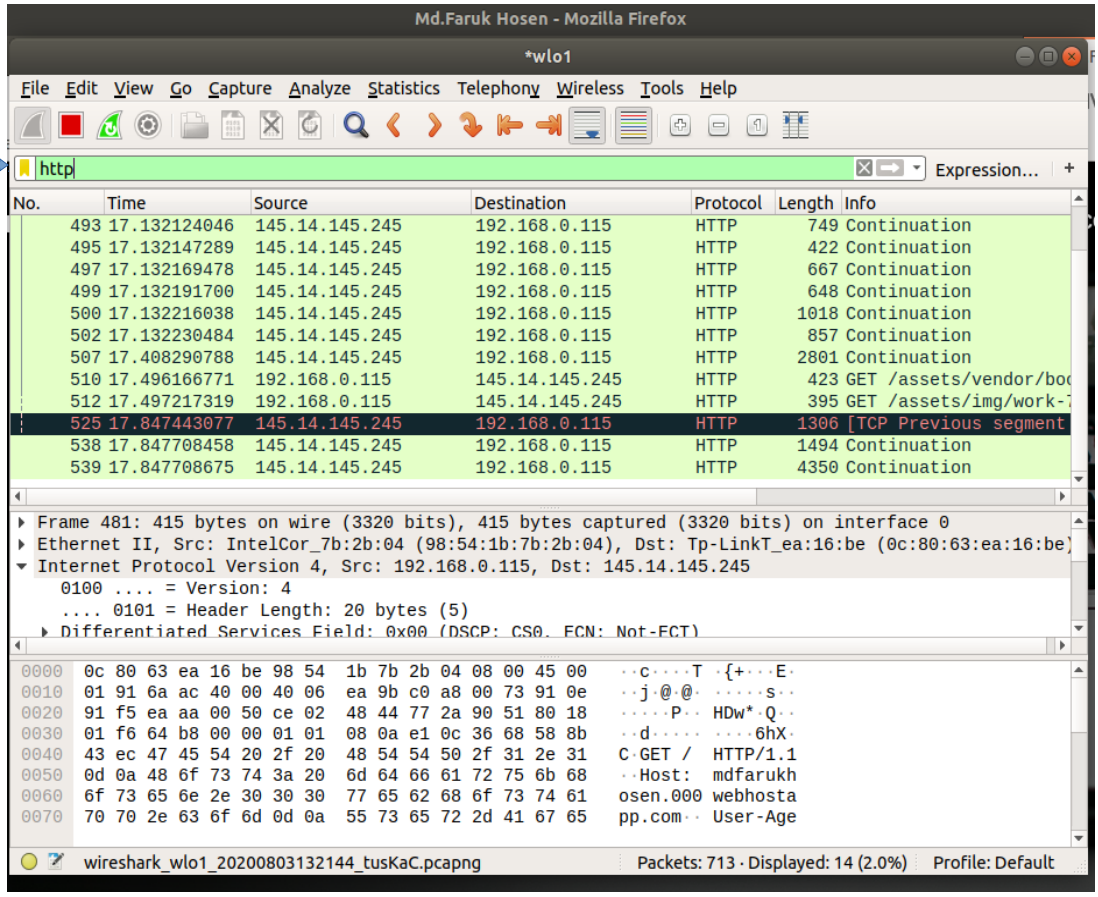


8. How to filtering protocol in wireshark ?

Ans : Filter by entering the protocol field name in Apply a display filter and press enter.

Detailed filters can be applied by creating expressions.

Filter by entering the protocol name in filter field



9. How to do protocol analysis with wireshark ?

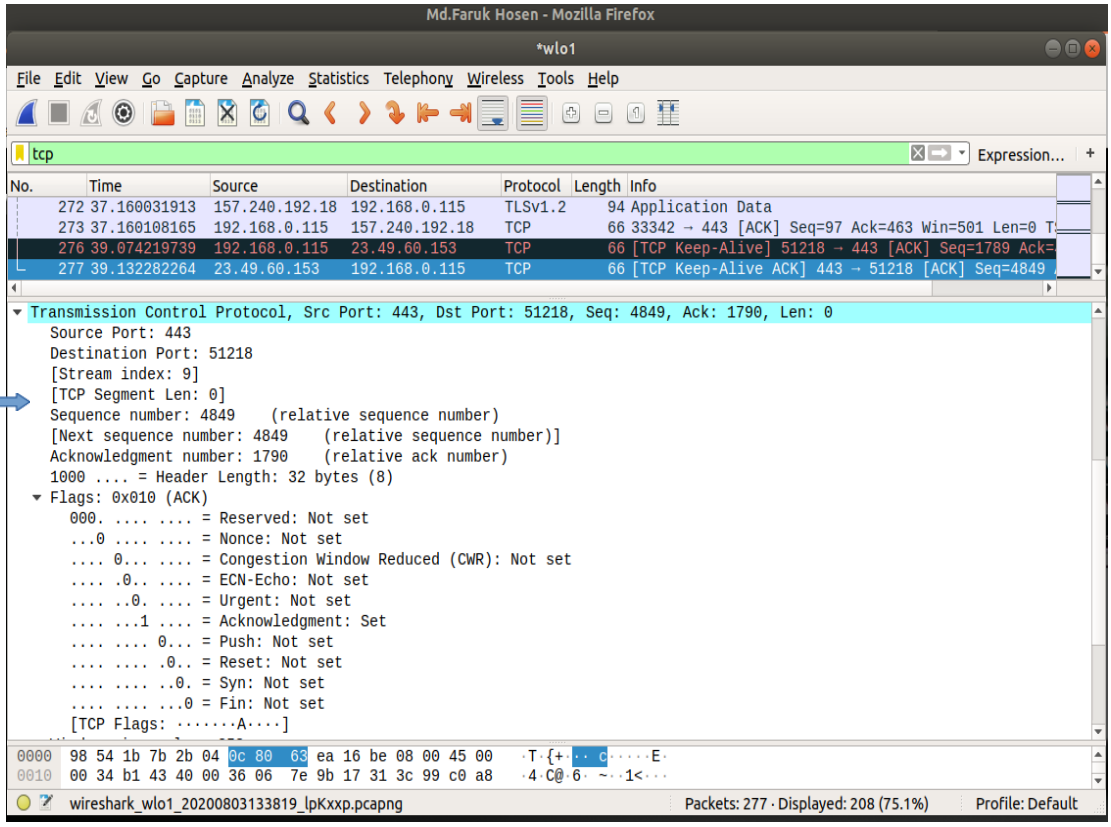
Ans: Protocol Analysis :

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

Analysis is performed manually. First of all, we see the TCP segment. The below example shows TCP segment with SYN and ACK fields set to 1.

<u>Protocol detail pane figure</u> :

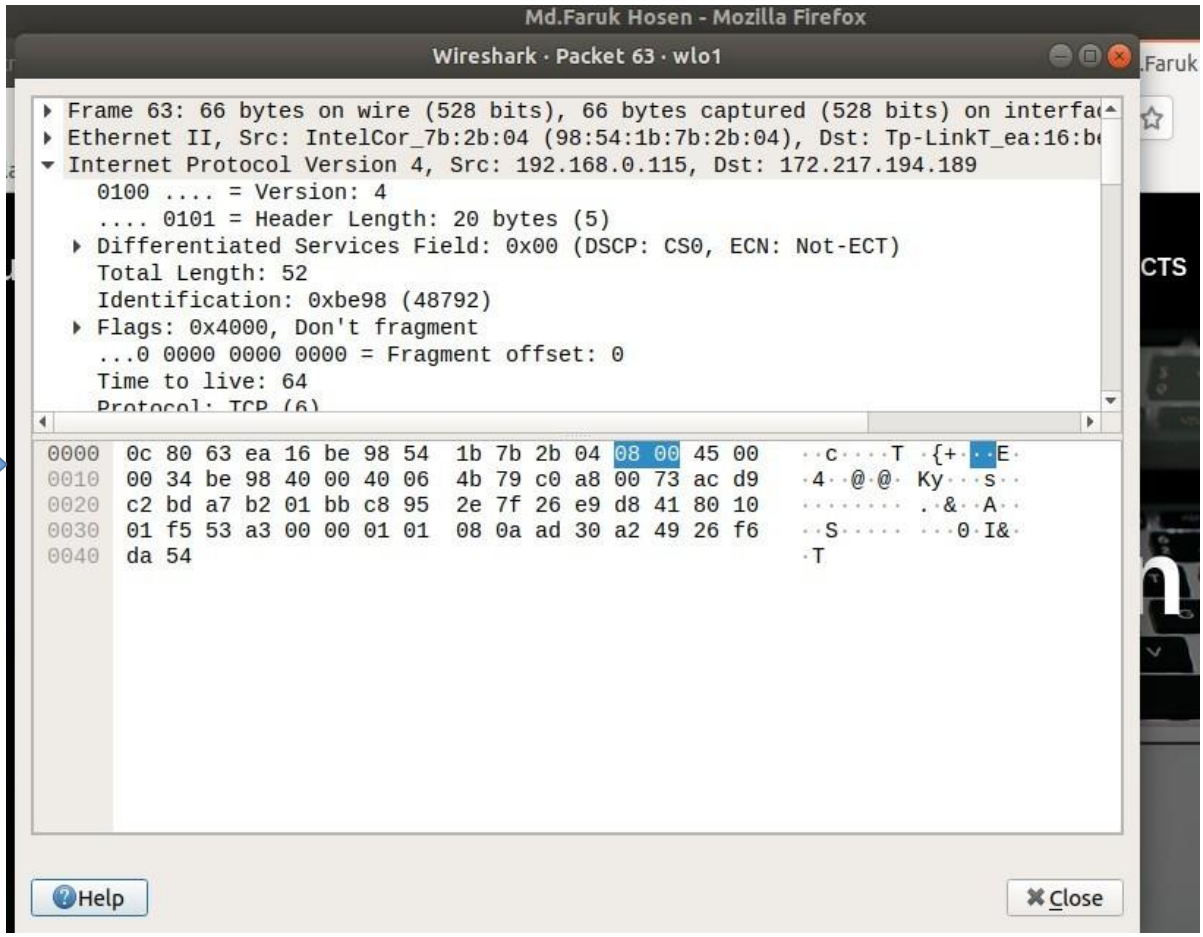
shows TCP segment with syn and ack fields set to 1



Then we see the packet byte pane consists of offset, Hex and Ascii fields.

Packet byte pane :

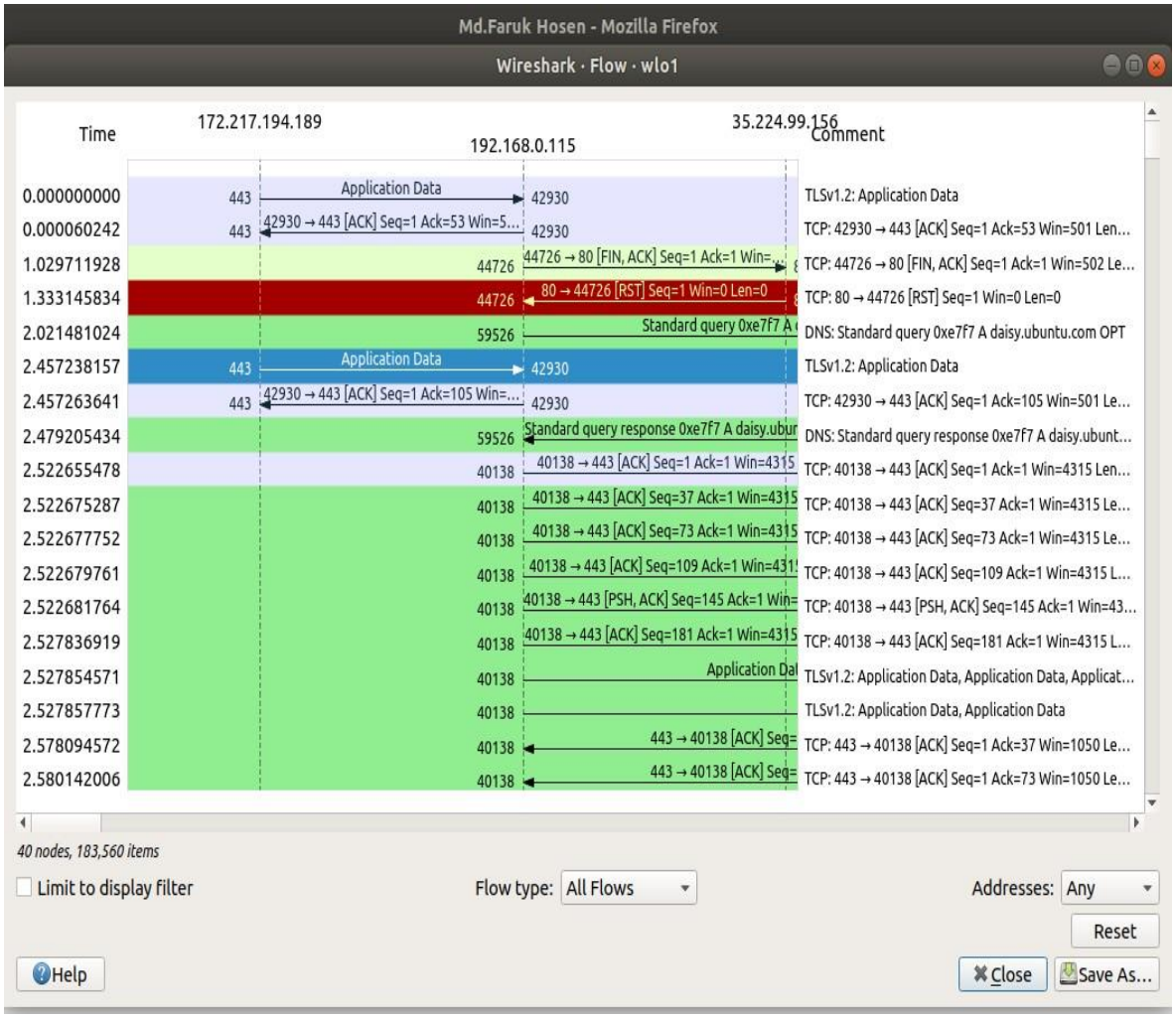
packet byte pane consists of offset, Hex and ASCII fields.



Then we see the statistics-flow graph example to analysis the protocol.

Flow Graph example :

In statistics menu, TCP plots and flow graphs are available



END