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.

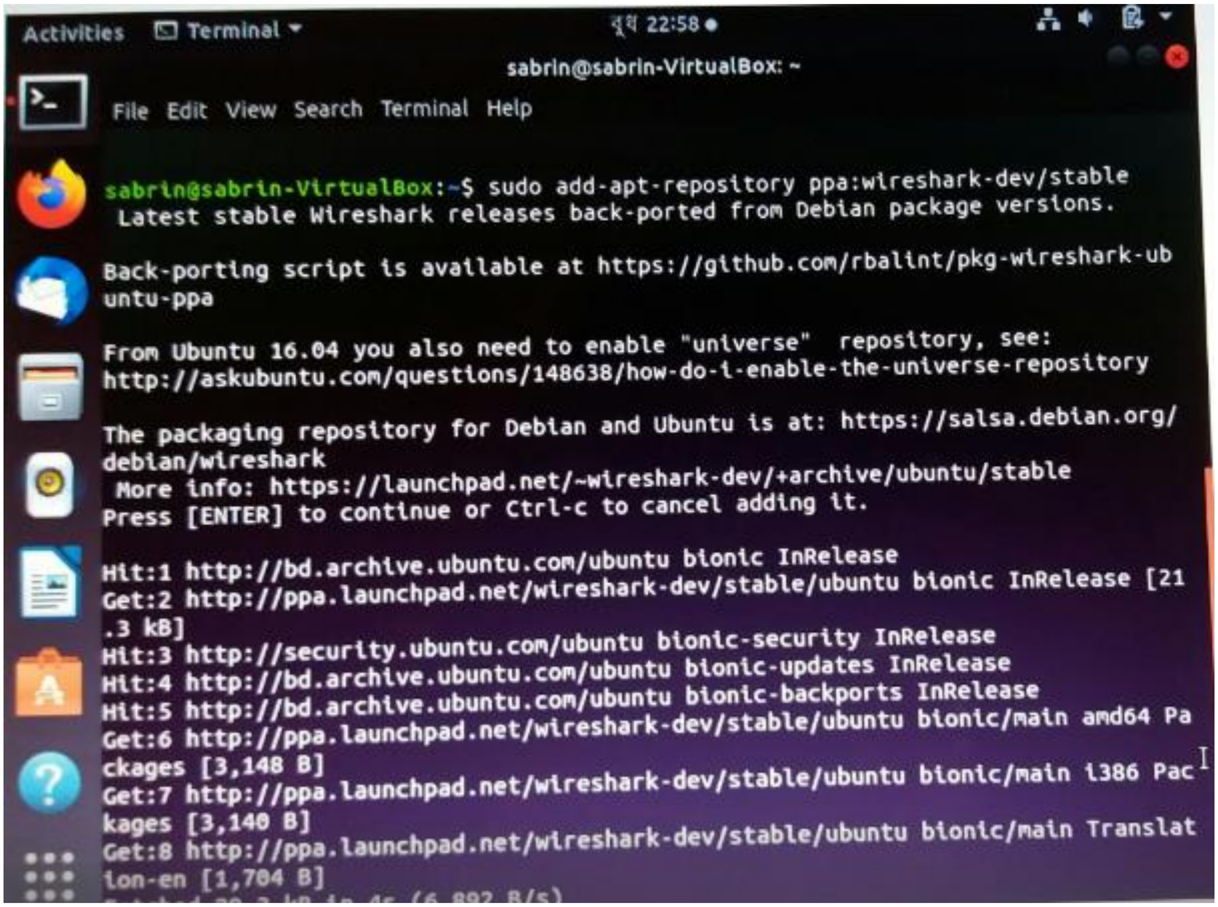
Installation of Wireshark

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 :

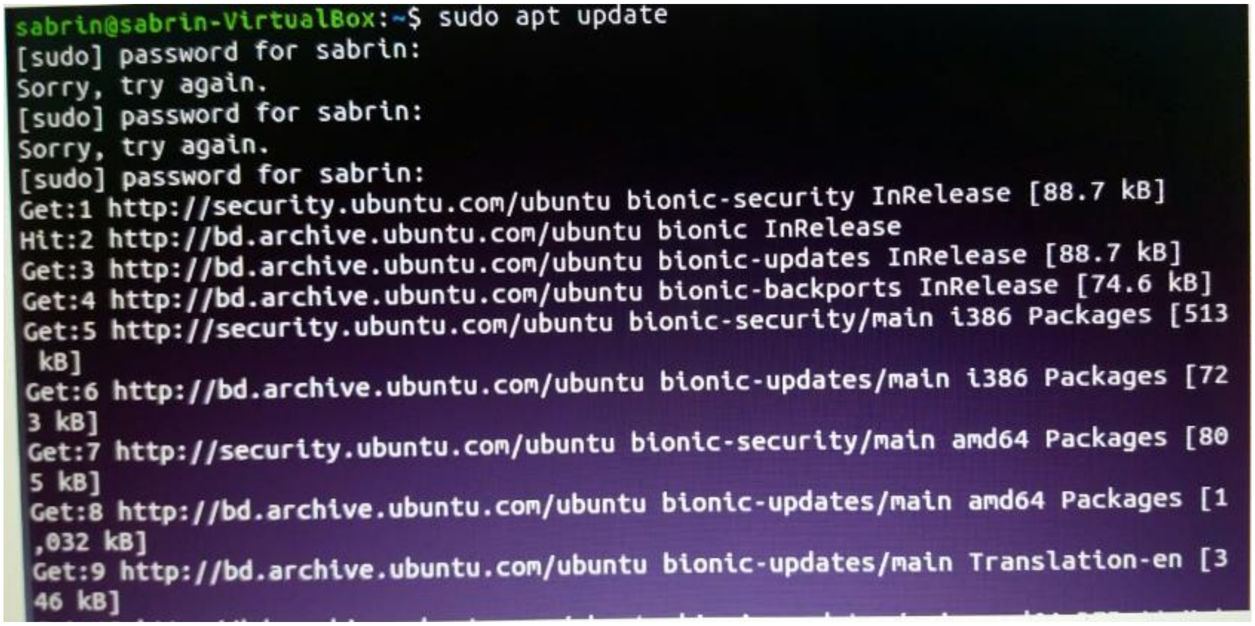
sudo add-apt-repository ppa:wireshark-dev/stable


Activities
Terminal
বুধ 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-ub
untu-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 Pa
ckages [3,148 B]
Get:7 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu bionic/main i386 Pac
kages [3,140 B]
Get:8 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu bionic/main Translat
ion-en [1,704 B]
Fetched 29.3 kB in 4s (6,892 B/s)
```

Step 2: Update the repository :

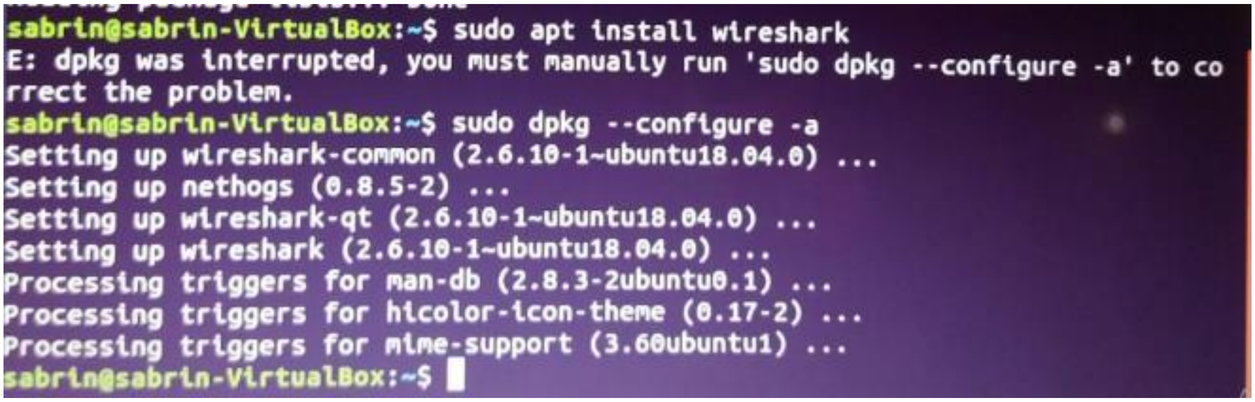
sudo apt-get update



```
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 :

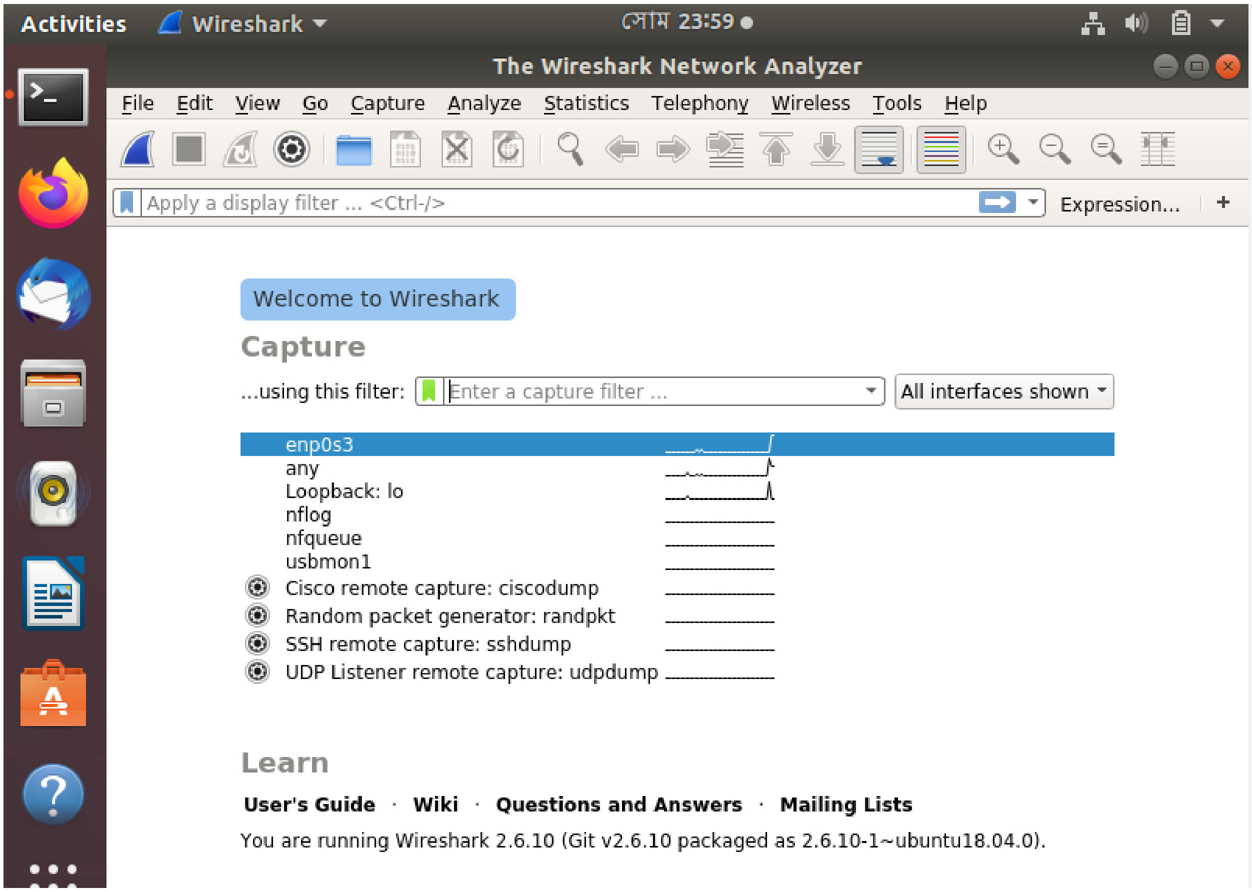
sudo apt-get install wireshark



```
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
```

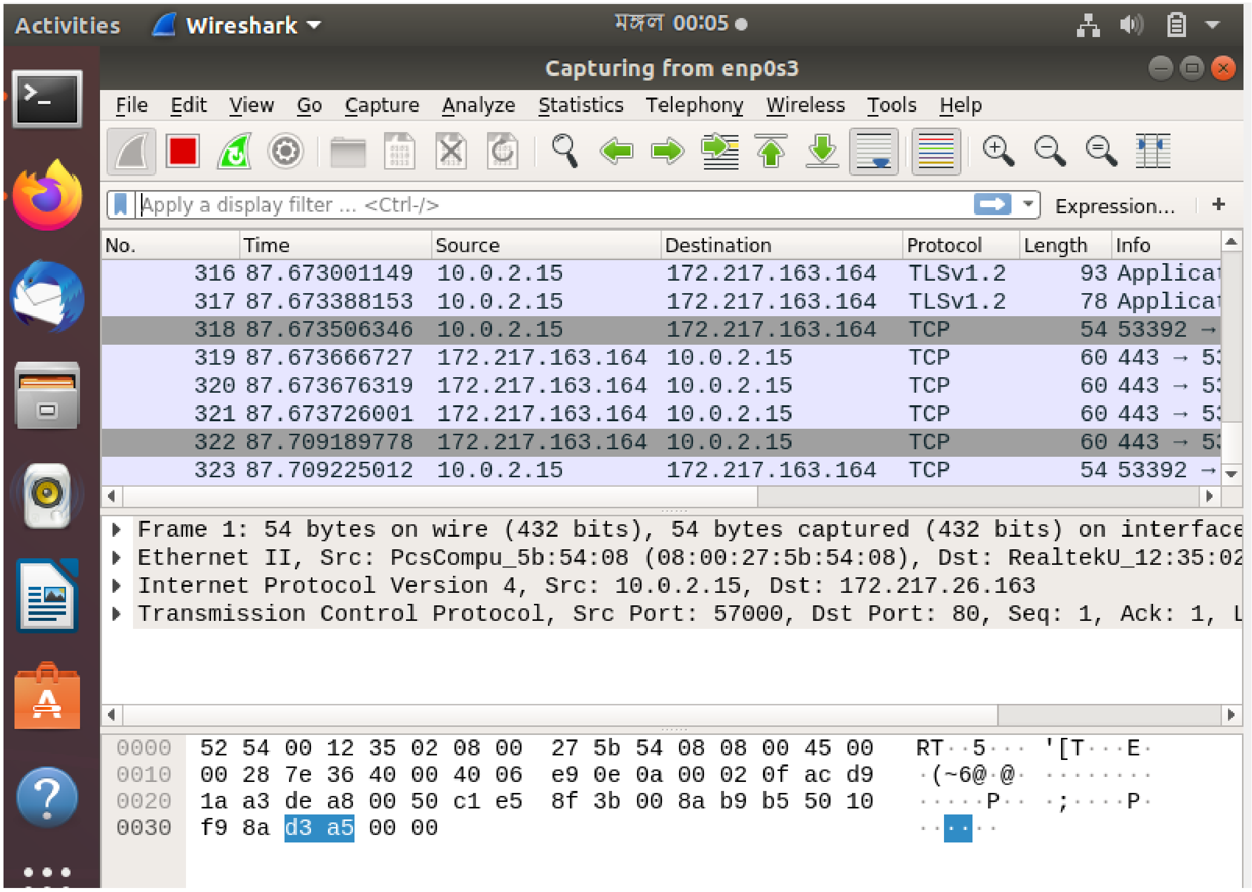


Activities
Wireshark
সোম 23:59
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

```
enp0s3
any
Loopback: lo
nflog
nfqueue
usbmon1
Cisco remote capture: ciscodump
Random packet generator: randpkt
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
```

You are running Wireshark 2.6.10 (Git v2.6.10 packaged as 2.6.10-1~ubuntu18.04.0).

Main Window :



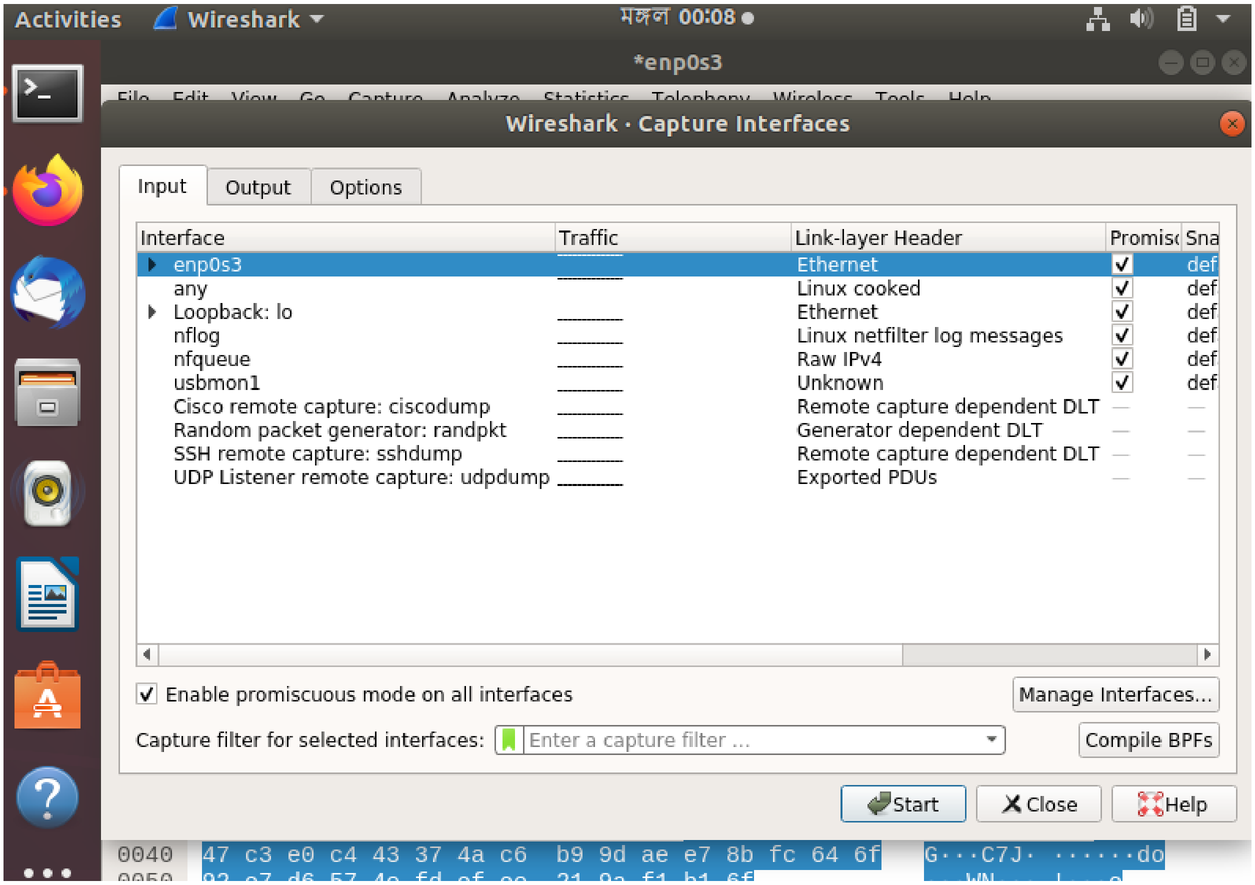
```
No.     Time           Source          Destination     Protocol  Length Info
    316 87.673001149   10.0.2.15       172.217.163.164 TLSv1.2       93 Applicat
    317 87.673388153   10.0.2.15       172.217.163.164 TLSv1.2       78 Applicat
    318 87.673506346   10.0.2.15       172.217.163.164 TCP           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   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 10   ·····P···;····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.


Activities
Wireshark
मङ्गल 00:08
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Capture Interfaces
Input
Output
Options
Manage Interfaces...
Compile BPFs
Start
Close
Help

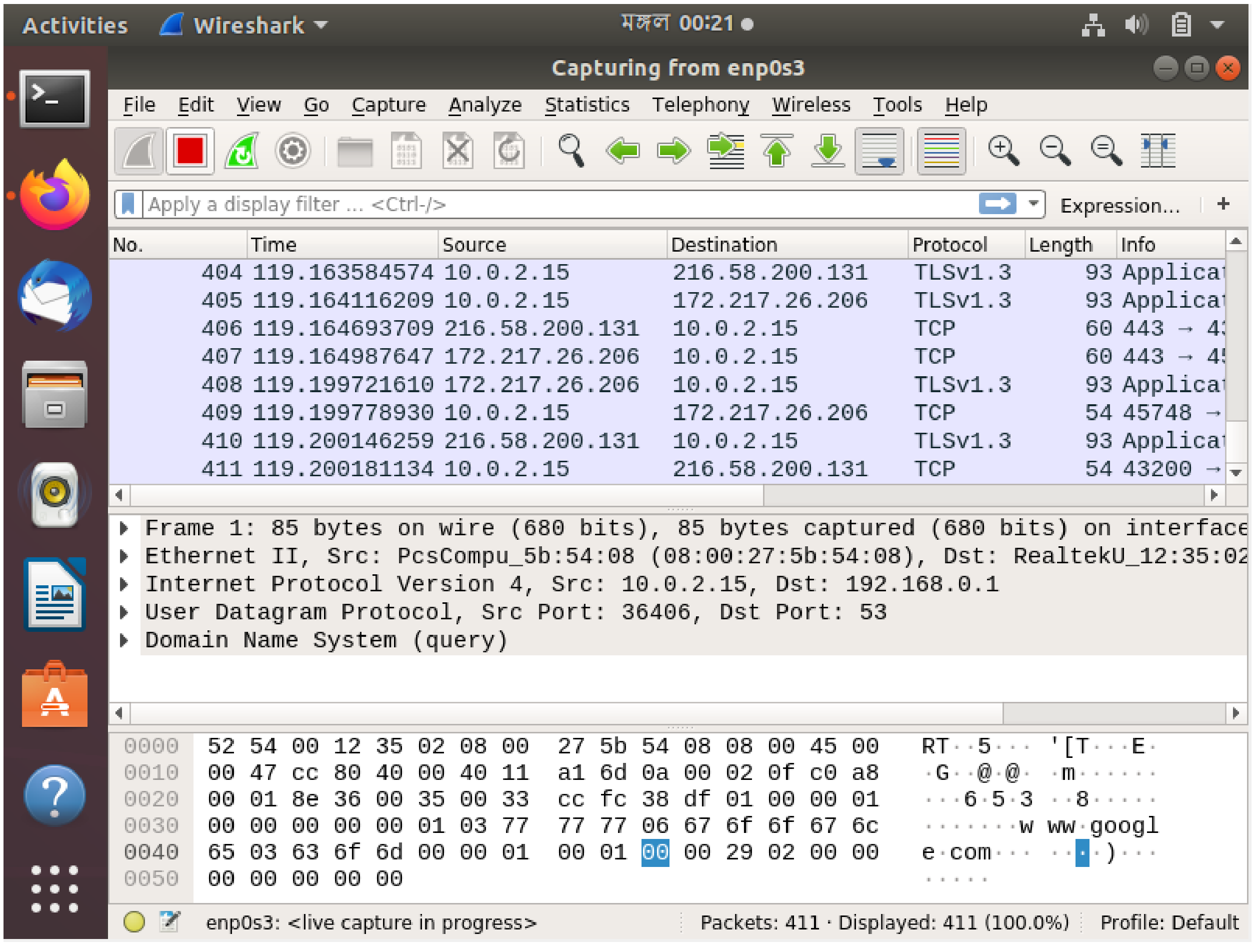
Interface	Traffic	Link-layer Header	Promisc	Sna
enp0s3		Ethernet	☑	def
any		Linux cooked	☑	def
Loopback: lo		Ethernet	☑	def
nflog		Linux netfilter log messages	☑	def
nfqueue		Raw IPv4	☑	def
usbmon1		Unknown	☑	def
Cisco remote capture: ciscodump		Remote capture dependent DLT	—	—
Random packet generator: randpkt		Generator dependent DLT	—	—
SSH remote capture: sshdump		Remote capture dependent DLT	—	—
UDP Listener remote capture: udpdump		Exported PDUs	—	—

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

```
0040  47 c3 e0 c4 43 37 4a c6  b9 9d ae e7 8b fc 64 6f   G···C7J· ······do
```

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.


Activities
Wireshark
मङ्गल 00:21
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
   404 119.163584574 10.0.2.15       216.58.200.131  TLSv1.3       93 Applicat
   405 119.164116209 10.0.2.15       172.217.26.206  TLSv1.3       93 Applicat
   406 119.164693709 216.58.200.131  10.0.2.15       TCP           60 443 → 43
   407 119.164987647 172.217.26.206  10.0.2.15       TCP           60 443 → 45
   408 119.199721610 172.217.26.206  10.0.2.15       TLSv1.3       93 Applicat
   409 119.199778930 10.0.2.15       172.217.26.206  TCP           54 45748 →
   410 119.200146259 216.58.200.131  10.0.2.15       TLSv1.3       93 Applicat
   411 119.200181134 10.0.2.15       216.58.200.131  TCP           54 43200 →
```

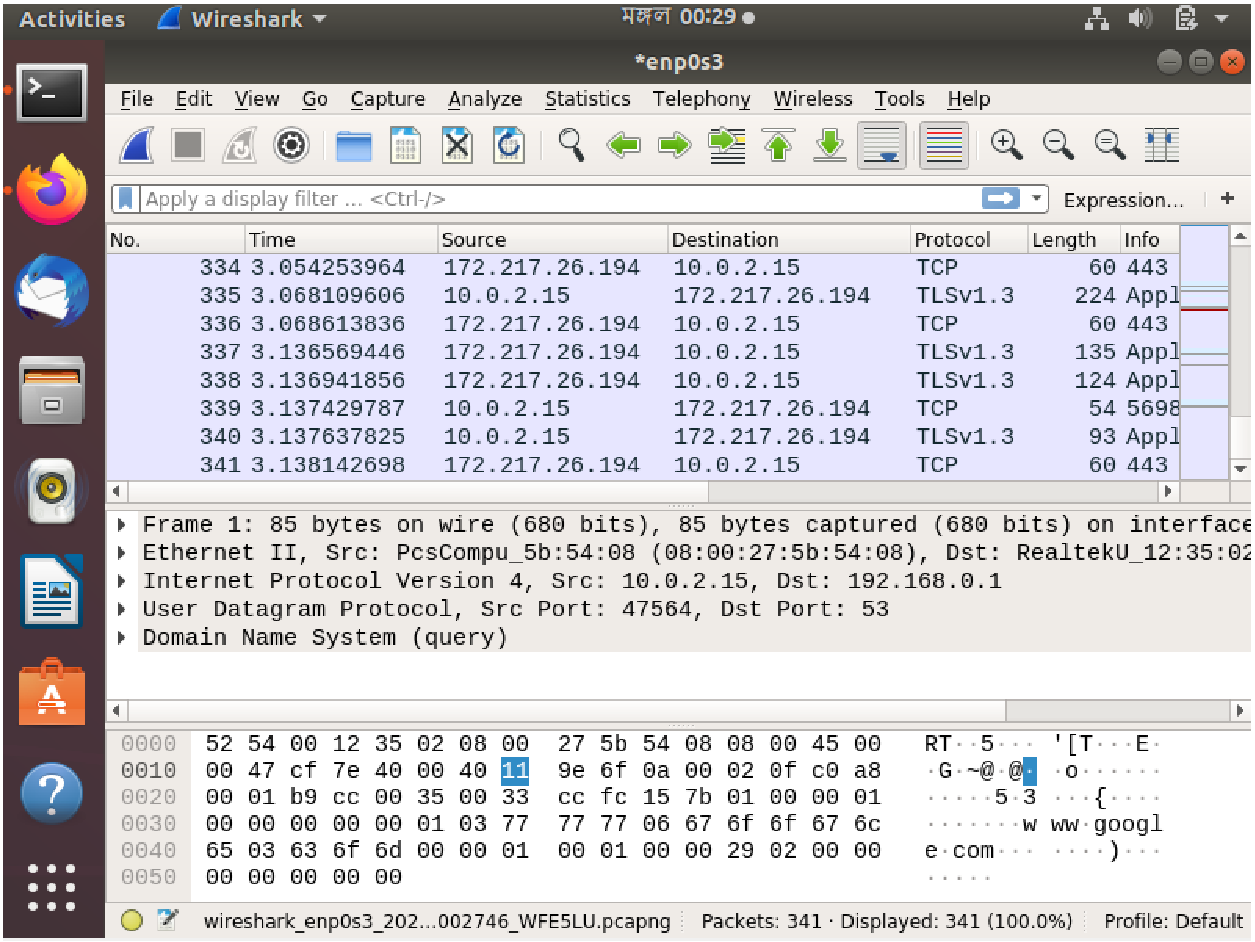
```
▸ Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface
▸ Ethernet II, Src: PcsCompu_5b:54:08 (08:00:27:5b:54:08), Dst: RealtekU_12:35:02
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.0.1
▸ User Datagram Protocol, Src Port: 36406, Dst Port: 53
▸ Domain Name System (query)
```

```
0000  52 54 00 12 35 02 08 00  27 5b 54 08 08 00 45 00   RT··5··· '[T···E·
0010  00 47 cc 80 40 00 40 11  a1 6d 0a 00 02 0f c0 a8   ·G··@·@· ·m······
0020  00 01 8e 36 00 35 00 33  cc fc 38 df 01 00 00 01   ···6·5·3 ··8·····
0030  00 00 00 00 00 01 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0040  65 03 63 6f 6d 00 00 01  00 01 00 00 29 02 00 00   e·com··· ····)···
0050  00 00 00 00 00                                     ·····
```

enp0s3: <live capture in progress> Packets: 411 · Displayed: 411 (100.0%) Profile: Default

Stopping Capture :

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


Activities
Wireshark
मङ्गल 00:29
*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
       334 3.054253964  172.217.26.194   10.0.2.15        TCP             60 443
       335 3.068109606  10.0.2.15        172.217.26.194   TLSv1.3        224 Appl
       336 3.068613836  172.217.26.194   10.0.2.15        TCP             60 443
       337 3.136569446  172.217.26.194   10.0.2.15        TLSv1.3        135 Appl
       338 3.136941856  172.217.26.194   10.0.2.15        TLSv1.3        124 Appl
       339 3.137429787  10.0.2.15        172.217.26.194   TCP             54 5698
       340 3.137637825  10.0.2.15        172.217.26.194   TLSv1.3         93 Appl
       341 3.138142698  172.217.26.194   10.0.2.15        TCP             60 443
```

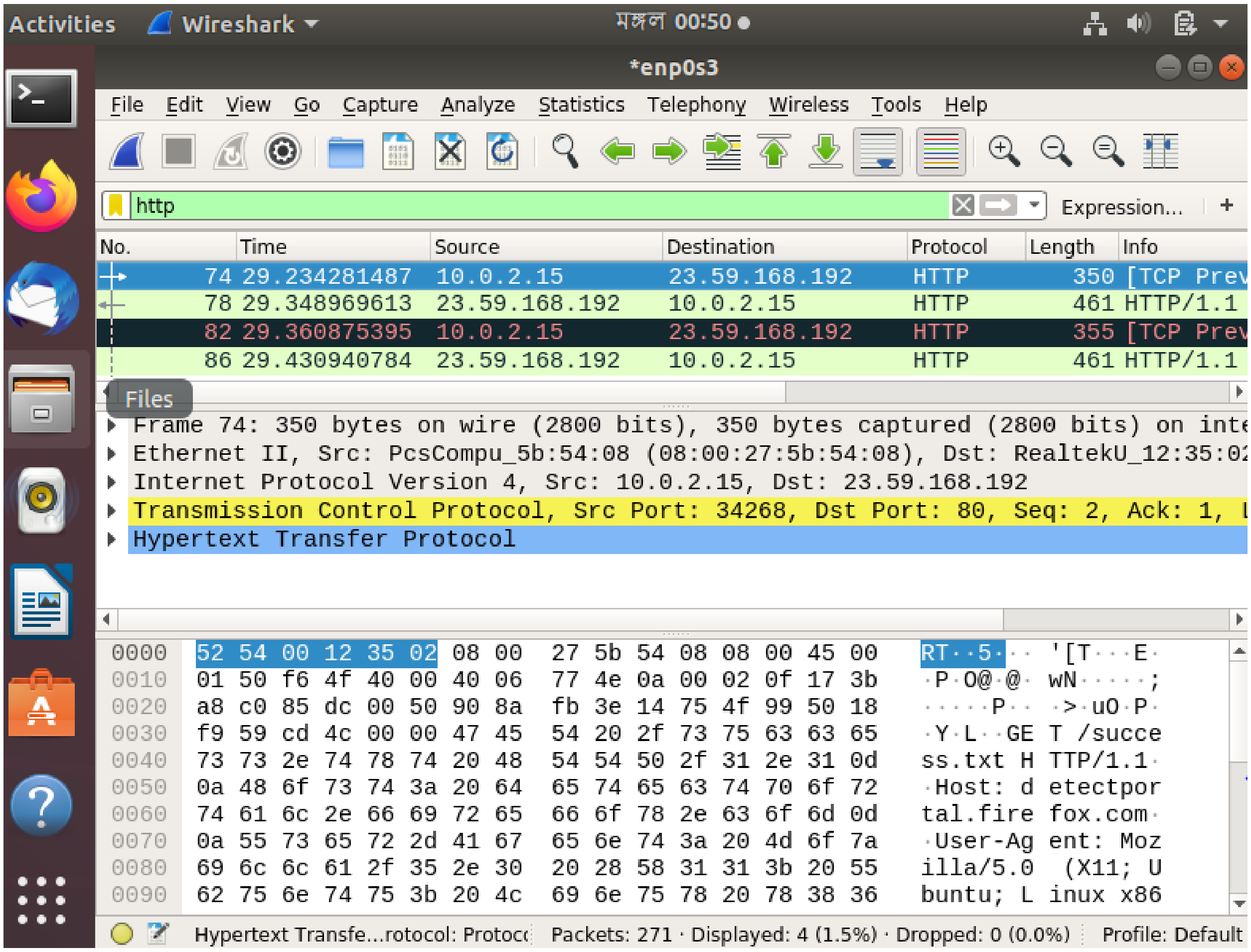
```
▸ Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface
▸ Ethernet II, Src: PcsCompu_5b:54:08 (08:00:27:5b:54:08), Dst: RealtekU_12:35:02
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.0.1
▸ User Datagram Protocol, Src Port: 47564, Dst Port: 53
▸ Domain Name System (query)
```

```
0000  52 54 00 12 35 02 08 00  27 5b 54 08 08 00 45 00   RT··5···'[T···E·
0010  00 47 cf 7e 40 00 40 11  9e 6f 0a 00 02 0f c0 a8   ·G·~@·@· ·o······
0020  00 01 b9 cc 00 35 00 33  cc fc 15 7b 01 00 00 01   ·····5·3 ···{····
0030  00 00 00 00 00 01 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0040  65 03 63 6f 6d 00 00 01  00 01 00 00 29 02 00 00   e·com··· ····)···
0050  00 00 00 00 00                                      ·····
```

wireshark_enp0s3_202...002746_WFE5LU.pcapng   Packets: 341 · Displayed: 341 (100.0%)   Profile: Default

Filtering :

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


Activities
Wireshark
मङ्गल 00:50
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+
Files

```
http
```

```
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
```

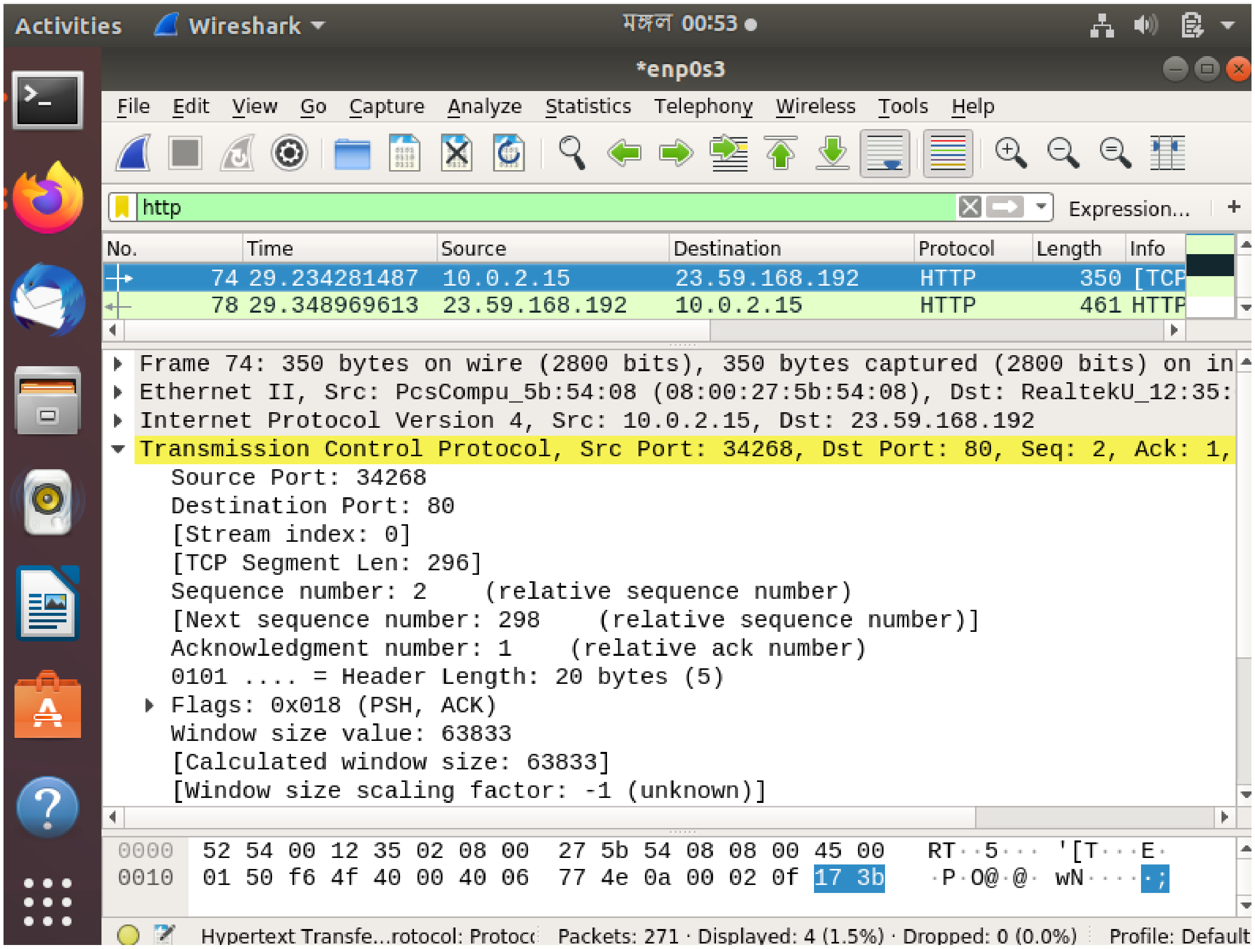
```
▸ Frame 74: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits) on inte
▸ Ethernet II, Src: PcsCompu_5b:54:08 (08:00:27:5b:54:08), Dst: RealtekU_12:35:02
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 23.59.168.192
▸ Transmission Control Protocol, Src Port: 34268, Dst Port: 80, Seq: 2, Ack: 1, L
▸ 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·O@·@· wN·····;
0020  a8 c0 85 dc 00 50 90 8a  fb 3e 14 75 4f 99 50 18   ·····P·· ·>·uO·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: Protoco 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.



http

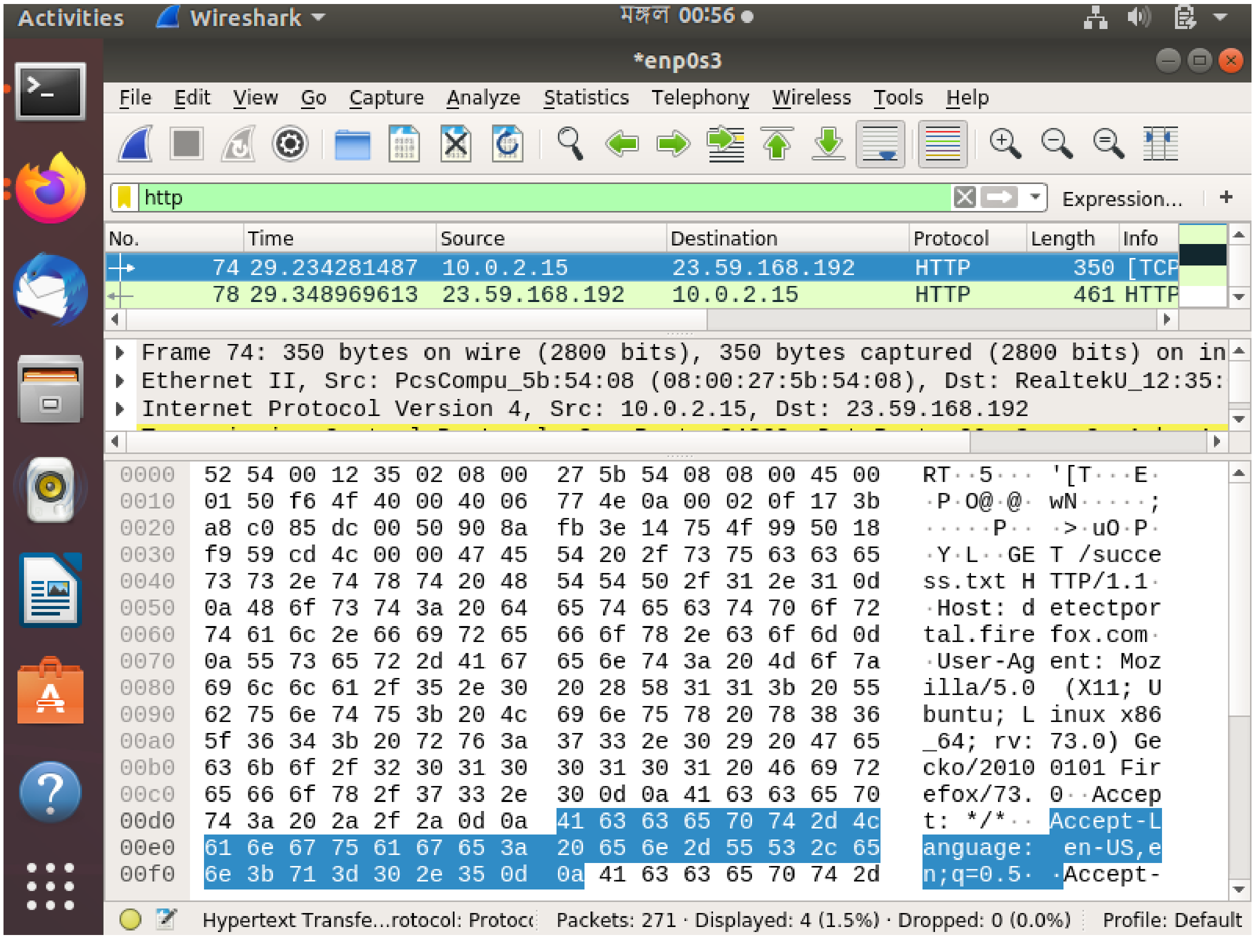
```
No.      Time             Source           Destination      Protocol   Length  Info
    74 29.234281487  10.0.2.15        23.59.168.192    HTTP          350 [TCP
    78 29.348969613  23.59.168.192    10.0.2.15        HTTP          461 HTTP
```

```
▸ 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
▾ Transmission Control Protocol, Src Port: 34268, Dst Port: 80, Seq: 2, Ack: 1,
    Source Port: 34268
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 296]
    Sequence number: 2    (relative sequence number)
    [Next sequence number: 298    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 63833
    [Calculated window size: 63833]
    [Window size scaling factor: -1 (unknown)]
```

```
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·O@·@· wN·····;
```

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

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



Activities
Wireshark
मङ्गल 00:56
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…
+

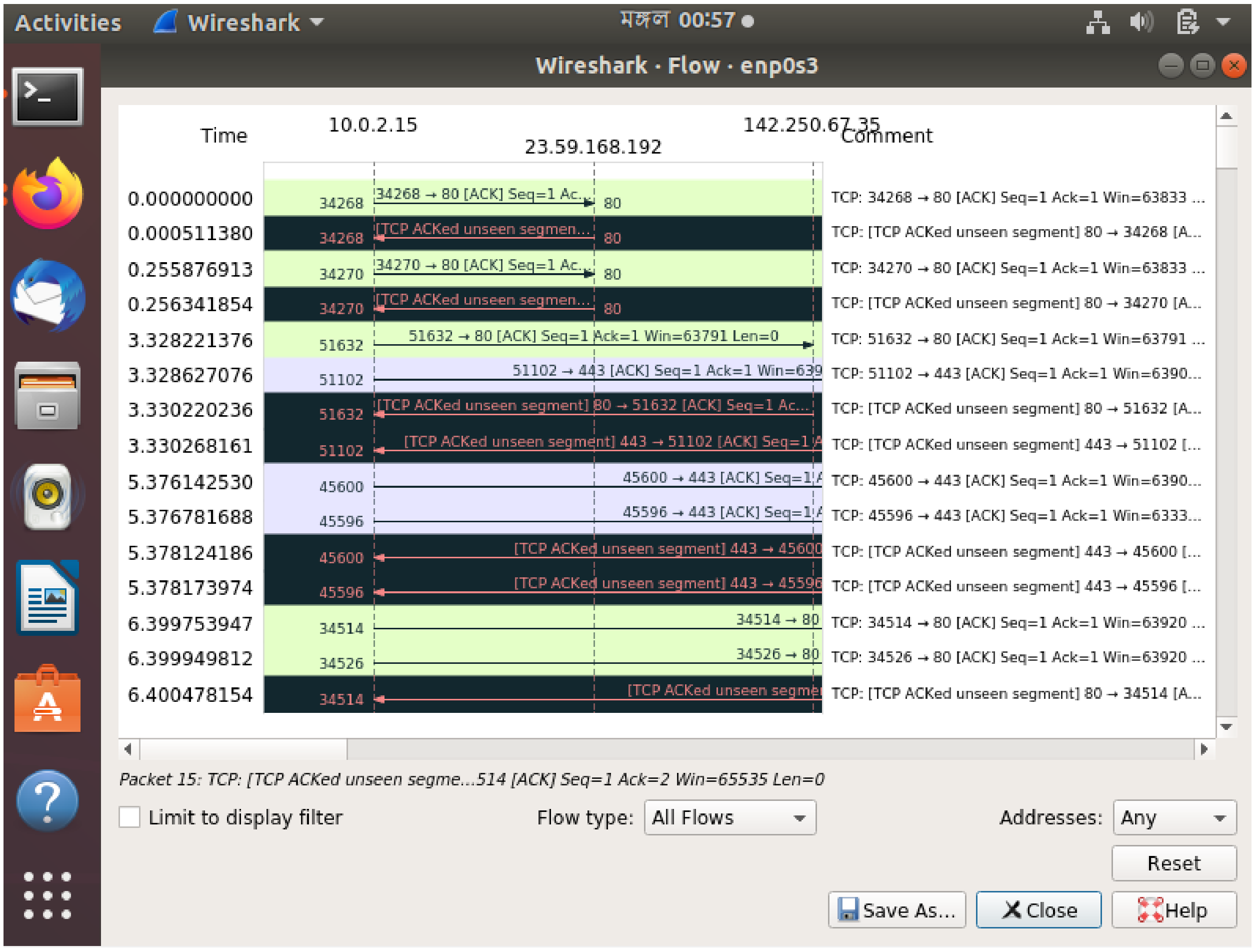
```
No.       Time          Source          Destination     Protocol  Length Info
      74 29.234281487  10.0.2.15       23.59.168.192   HTTP         350 [TCP
      78 29.348969613  23.59.168.192   10.0.2.15       HTTP         461 HTTP
```

```
▸ 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
```

```
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·O@·@· wN·····;
0020  a8 c0 85 dc 00 50 90 8a  fb 3e 14 75 4f 99 50 18   ·····P·· ·>·uO·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
00a0  5f 36 34 3b 20 72 76 3a  37 33 2e 30 29 20 47 65   _64; rv: 73.0) Ge
00b0  63 6b 6f 2f 32 30 31 30  30 31 30 31 20 46 69 72   cko/2010 0101 Fir
00c0  65 66 6f 78 2f 37 33 2e  30 0d 0a 41 63 63 65 70   efox/73. 0··Accep
00d0  74 3a 20 2a 2f 2a 0d 0a  41 63 63 65 70 74 2d 4c   t: */*·· Accept-L
00e0  61 6e 67 75 61 67 65 3a  20 65 6e 2d 55 53 2c 65   anguage:  en-US,e
00f0  6e 3b 71 3d 30 2e 35 0d  0a 41 63 63 65 70 74 2d   n;q=0.5· ·Accept-
```

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

Statistics – Flow Graph Example :



Time	10.0.2.15	23.59.168.192		142.250.67.35	Comment
0.000000000	34268	34268 → 80 [ACK] Seq=1 Ac...	80		TCP: 34268 → 80 [ACK] Seq=1 Ack=1 Win=63833 ...
0.000511380	34268	[TCP ACKed unseen segmen...	80		TCP: [TCP ACKed unseen segment] 80 → 34268 [A...
0.255876913	34270	34270 → 80 [ACK] Seq=1 Ac...	80		TCP: 34270 → 80 [ACK] Seq=1 Ack=1 Win=63833 ...
0.256341854	34270	[TCP ACKed unseen segmen...	80		TCP: [TCP ACKed unseen segment] 80 → 34270 [A...
3.328221376	51632	51632 → 80 [ACK] Seq=1 Ack=1 Win=63791 Len=0			TCP: 51632 → 80 [ACK] Seq=1 Ack=1 Win=63791 ...
3.328627076	51102	51102 → 443 [ACK] Seq=1 Ack=1 Win=639			TCP: 51102 → 443 [ACK] Seq=1 Ack=1 Win=6390...
3.330220236	51632	[TCP ACKed unseen segment] 80 → 51632 [ACK] Seq=1 Ac...			TCP: [TCP ACKed unseen segment] 80 → 51632 [A...
3.330268161	51102	[TCP ACKed unseen segment] 443 → 51102 [ACK] Seq=1 A			TCP: [TCP ACKed unseen segment] 443 → 51102 [...
5.376142530	45600	45600 → 443 [ACK] Seq=1 A			TCP: 45600 → 443 [ACK] Seq=1 Ack=1 Win=6390...
5.376781688	45596	45596 → 443 [ACK] Seq=1 A			TCP: 45596 → 443 [ACK] Seq=1 Ack=1 Win=6333...
5.378124186	45600	[TCP ACKed unseen segment] 443 → 45600			TCP: [TCP ACKed unseen segment] 443 → 45600 [...
5.378173974	45596	[TCP ACKed unseen segment] 443 → 45596			TCP: [TCP ACKed unseen segment] 443 → 45596 [...
6.399753947	34514	34514 → 80			TCP: 34514 → 80 [ACK] Seq=1 Ack=1 Win=63920 ...
6.399949812	34526	34526 → 80			TCP: 34526 → 80 [ACK] Seq=1 Ack=1 Win=63920 ...
6.400478154	34514	[TCP ACKed unseen segme			TCP: [TCP ACKed unseen segment] 80 → 34514 [A...

Packet 15: TCP: [TCP ACKed unseen segme...514 [ACK] Seq=1 Ack=2 Win=65535 Len=0

☐ Limit to display filter

Flow type: All Flows

Addresses: Any

Conclusion : Wireshark is absolutely safe to use. Government agencies, corporations, non-profits, and educational institutions use Wireshark for troubleshooting and teaching purposes. There isn’t a better way to learn networking than to look at the traffic under the Wireshark microscope. There are questions about the legality of Wireshark since it is a powerful packet sniffer. The Light side of the Force says that we should only use Wireshark on networks where we have permission to inspect network packets. Using Wireshark to look at packets without permission is a path to the Dark Side. Wireshark allows us to filter the log either before the capture starts or during analysis, so you can narrow down and zero into what you are looking for in the network trace. For example, we can set a filter to see TCP traffic between two IP addresses. We can set it only to show us the packets sent from one computer. The filters in Wireshark are one of the primary reasons it became the standard tool for packet analysis. Wireshark is implemented in ANSI C, which is vulnerable to security problems like buffer overflows (compared to more securely designed languages like Java or C#). ANSI C is used for several reasons; the main reason is performance, as Wireshark is often used to work with huge amounts of data.