MAWLANA BHASHANI SCIENCE AND TECHNOLOGY UNIVERSITY

Santosh, Tangail -1902

Lab Report No : 02

Lab Report Name : Installing wireshark in Linux operating system

Course Name : Computer Networks Lab

Submitted by,

Name : Sabrin Afroz

ID : IT-17007

Session : 2016-17

Dept. of ICT, MBSTU.

Submitted to,

Nazrul Islam

Assistant Professor

Dept. of ICT, MBSTU.

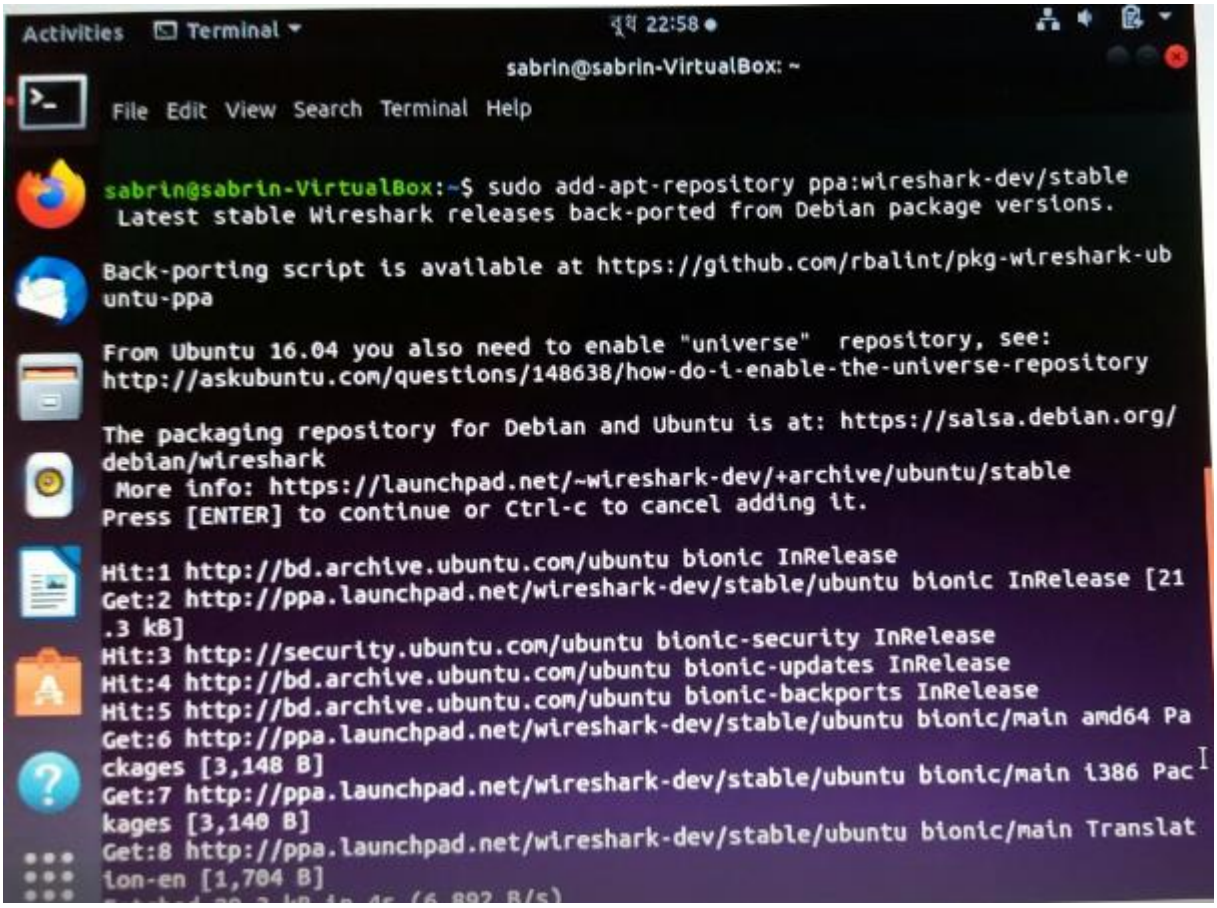
Installation of Wireshark

Wireshark is free and open source, cross platform. It captures network packets in real time & presents them in human readable format. Wireshark allows us to monitor the network packets up to microscopic level.

How to install Wireshark is given below step by step

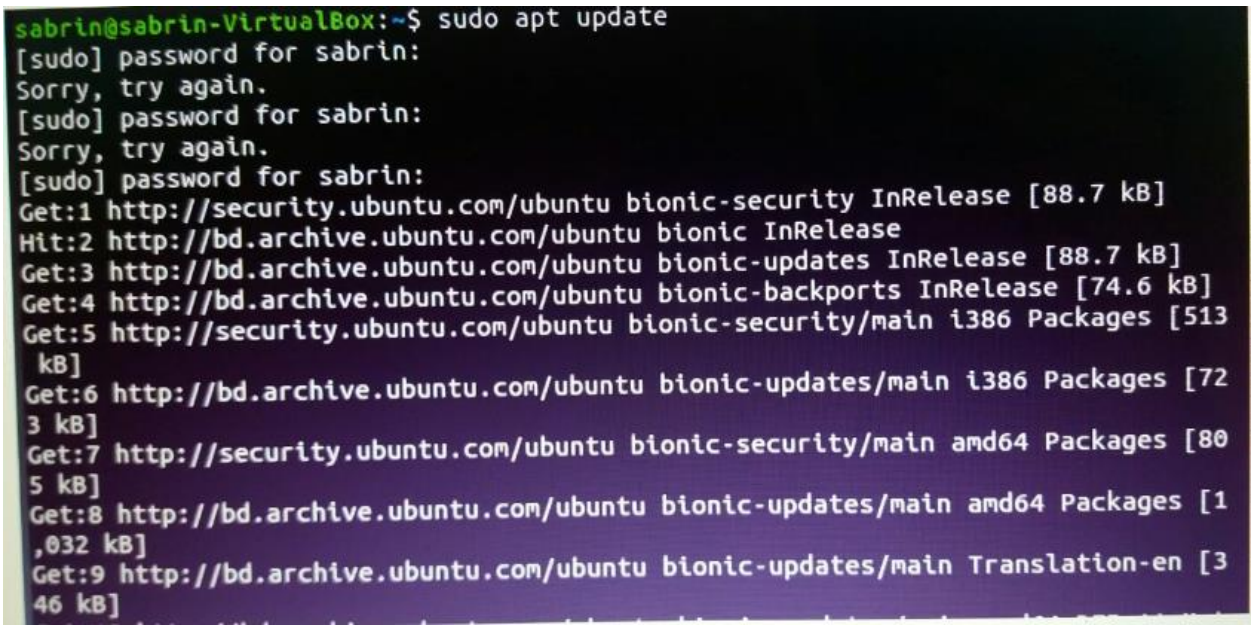
Step 1: Add the stable official PPA :

sudo add-apt-repository ppa:wireshark-dev/stable



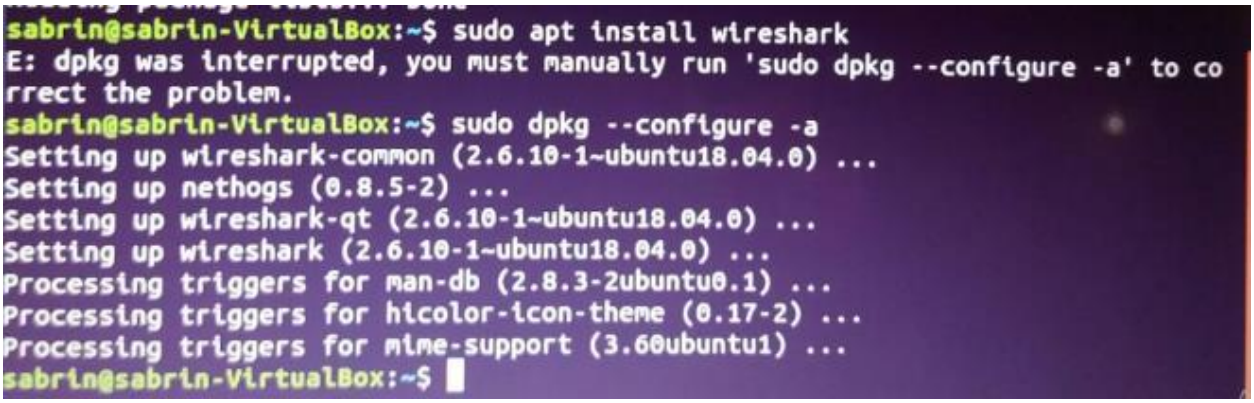
Step 2: Update the repository :

sudo apt-get update



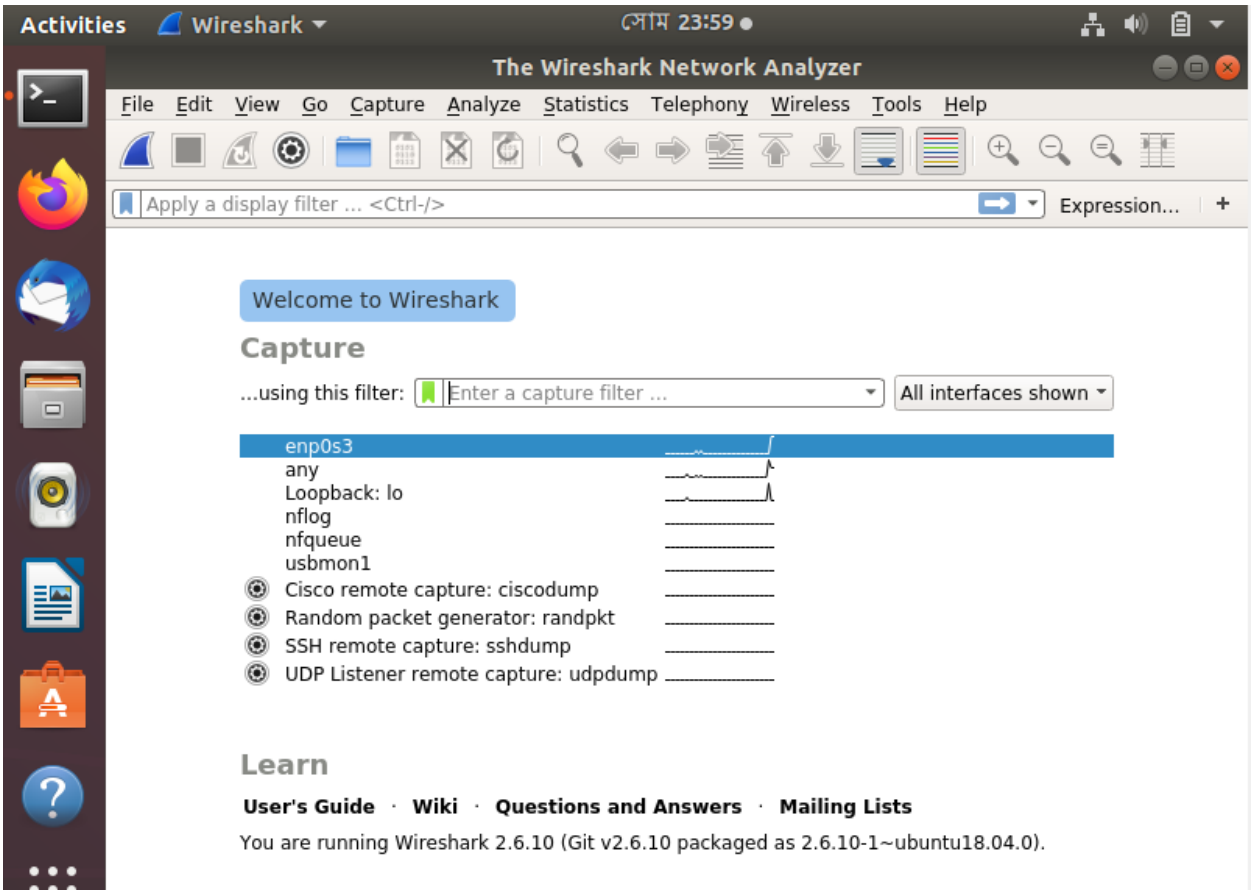
Step 3: Install wireshark :

sudo apt-get install wireshark

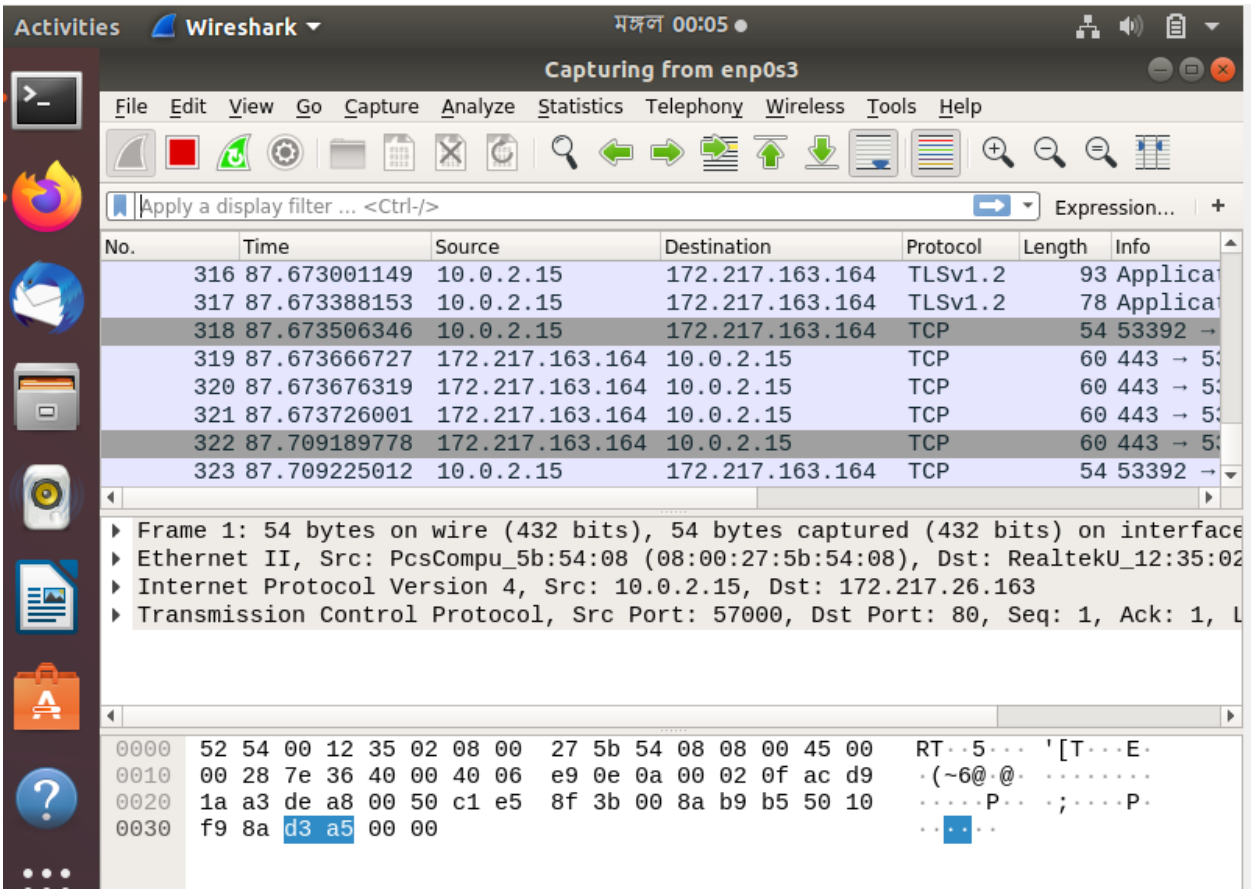


Step 4: Run wireshark

sudo wireshark

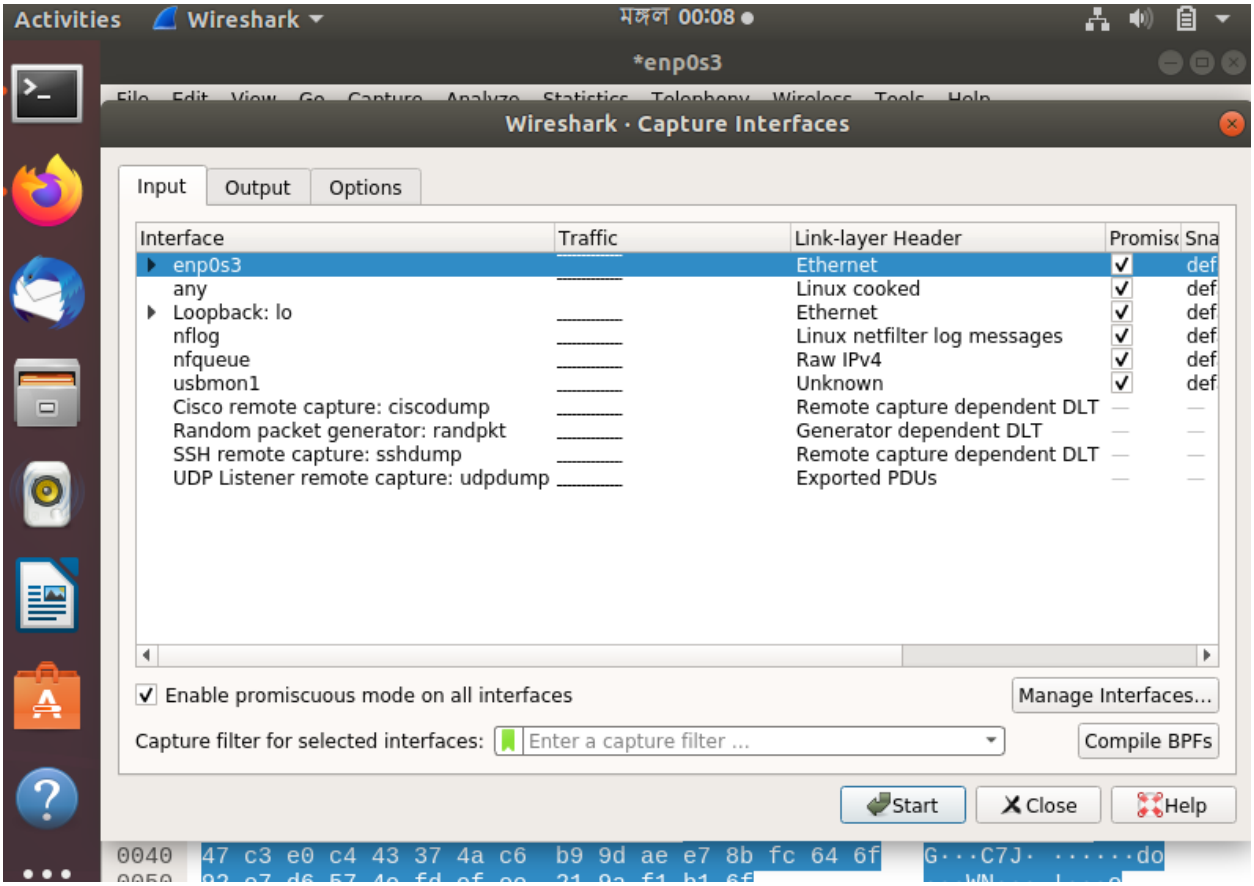


Main Window :

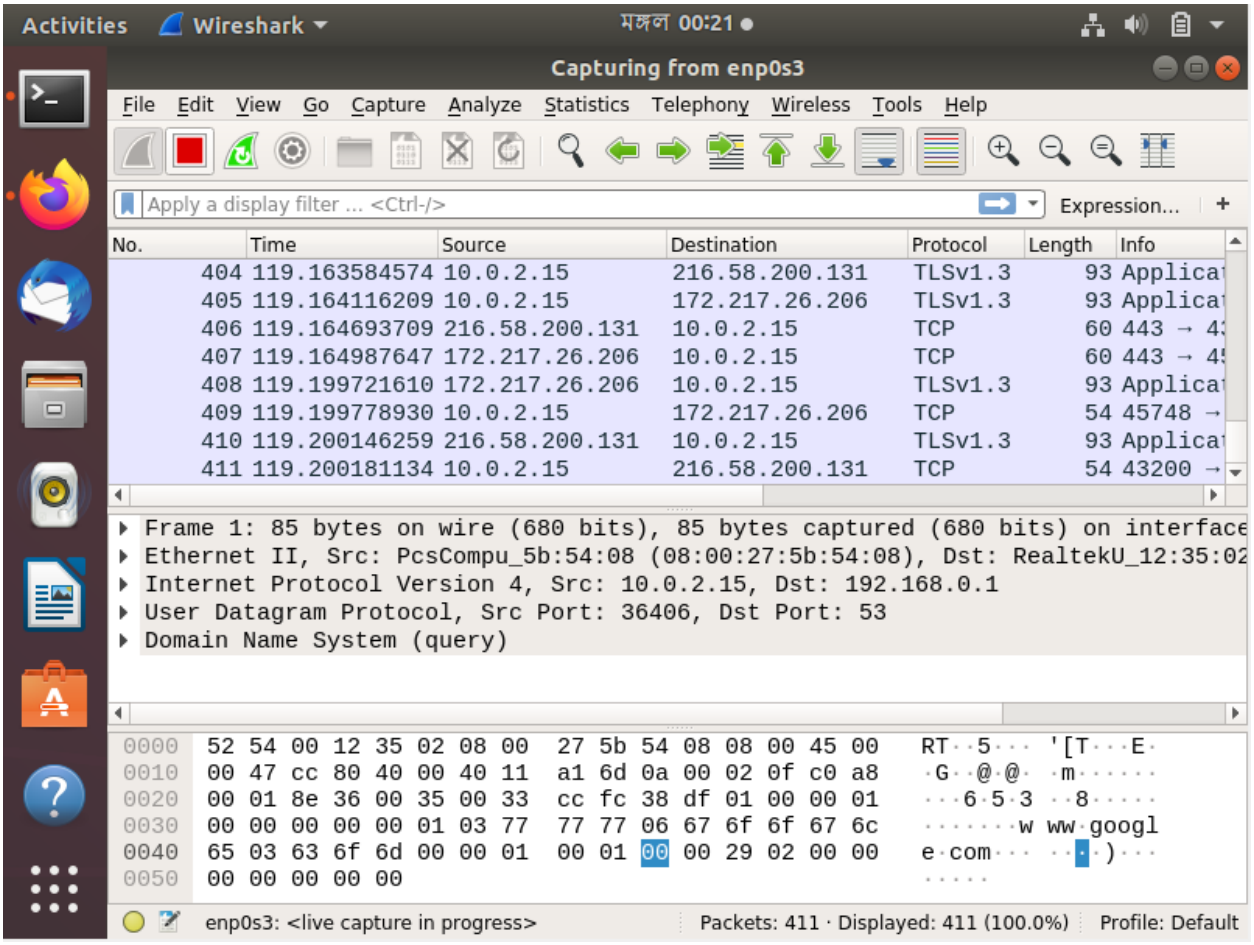

Activities
Wireshark
मङ्गल 00:05
Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
316 87.673001149 10.0.2.15 172.217.163.164 TLSv1.2 93 Applica
317 87.673388153 10.0.2.15 172.217.163.164 TLSv1.2 78 Applica
318 87.673506346 10.0.2.15 172.217.163.164 TCP 54 53392 →
319 87.673666727 172.217.163.164 10.0.2.15 TCP 60 443 → 5
320 87.673676319 172.217.163.164 10.0.2.15 TCP 60 443 → 5
321 87.673726001 172.217.163.164 10.0.2.15 TCP 60 443 → 5
322 87.709189778 172.217.163.164 10.0.2.15 TCP 60 443 → 5
323 87.709225012 10.0.2.15 172.217.163.164 TCP 54 53392 →
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface
Ethernet II, Src: PcsCompu_5b:54:08 (08:00:27:5b:54:08), Dst: RealtekU_12:35:02
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.217.26.163
Transmission Control Protocol, Src Port: 57000, Dst Port: 80, Seq: 1, Ack: 1, L
0000 52 54 00 12 35 02 08 00 27 5b 54 08 08 00 45 00
0010 00 28 7e 36 40 00 40 06 e9 0e 0a 00 02 0f ac d9
0020 1a a3 de a8 00 50 c1 e5 8f 3b 00 8a b9 b5 50 10
0030 f9 8a d3 a5 00 00

Starting Capture :

To capture, go to capture menu and select options (Capture Interfaces). Start capturing on interface that has IP address.

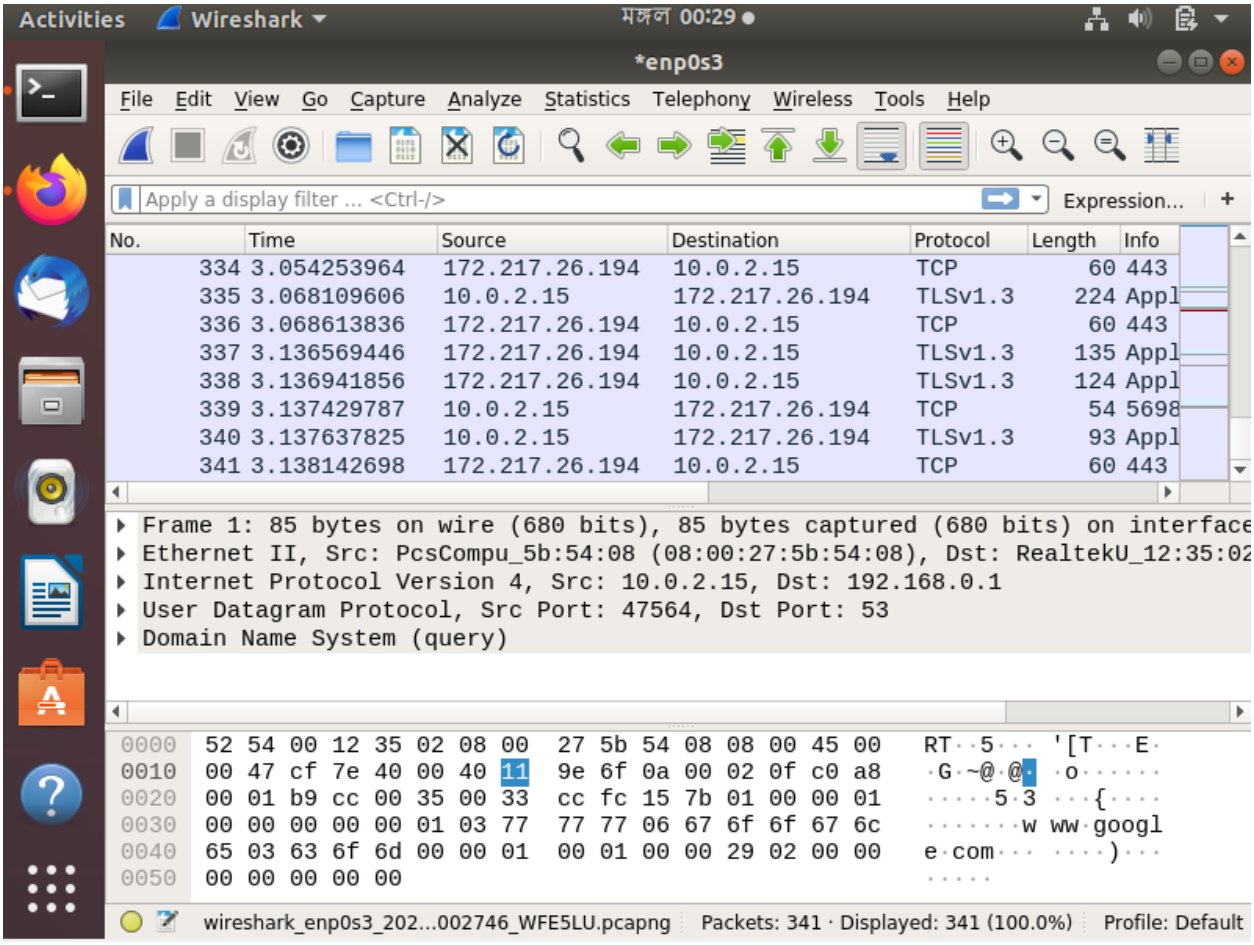


Once the capturing starts, main window will be blank until the data is exchanged on network interface(NIC). When packets exchanged on NIC, the packets will be dumped to main window.



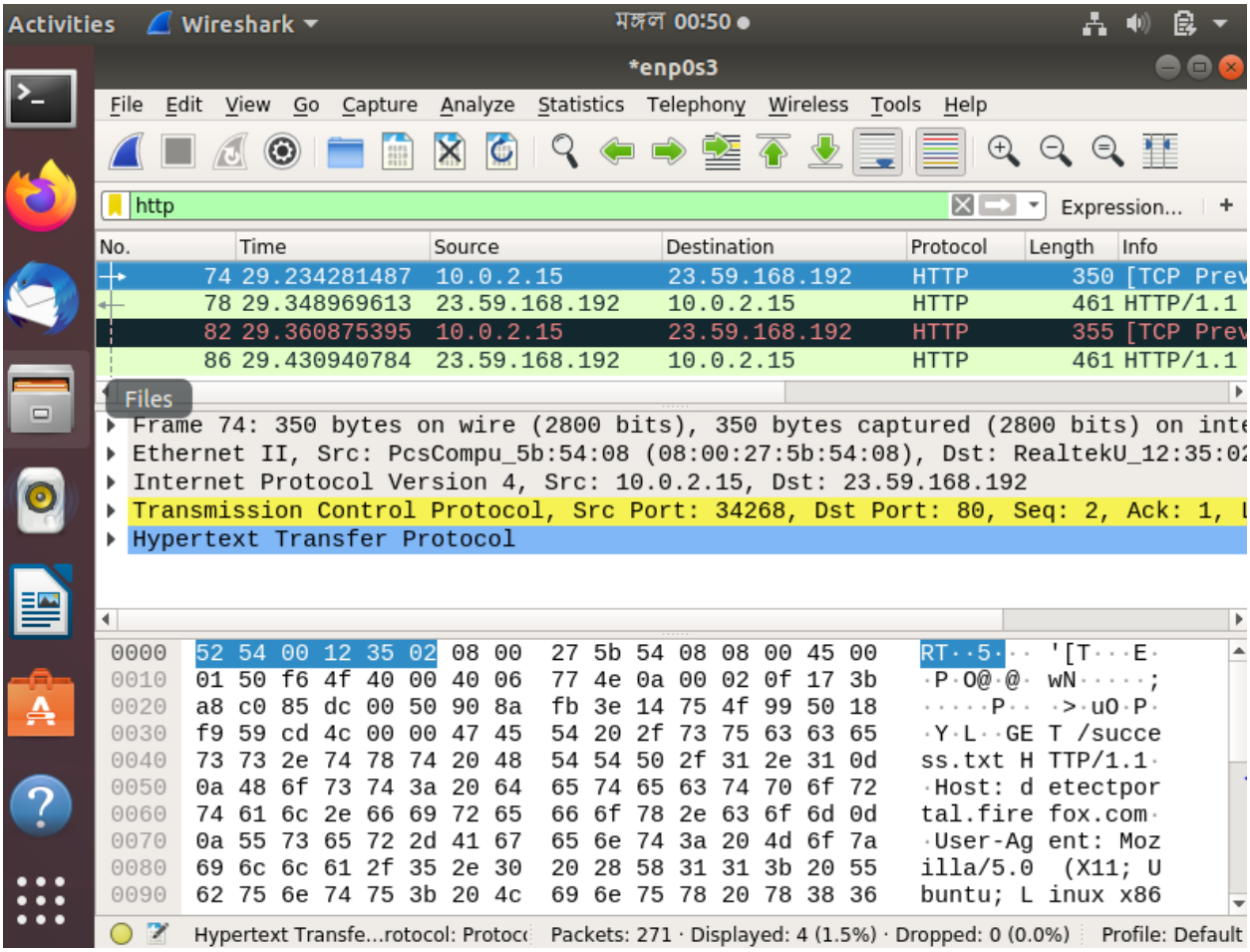
Stopping Capture :

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



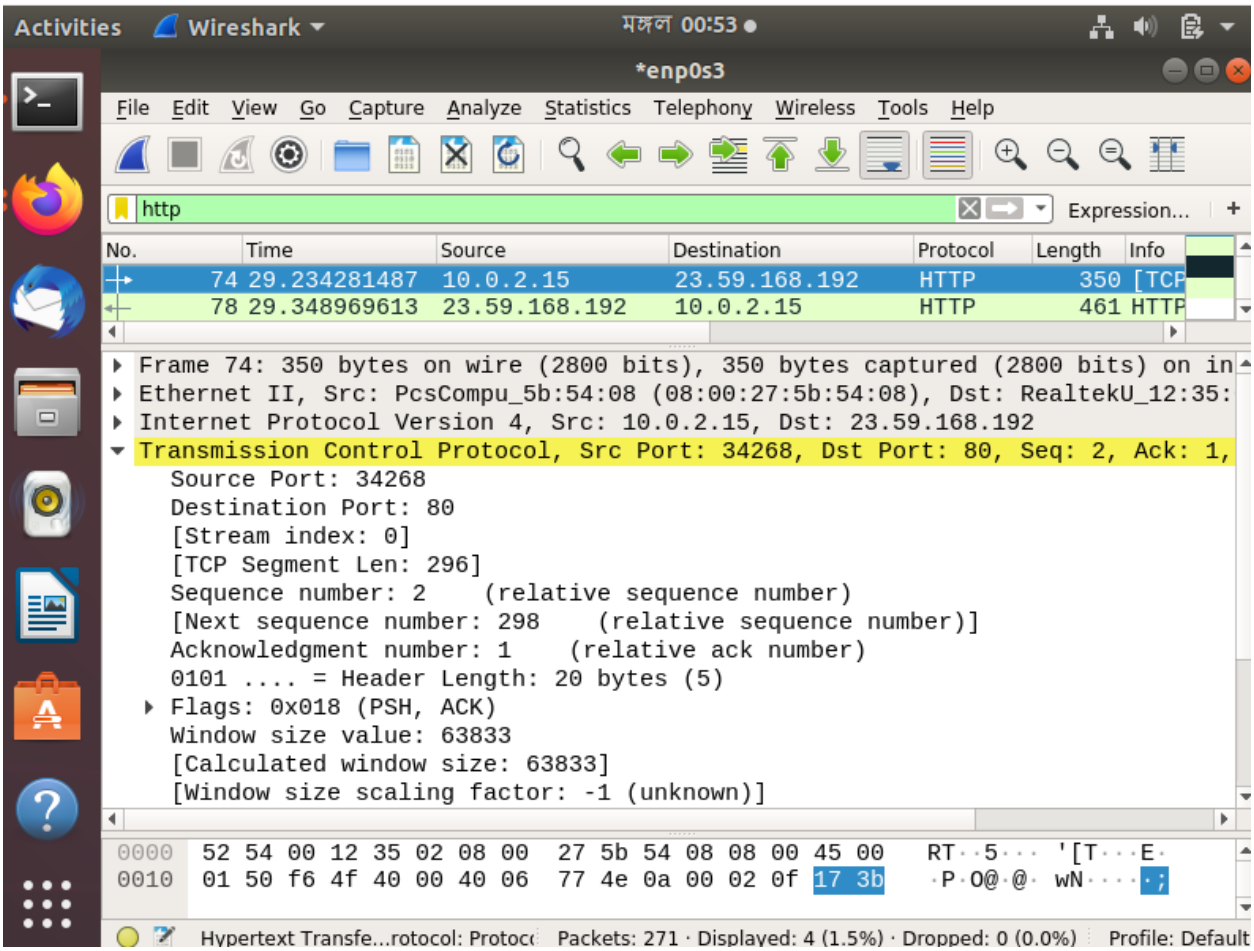
Filtering :

Filter by entering the protocol or field name in apply a display filter and enter.

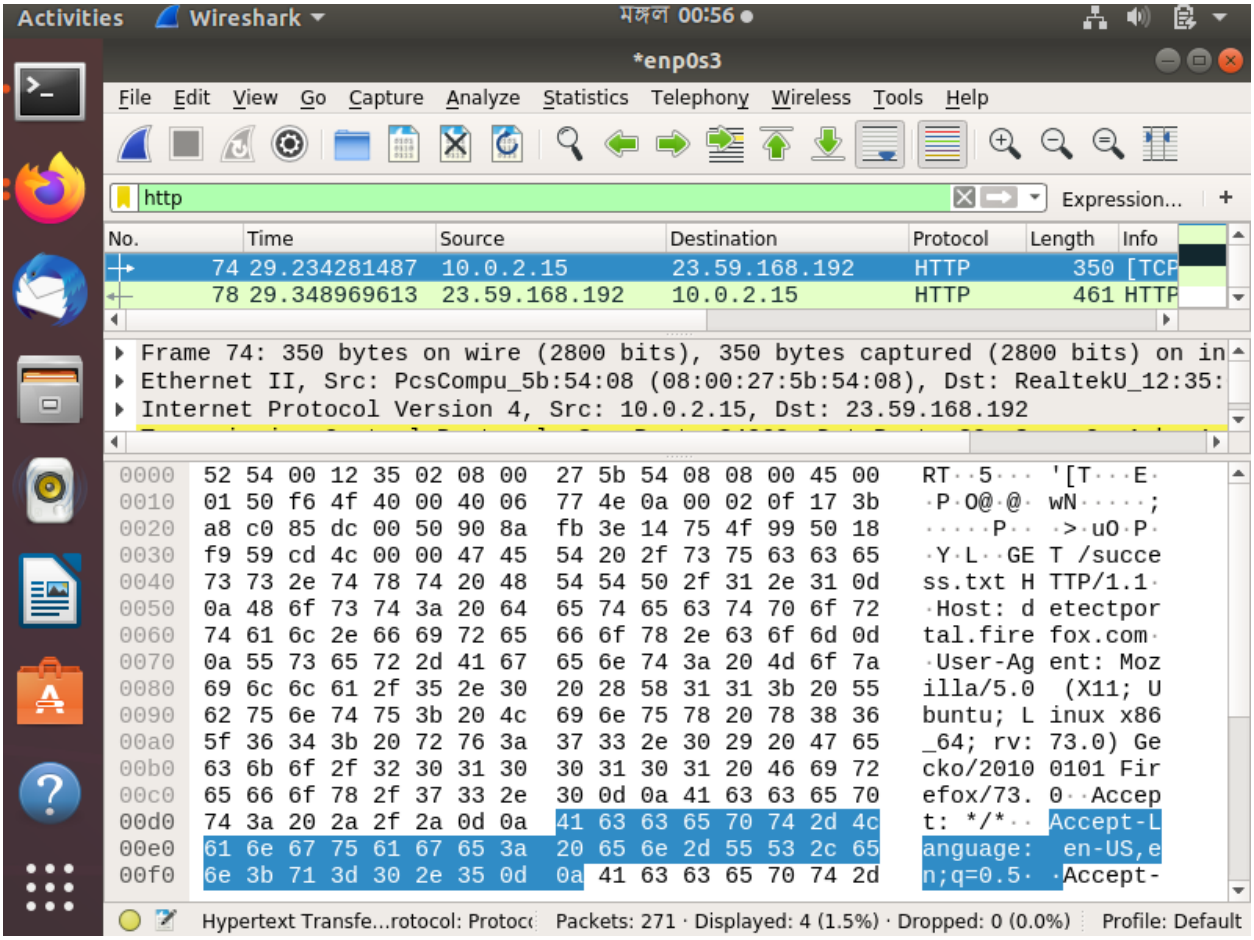


Protocol analysis :

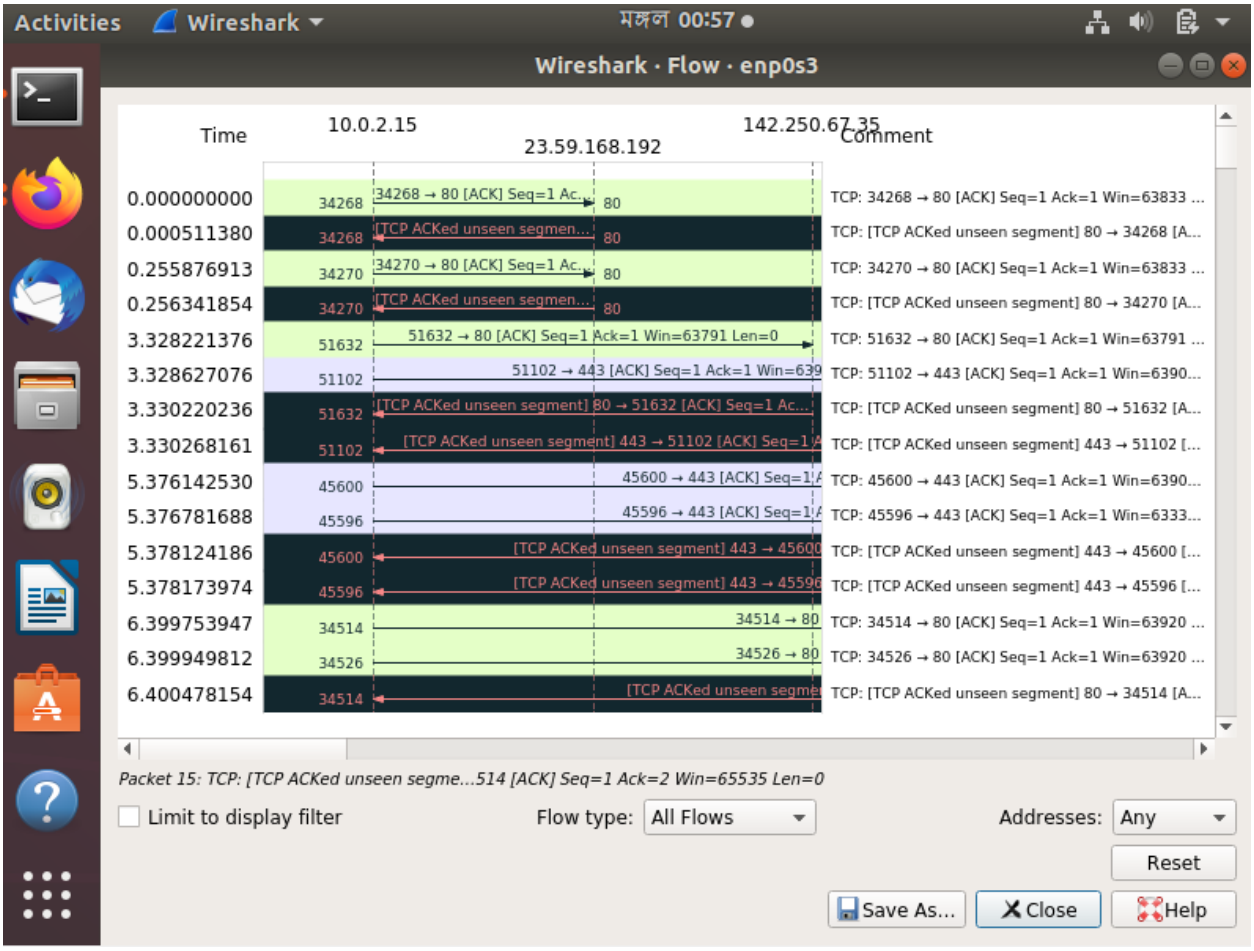
Packet details pane : Analysis is performed manually. Example – shows TCP segment.



Packet Byte Pane : Packet Byte Pane consists of offset, Hex, and ASCII fields.



Statistics – Flow Graph Example :



Conclusion : Wireshark can help troubleshoot include dropped packets, latency issues, and malicious activity on our network. It lets us put our 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.