

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.

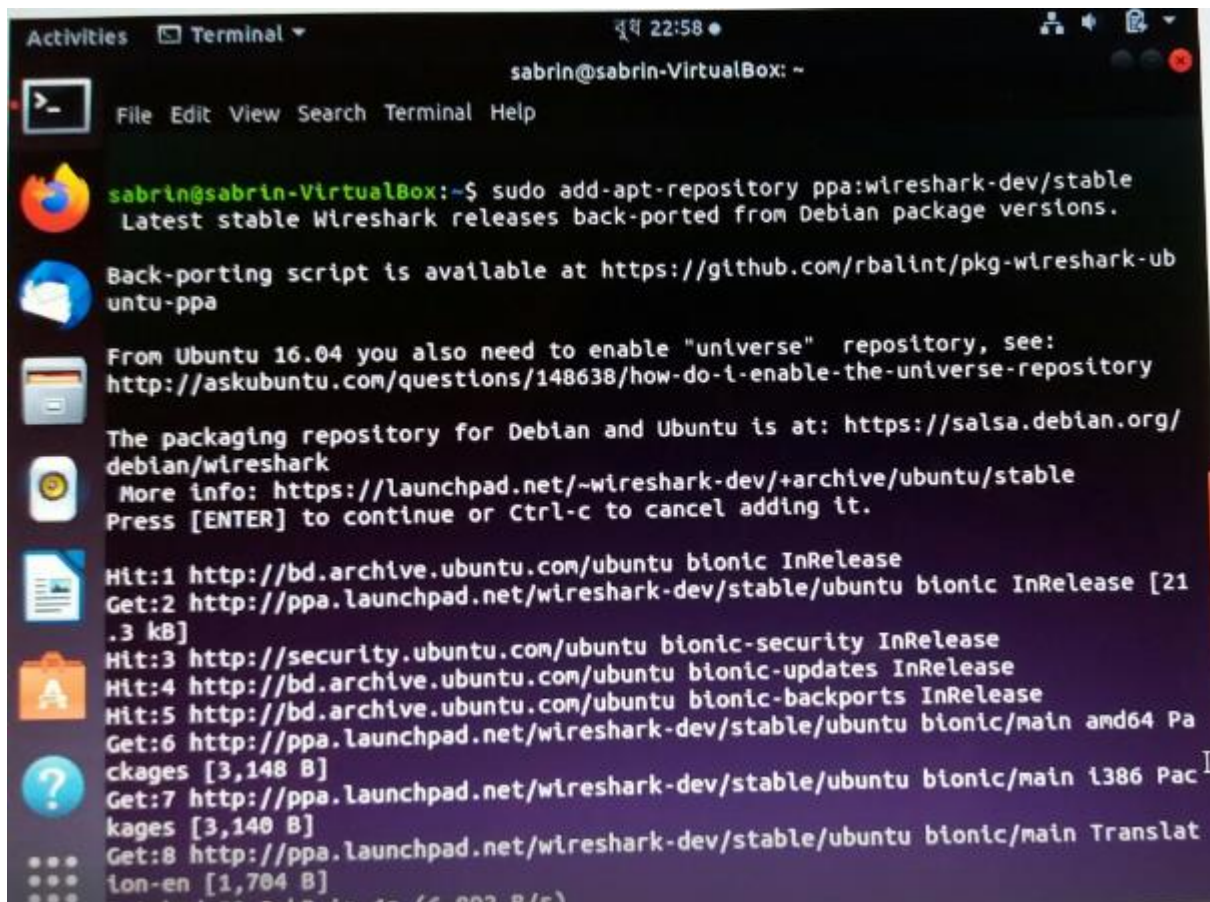
Installation of Wireshark

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
```



```
Activities  Terminal  22:58  sabrin@sabrin-VirtualBox: ~
File Edit View Search Terminal Help

sabrin@sabrin-VirtualBox:~$ sudo add-apt-repository ppa:wireshark-dev/stable
Latest stable Wireshark releases back-ported from Debian package versions.

Back-porting script is available at https://github.com/rbalint/pkg-wireshark-ubuntu-ppa

From Ubuntu 16.04 you also need to enable "universe" repository, see:
http://askubuntu.com/questions/148638/how-do-i-enable-the-universe-repository

The packaging repository for Debian and Ubuntu is at: https://salsa.debian.org/debian/wireshark
More info: https://launchpad.net/~wireshark-dev/+archive/ubuntu/stable
Press [ENTER] to continue or Ctrl-c to cancel adding it.

Hit:1 http://bd.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu bionic InRelease [21.3 kB]
Hit:3 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:4 http://bd.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:5 http://bd.archive.ubuntu.com/ubuntu bionic-backports InRelease
Get:6 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu bionic/main amd64 Packages [3,148 B]
Get:7 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu bionic/main i386 Packages [3,140 B]
Get:8 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu bionic/main Translation-en [1,704 B]
```

Step 2: Update the repository :

`sudo apt-get update`

```
sabrin@sabrin-VirtualBox:~$ sudo apt update
[sudo] password for sabrin:
Sorry, try again.
[sudo] password for sabrin:
Sorry, try again.
[sudo] password for sabrin:
Get:1 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Hit:2 http://bd.archive.ubuntu.com/ubuntu bionic InRelease
Get:3 http://bd.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:4 http://bd.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Get:5 http://security.ubuntu.com/ubuntu bionic-security/main i386 Packages [513
kB]
Get:6 http://bd.archive.ubuntu.com/ubuntu bionic-updates/main i386 Packages [72
3 kB]
Get:7 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages [80
5 kB]
Get:8 http://bd.archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [1
,032 kB]
Get:9 http://bd.archive.ubuntu.com/ubuntu bionic-updates/main Translation-en [3
46 kB]
```

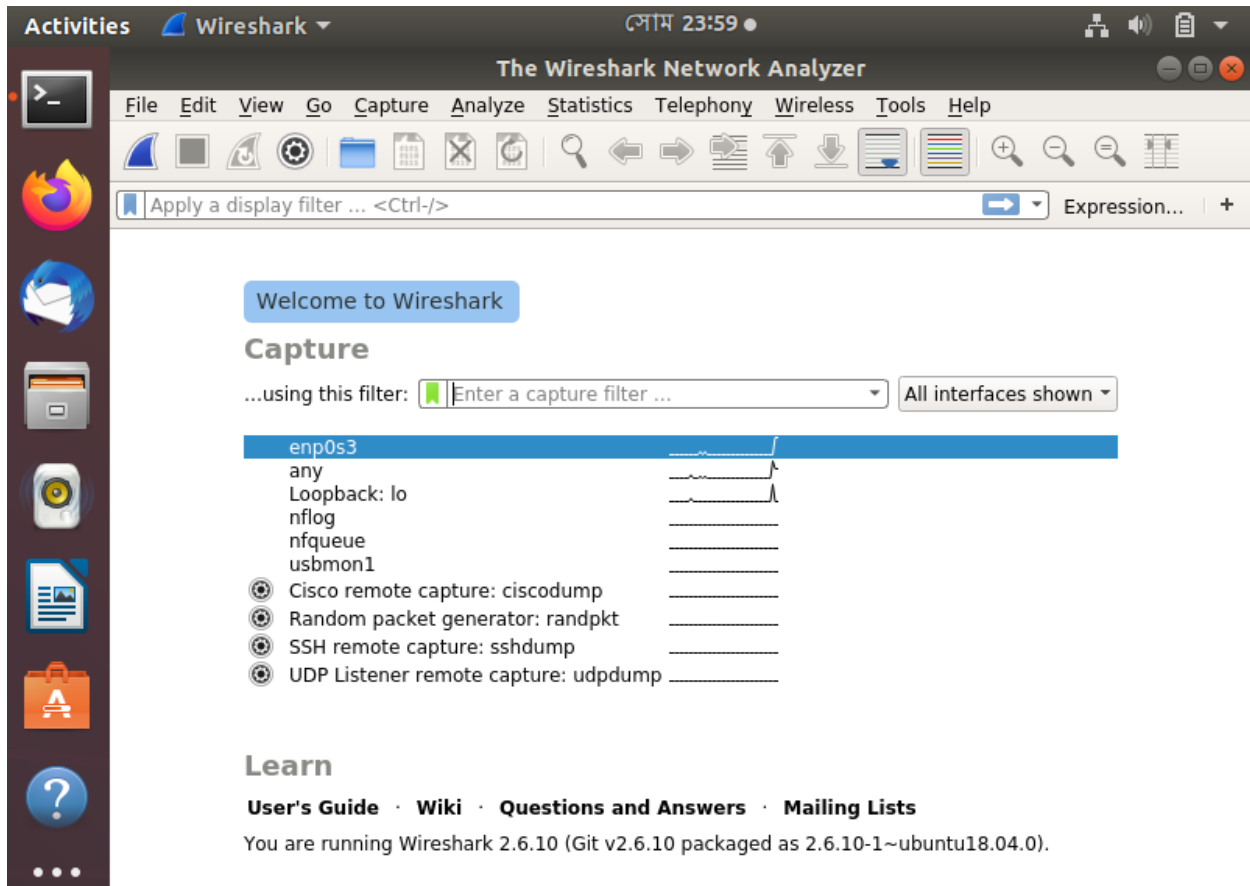
Step 3: Install wireshark :

`sudo apt-get install wireshark`

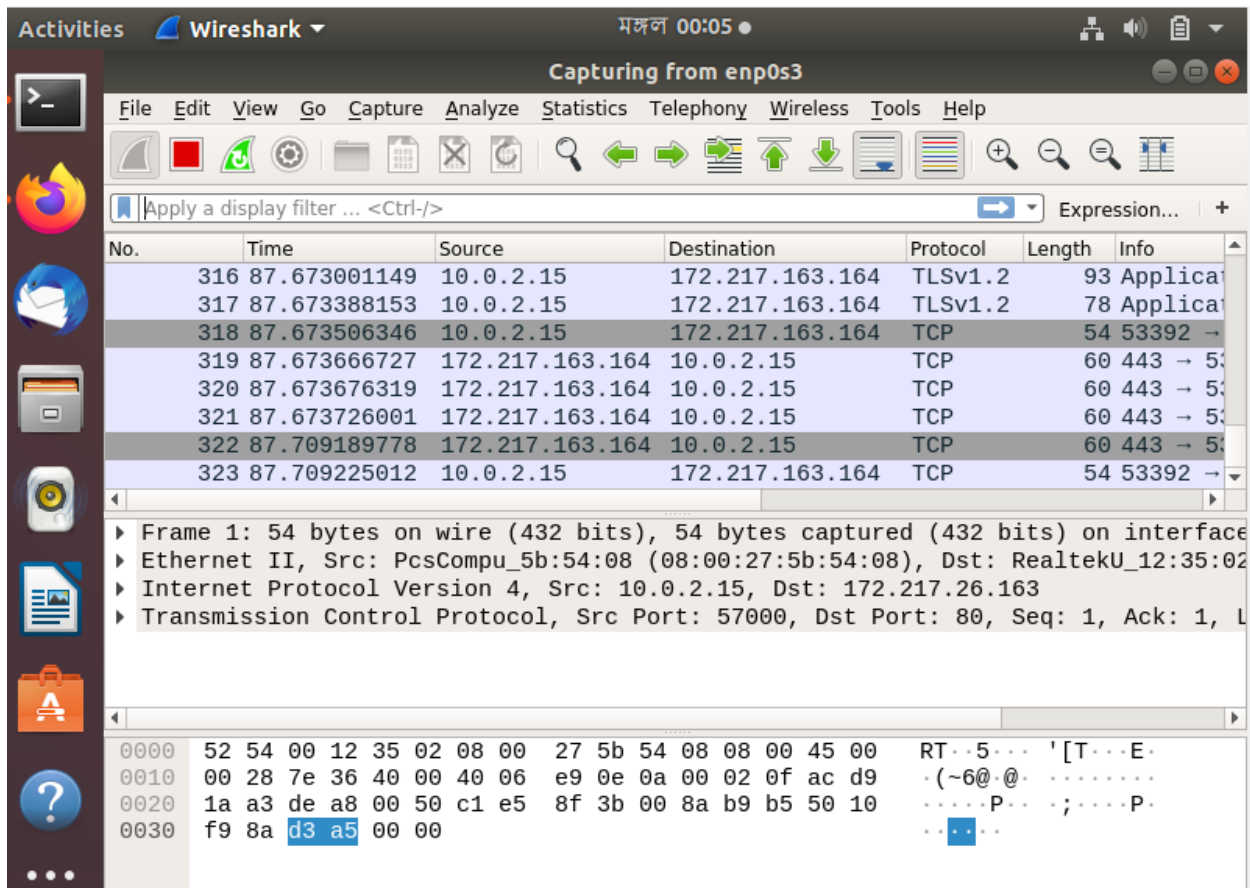
```
sabrin@sabrin-VirtualBox:~$ sudo apt install wireshark
E: dpkg was interrupted, you must manually run 'sudo dpkg --configure -a' to co
rrect the problem.
sabrin@sabrin-VirtualBox:~$ sudo dpkg --configure -a
Setting up wireshark-common (2.6.10-1-ubuntu18.04.0) ...
Setting up nethogs (0.8.5-2) ...
Setting up wireshark-qt (2.6.10-1-ubuntu18.04.0) ...
Setting up wireshark (2.6.10-1-ubuntu18.04.0) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for mime-support (3.60ubuntu1) ...
sabrin@sabrin-VirtualBox:~$
```

Step 4: Run wireshark

`sudo wireshark`



Main Window :



Activities Wireshark ॐ 00:05 ●

Capturing from enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

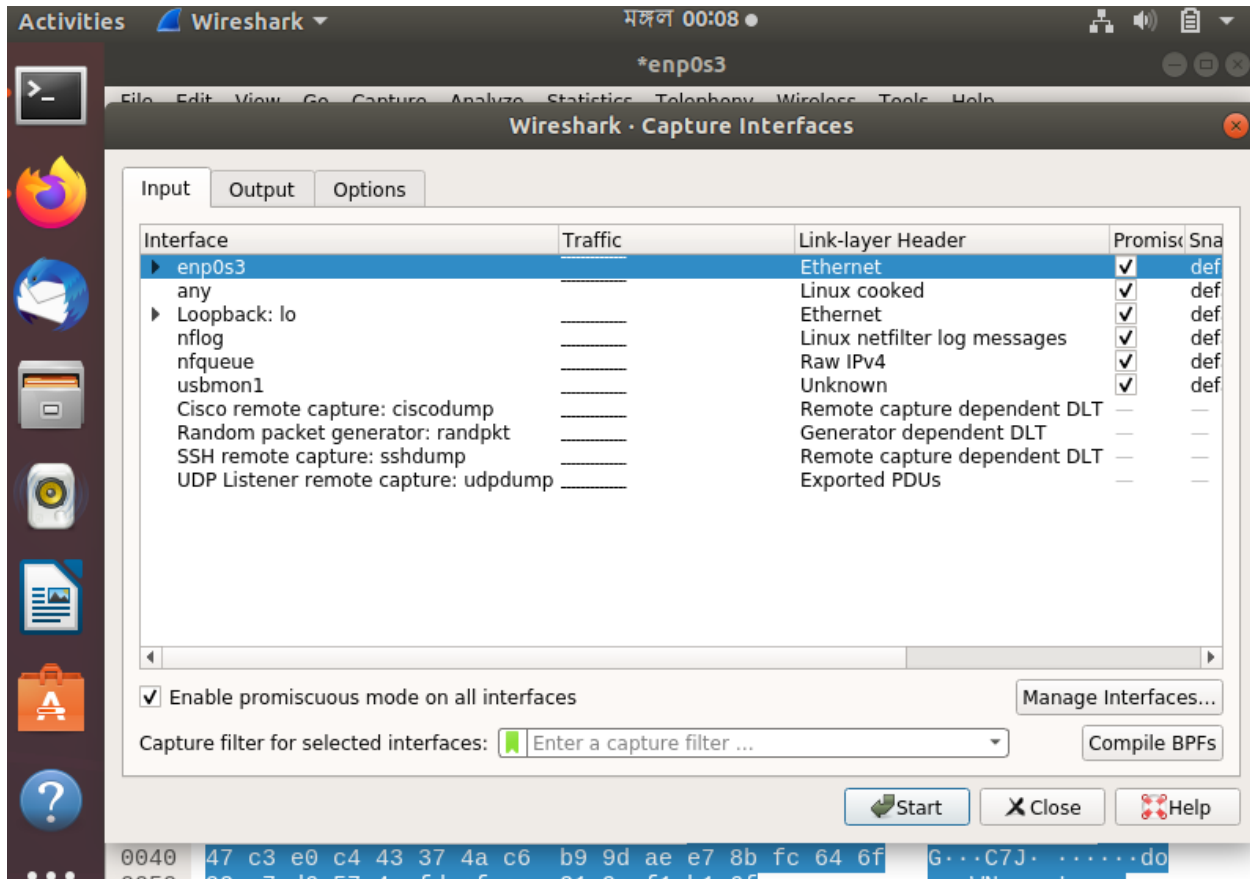
No.	Time	Source	Destination	Protocol	Length	Info
316	87.673001149	10.0.2.15	172.217.163.164	TLSv1.2	93	Application
317	87.673388153	10.0.2.15	172.217.163.164	TLSv1.2	78	Application
318	87.673506346	10.0.2.15	172.217.163.164	TCP	54	53392 →
319	87.673666727	172.217.163.164	10.0.2.15	TCP	60	443 → 53
320	87.673676319	172.217.163.164	10.0.2.15	TCP	60	443 → 53
321	87.673726001	172.217.163.164	10.0.2.15	TCP	60	443 → 53
322	87.709189778	172.217.163.164	10.0.2.15	TCP	60	443 → 53
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

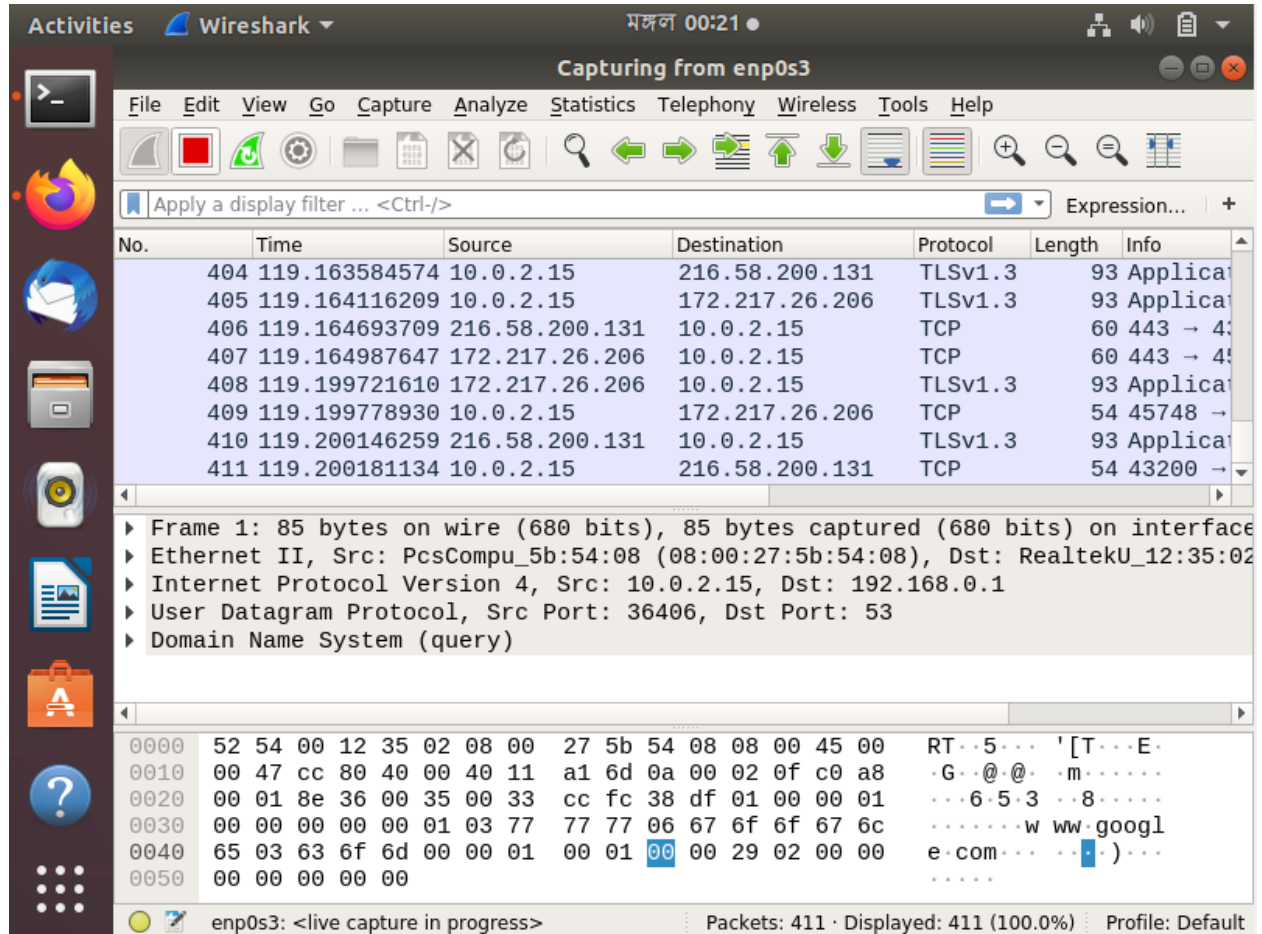
Offset	Hex	ASCII
0000	52 54 00 12 35 02 08 00 27 5b 54 08 08 00 45 00	RT...5... '[T...E.
0010	00 28 7e 36 40 00 40 06 e9 0e 0a 00 02 0f ac d9	..(~6@..@.
0020	1a a3 de a8 00 50 c1 e5 8f 3b 00 8a b9 b5 50 10P...;....P.
0030	f9 8a d3 a5 00 00

Starting Capture :

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

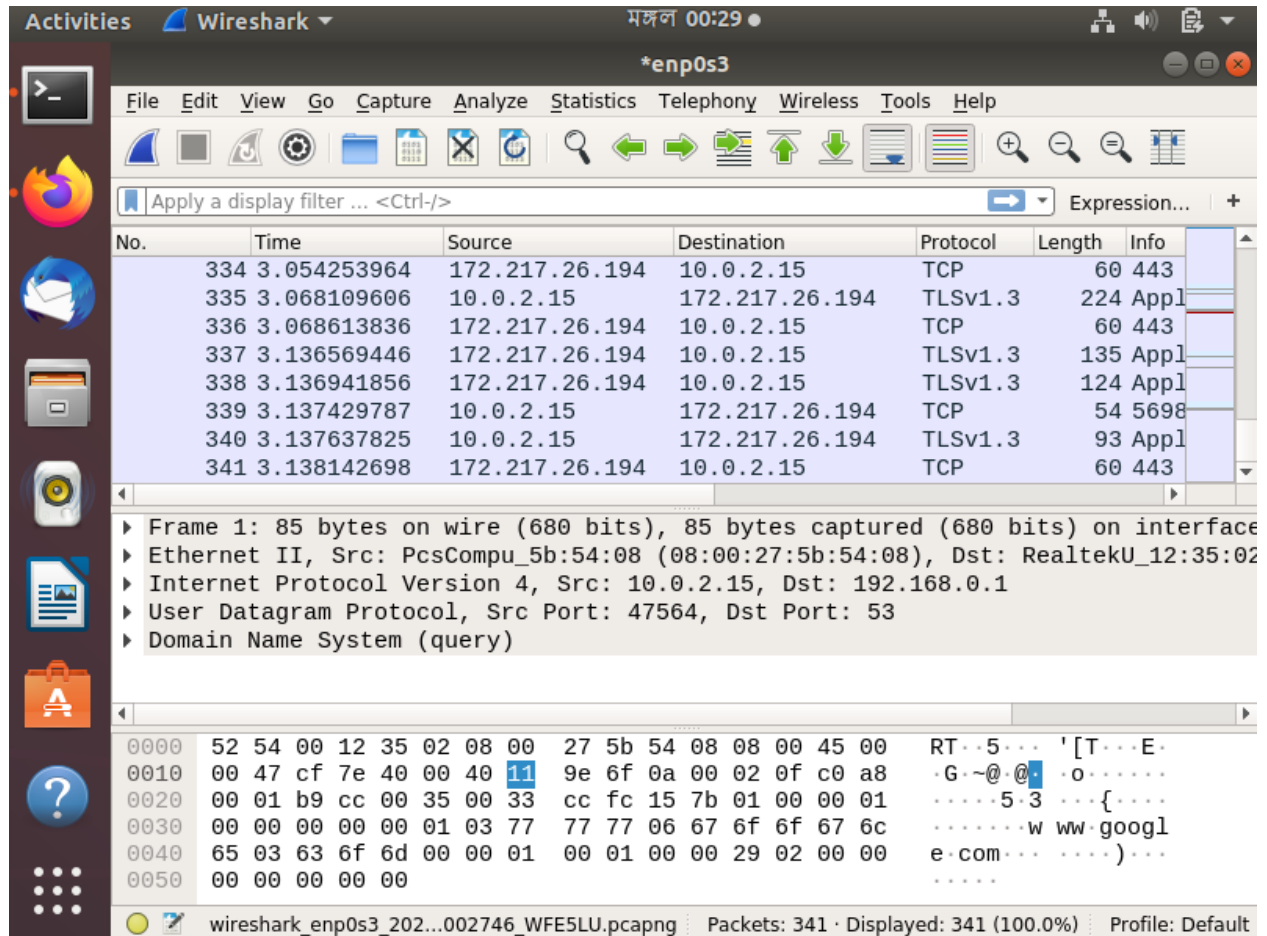


Once the capturing starts, main window will be blank until the data is exchanged on network interface(NIC). When packets exchanged on NIC, the packets will be dumped to main window.



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.

The image shows the Wireshark network traffic analysis interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture, analysis, and display. The filter bar at the top shows the filter expression 'http'. The packet list pane displays four captured packets, all of which are HTTP requests. The packet details pane shows the structure of the selected packet (No. 74), including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data of the selected packet in hexadecimal and ASCII. The status bar at the bottom indicates that 271 packets were captured, 4 (1.5%) are displayed, and 0 (0.0%) are dropped.

No.	Time	Source	Destination	Protocol	Length	Info
74	29.234281487	10.0.2.15	23.59.168.192	HTTP	350	[TCP Prev
78	29.348969613	23.59.168.192	10.0.2.15	HTTP	461	HTTP/1.1
82	29.360875395	10.0.2.15	23.59.168.192	HTTP	355	[TCP Prev
86	29.430940784	23.59.168.192	10.0.2.15	HTTP	461	HTTP/1.1

Files

- Frame 74: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits) on interface
- Ethernet II, Src: PcsCompu_5b:54:08 (08:00:27:5b:54:08), Dst: RealtekU_12:35:08
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 23.59.168.192
- Transmission Control Protocol, Src Port: 34268, Dst Port: 80, Seq: 2, Ack: 1, Len: 350
- Hypertext Transfer Protocol

0000 52 54 00 12 35 02 08 00 27 5b 54 08 08 00 45 00 RT..5... '[T...E..

0010 01 50 f6 4f 40 00 40 06 77 4e 0a 00 02 0f 17 3b .P.0@.@. wN.....;

0020 a8 c0 85 dc 00 50 90 8a fb 3e 14 75 4f 99 50 18P...>.u0.P.

0030 f9 59 cd 4c 00 00 47 45 54 20 2f 73 75 63 63 65 .Y.L..GE T /succe

0040 73 73 2e 74 78 74 20 48 54 54 50 2f 31 2e 31 0d ss.txt H TTP/1.1.

0050 0a 48 6f 73 74 3a 20 64 65 74 65 63 74 70 6f 72 .Host: d etectpor

0060 74 61 6c 2e 66 69 72 65 66 6f 78 2e 63 6f 6d 0d tal.fire fox.com.

0070 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a .User-Ag ent: Moz

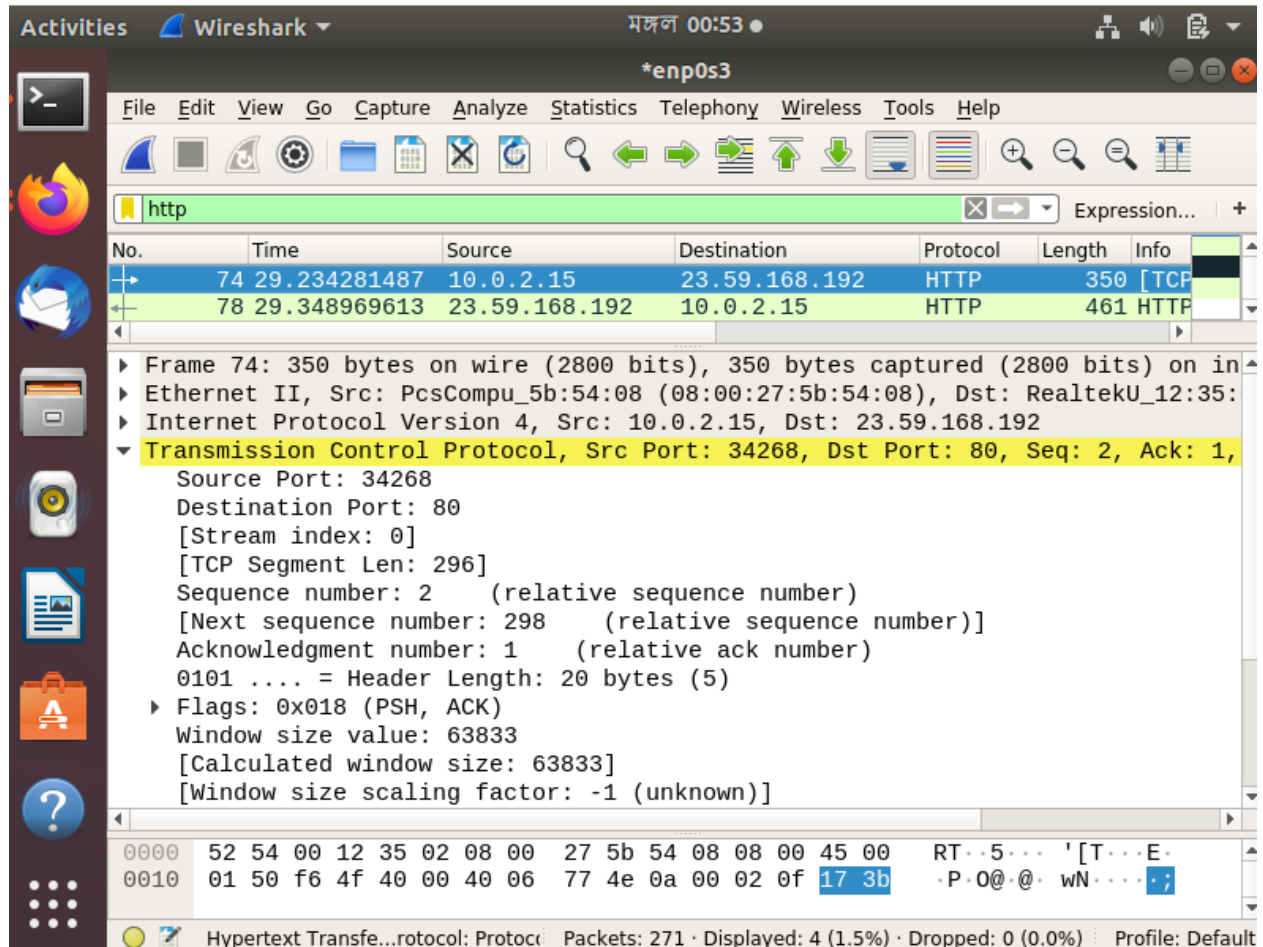
0080 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b 20 55 illa/5.0 (X11; U

0090 62 75 6e 74 75 3b 20 4c 69 6e 75 78 20 78 38 36 buntu; L inux x86

Hypertext Transfe...rotocol: Protoc Packets: 271 · Displayed: 4 (1.5%) · Dropped: 0 (0.0%) Profile: Default

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.

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The interface is titled '*enp0s3'.

The packet list pane shows two captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
74	29.234281487	10.0.2.15	23.59.168.192	HTTP	350	[TCP]
78	29.348969613	23.59.168.192	10.0.2.15	HTTP	461	HTTP

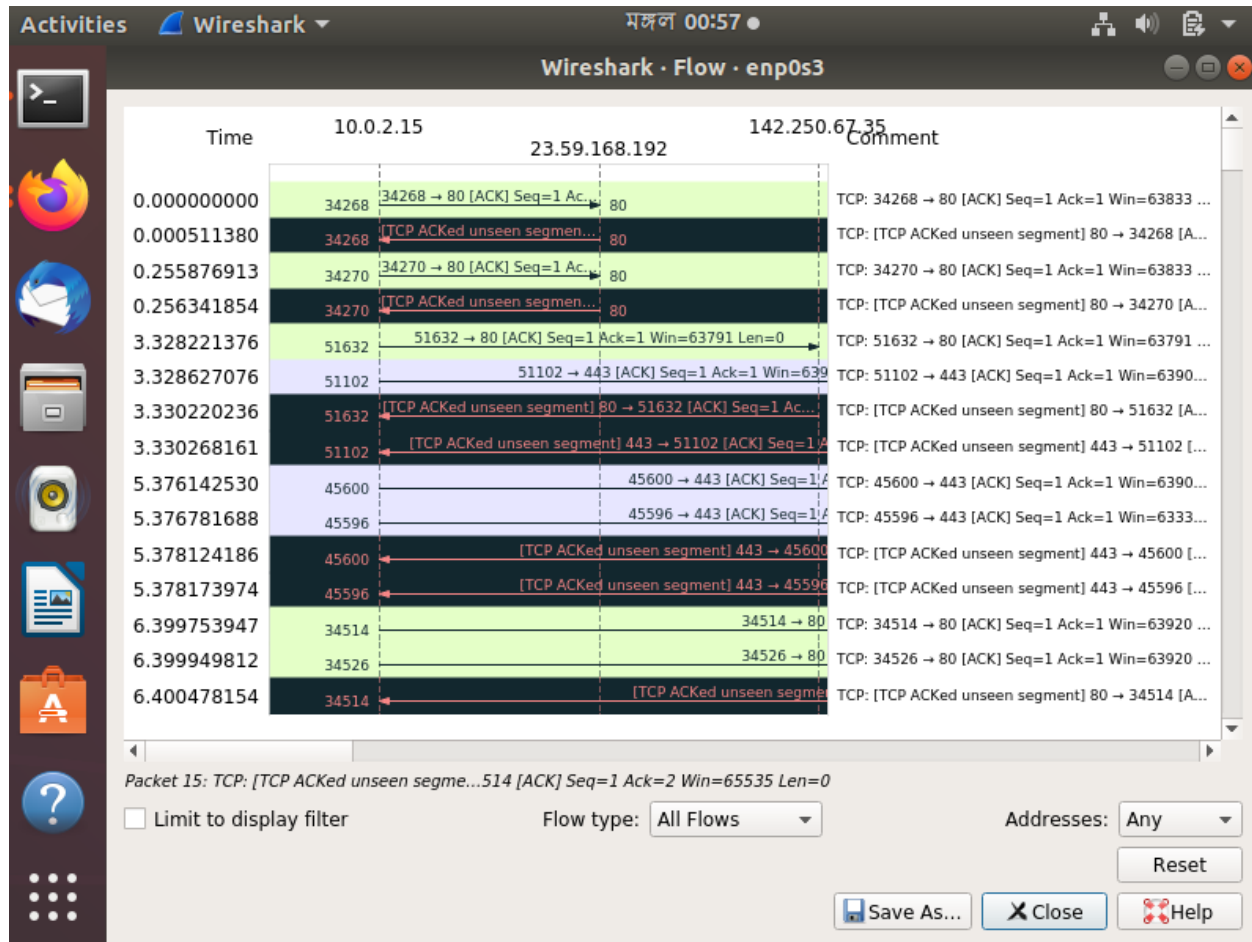
The packet details pane for the selected packet (Frame 74) shows the following structure:

- Frame 74: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits) on in
- Ethernet II, Src: PcsCompu_5b:54:08 (08:00:27:5b:54:08), Dst: RealtekU_12:35:
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 23.59.168.192

The packet bytes pane displays the raw data in hexadecimal and ASCII. The hex data is shown in columns, and the ASCII data is shown in a single column. The ASCII data is truncated with dots, indicating it continues.

The status bar at the bottom indicates: Hypertext Transfe...rotocol: Protoc: Packets: 271 · Displayed: 4 (1.5%) · Dropped: 0 (0.0%) · Profile: Default

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.