

MAWLANA BHASHANI SCIENCE AND TECHNOLOGY UNIVERSITY

Santosh, Tangail – 1902



Course Title: Computer Networks Lab

Submitted by,

Name : Nadira Islam

ID: IT-17051

Session: 2016-17

Dept. of ICT, MBSTU.

Submitted to,

NAZRUL ISLAM

Assistant Professor

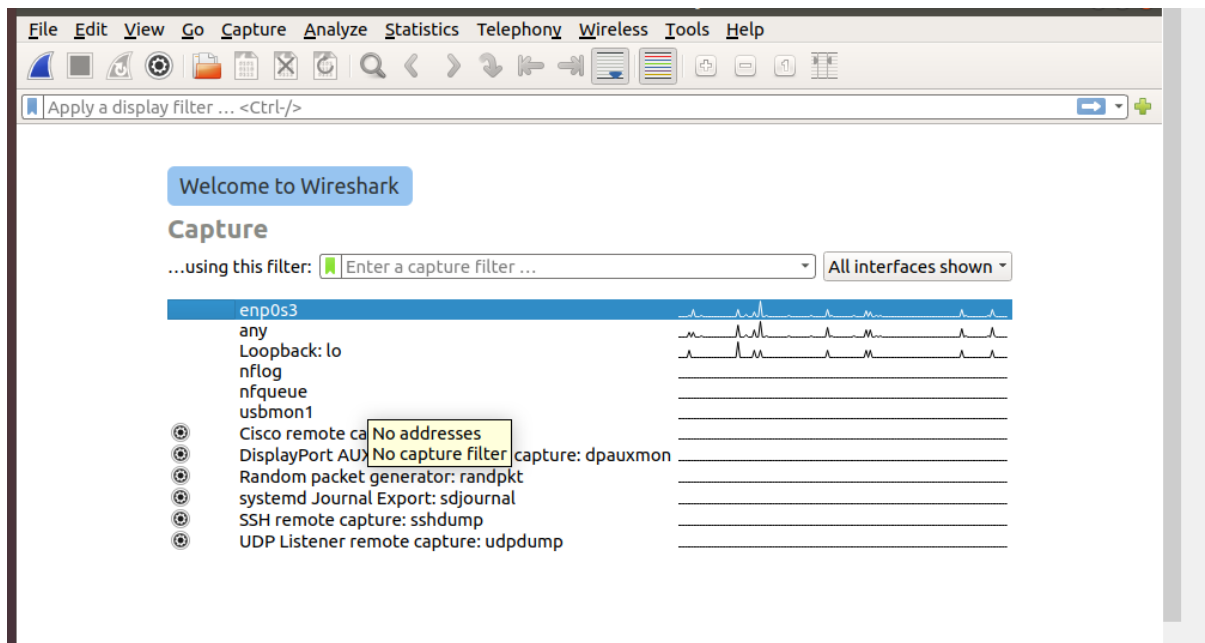
Dept. of ICT, MBSTU.

Wireshark : Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.

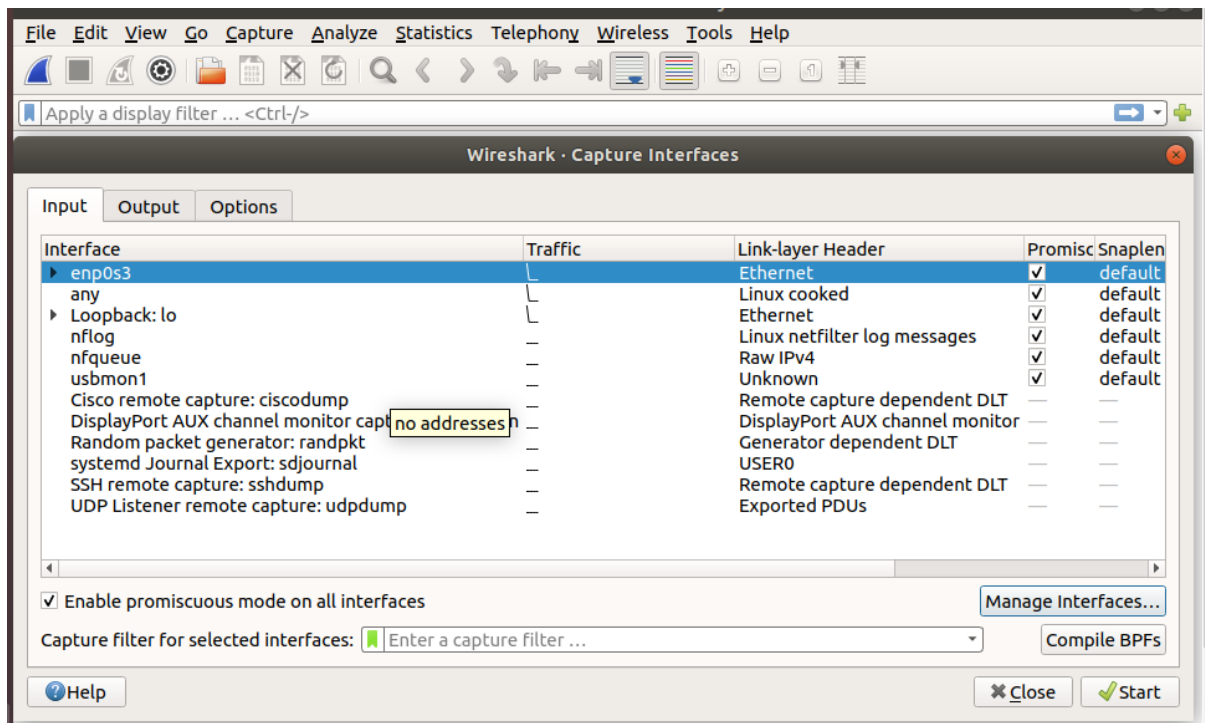
Installation: To install wireshark we have to write the following command

```
nadira@nadira-VirtualBox:~$ sudo apt-get install wireshark
[sudo] password for nadira:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  efibootmgr libfwup1 libwayland-egl1-mesa
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  gir1.2-nma-1.0 libc-ares2 libdouble-conversion1 liblua5.2-0 libmaxminddb0
  libnl-route-3-200 libqgsttools-p1 libqt5core5a libqt5dbus5 libqt5gui5
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediawidgets5
  libqt5network5 libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5
  libsmi2ldbl libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data
  libwireshark13 libwiretap10 libwsutil11 libxcb-xinerama0
  qt5-gtk-platformtheme qttranslations5-l10n wireshark-common wireshark-qt
Suggested packages:
  mmdb-bin qt5-image-formats-plugins qtwayland5 snmp-mibs-downloader
  geoipupdate geoip-database-extra libjs-leaflet libjs-leaflet.markercluster
  wireshark-doc
The following NEW packages will be installed:
  libc-ares2 libdouble-conversion1 liblua5.2-0 libmaxminddb0 libnl-route-3-200
  libqgsttools-p1 libqt5core5a libqt5dbus5 libqt5gui5 libqt5multimedia5
  libqt5multimedia5-plugins libqt5multimediawidgets5 libqt5network5
  libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl
  libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark13
  libwiretap10 libwsutil11 libxcb-xinerama0 qt5-gtk-platformtheme
  qttranslations5-l10n wireshark wireshark-common wireshark-qt
The following packages will be upgraded:
  gir1.2-nma-1.0
1 upgraded, 31 newly installed, 0 to remove and 301 not upgraded.
3 not fully installed or removed.
```

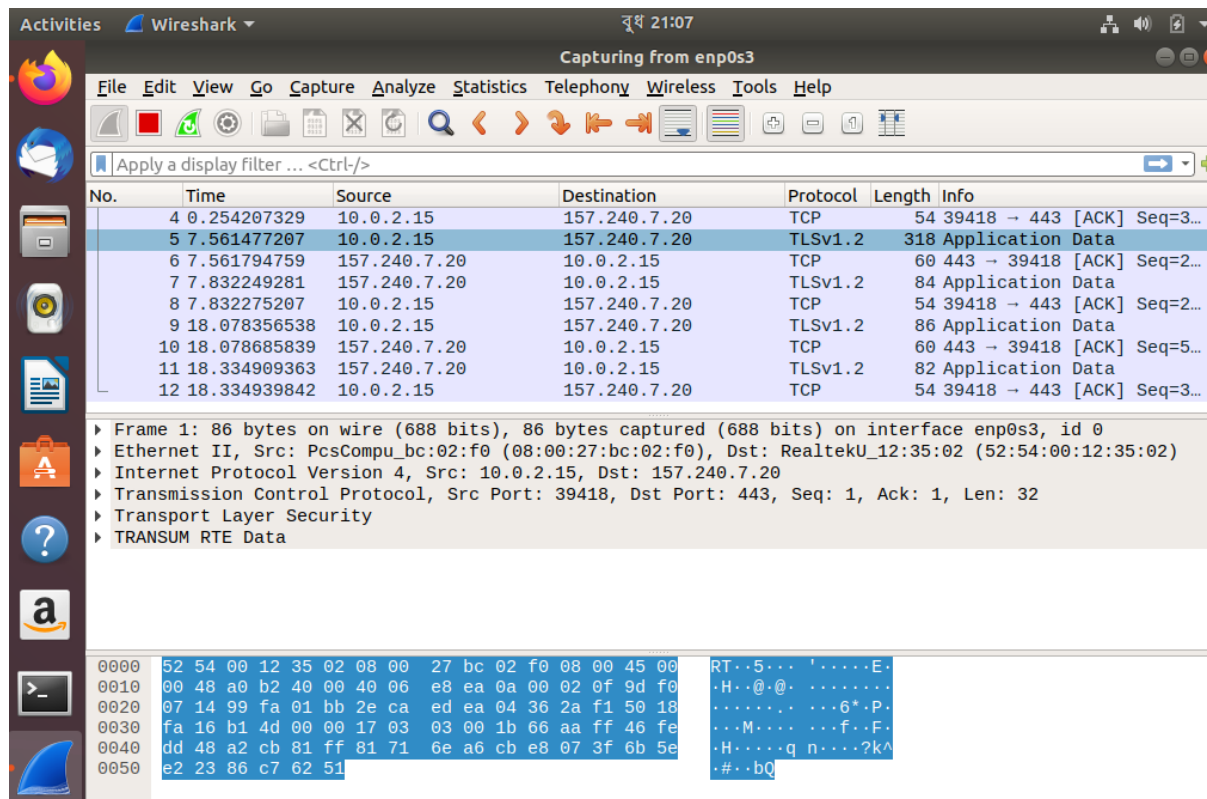
Use of Wireshark:



Capture:



Capturing 1:



Stop capturing:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
217	237.729590473	157.240.7.20	10.0.2.15	TCP	60	443 → 39418 [ACK] S...
218	237.984106459	157.240.7.20	10.0.2.15	TLSv1.2	82	Application Data
219	237.984161903	10.0.2.15	157.240.7.20	TCP	54	39418 → 443 [ACK] S...
220	242.592404455	10.0.2.15	91.189.89.199	NTP	90	NTP Version 4, clie...
221	242.802167927	157.240.7.20	10.0.2.15	TLSv1.2	100	Application Data
222	242.802198033	10.0.2.15	157.240.7.20	TCP	54	39418 → 443 [ACK] S...
223	242.831196787	91.189.89.199	10.0.2.15	NTP	90	NTP Version 4, serv...
224	244.621081143	157.240.7.20	10.0.2.15	TLSv1.2	102	Application Data
225	244.621098920	10.0.2.15	157.240.7.20	TCP	54	39418 → 443 [ACK] S...

▶ Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface enp0s3, id 0
 ▶ Ethernet II, Src: PcsCompu_bc:02:f0 (08:00:27:bc:02:f0), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
 ▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 157.240.7.20
 ▶ Transmission Control Protocol, Src Port: 39418, Dst Port: 443, Seq: 1, Ack: 1, Len: 32
 ▶ Transport Layer Security
 ▶ TRANSUM RTE Data

```

0000 52 54 00 12 35 02 08 00 27 bc 02 f0 08 00 45 00 RT..5... '....E.
0010 00 48 a0 b2 40 00 40 06 e8 ea 0a 00 02 0f 9d f0 .H..@. @. ....
0020 07 14 99 fa 01 bb 2e ca ed ea 04 36 2a f1 50 18 ..... 6*.P.
0030 fa 16 b1 4d 00 00 17 03 03 00 1b 66 aa ff 46 fe ...M.... .f..F.
0040 dd 48 a2 cb 81 ff 81 71 6e a6 cb e8 07 3f 6b 5e .H....q n....?k^
0050 e2 23 86 c7 62 51 .#..bQ
  
```

Filtering:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	157.240.7.20	TLSv1.2	86	Application Data
2	0.000381452	157.240.7.20	10.0.2.15	TCP	60	443 → 39418 [ACK] S...
3	0.254154374	157.240.7.20	10.0.2.15	TLSv1.2	82	Application Data
4	0.254207329	10.0.2.15	157.240.7.20	TCP	54	39418 → 443 [ACK] S...
5	7.561477207	10.0.2.15	157.240.7.20	TLSv1.2	318	Application Data
6	7.561794759	157.240.7.20	10.0.2.15	TCP	60	443 → 39418 [ACK] S...
7	7.832249281	157.240.7.20	10.0.2.15	TLSv1.2	84	Application Data
8	7.832275207	10.0.2.15	157.240.7.20	TCP	54	39418 → 443 [ACK] S...
9	18.078356538	10.0.2.15	157.240.7.20	TLSv1.2	86	Application Data
10	18.078685830	157.240.7.20	10.0.2.15	TCP	60	443 → 39418 [ACK] S...

▶ Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface enp0s3, id 0
 ▶ Ethernet II, Src: PcsCompu_bc:02:f0 (08:00:27:bc:02:f0), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
 ▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 157.240.7.20
 ▶ Transmission Control Protocol, Src Port: 39418, Dst Port: 443, Seq: 1, Ack: 1, Len: 32
 ▶ Transport Layer Security
 ▶ TRANSUM RTE Data

```

0000 52 54 00 12 35 02 08 00 27 bc 02 f0 08 00 45 00 RT..5... '....E.
0010 00 48 a0 b2 40 00 40 06 e8 ea 0a 00 02 0f 9d f0 .H..@. @. ....
0020 07 14 99 fa 01 bb 2e ca ed ea 04 36 2a f1 50 18 ..... 6*.P.
0030 fa 16 b1 4d 00 00 17 03 03 00 1b 66 aa ff 46 fe ...M.... .f..F.
0040 dd 48 a2 cb 81 ff 81 71 6e a6 cb e8 07 3f 6b 5e .H....q n....?k^
0050 e2 23 86 c7 62 51 .#..bQ
  
```

Packet details pane:

The Packet Details pane displays the structure of the captured packet. It shows the Ethernet II header with source and destination MAC addresses, and the Internet Protocol Version 4 header with source and destination IP addresses. The packet is identified as Frame 1, 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface enp0s3, id 0.

eth.addr eq 08:00:27:bc:02:f0 and eth.addr eq 52:54:00:12:35:02

No.	Time	Source	Destination	Protocol	Length	Info
1				Ethernet II	86	Src: PcsCompu_bc:02:f0 (08:00:27:bc:02:f0), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 157.240.7.20						

Encapsulation type: Ethernet (1)
Arrival Time: Aug 5, 2020 21:07:12.853703004 +06
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1596640032.853703004 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 86 bytes (688 bits)
Capture Length: 86 bytes (688 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:tls]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]

Ethernet II, Src: PcsCompu_bc:02:f0 (08:00:27:bc:02:f0), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
Source: PcsCompu_bc:02:f0 (08:00:27:bc:02:f0)
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 157.240.7.20
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 72
Identification: 0xa0b2 (41138)
Flags: 0x4000, Don't fragment

Packet byte pane:

The Packet Byte pane displays the raw data of the packet in hexadecimal and ASCII. The data is organized into columns, with the first column showing the offset (0000 to 0050) and the second column showing the hexadecimal data. The third column shows the ASCII representation of the data.

eth.addr eq 08:00:27:bc:02:f0 and eth.addr eq 52:54:00:12:35:02

No.	Time	Source	Destination	Protocol	Length	Info
[Coloring Rule Name: TCP] [Coloring Rule String: tcp]						
Ethernet II, Src: PcsCompu_bc:02:f0 (08:00:27:bc:02:f0), Dst: RealtekU_12:35:02...						
Destination: RealtekU_12:35:02 (52:54:00:12:35:02) Source: PcsCompu_bc:02:f0 (08:00:27:bc:02:f0) Type: IPv4 (0x0800)						

0000 52 54 00 12 35 02 08 00 27 bc 02 f0 08 00 45 00 RT..5... '.....E.
0010 00 48 a0 b2 40 00 40 06 e8 ea 0a 00 02 0f 9d f0 .H..@.@@.
0020 07 14 99 fa 01 bb 2e ca ed ea 04 36 2a f1 50 18 6*.P.
0030 fa 16 b1 4d 00 00 17 03 03 00 1b 66 aa ff 46 fe .M.... .f..F.
0040 dd 48 a2 cb 81 ff 81 71 6e a6 cb e8 07 3f 6b 5e .H....q n....?k^
0050 e2 23 86 c7 62 51 .#..bQ

