

## Lab Report No: 02

**Lab Report Name:** Introduction to protocol analysis with wireshark.

Name : Binodon

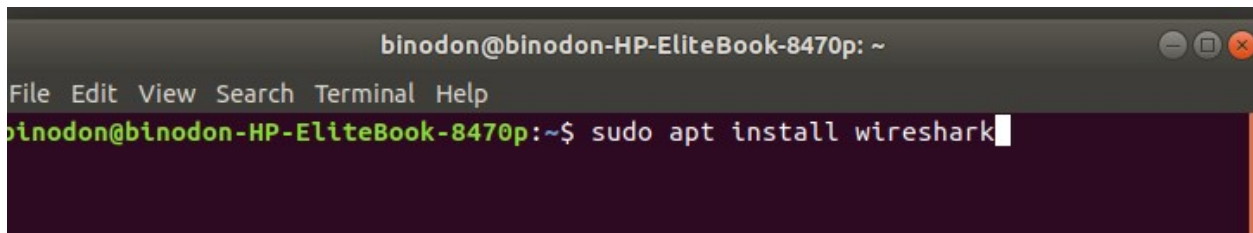
ID : IT-17046

### Objective:-

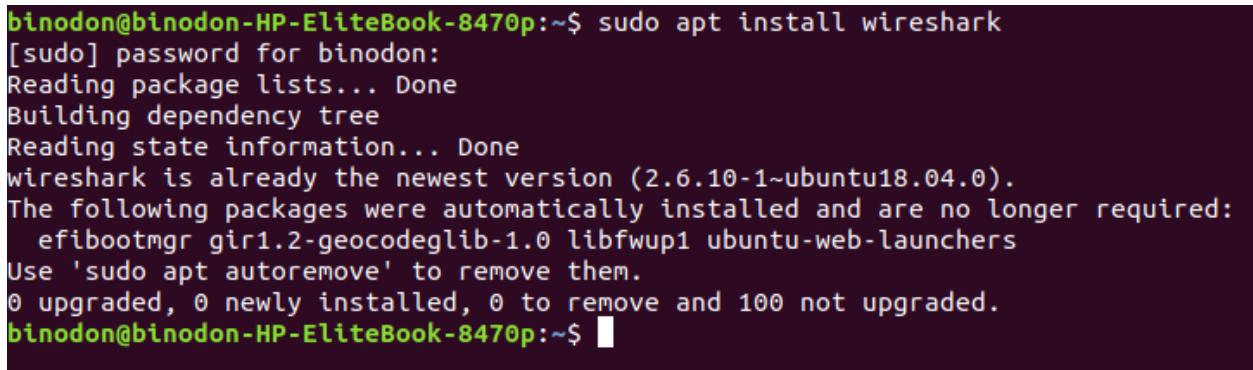
In this lab we will learn about installation process of Wireshark in Linux. After completion of installation Apply capturing on Wireshark.

First of All We are going to Discuss about the installation process of **Wireshark**.  
Current stable release of Wireshark 3.2.5 has been used.

Step 1: Open the linux Terminal and Apply the followed code below.

A terminal window titled 'binodon@binodon-HP-EliteBook-8470p: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The command 'sudo apt install wireshark' is entered at the prompt.

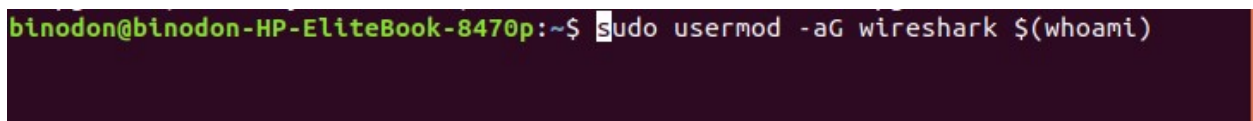
```
binodon@binodon-HP-EliteBook-8470p: ~  
File Edit View Search Terminal Help  
binodon@binodon-HP-EliteBook-8470p:~$ sudo apt install wireshark
```

The terminal window shows the output of the 'sudo apt install wireshark' command. It indicates that Wireshark is already the newest version and lists packages that are no longer required.

```
binodon@binodon-HP-EliteBook-8470p:~$ sudo apt install wireshark  
[sudo] password for binodon:  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
wireshark is already the newest version (2.6.10-1~ubuntu18.04.0).  
The following packages were automatically installed and are no longer required:  
  efibootmgr gir1.2-geocodeglib-1.0 libfwup1 ubuntu-web-launchers  
Use 'sudo apt autoremove' to remove them.  
0 upgraded, 0 newly installed, 0 to remove and 100 not upgraded.  
binodon@binodon-HP-EliteBook-8470p:~$
```

I have already installed So It is showing this type of announcement. When You will try for the first time then you will get an icon Y/N. You simply press Y. Then it will start installing.

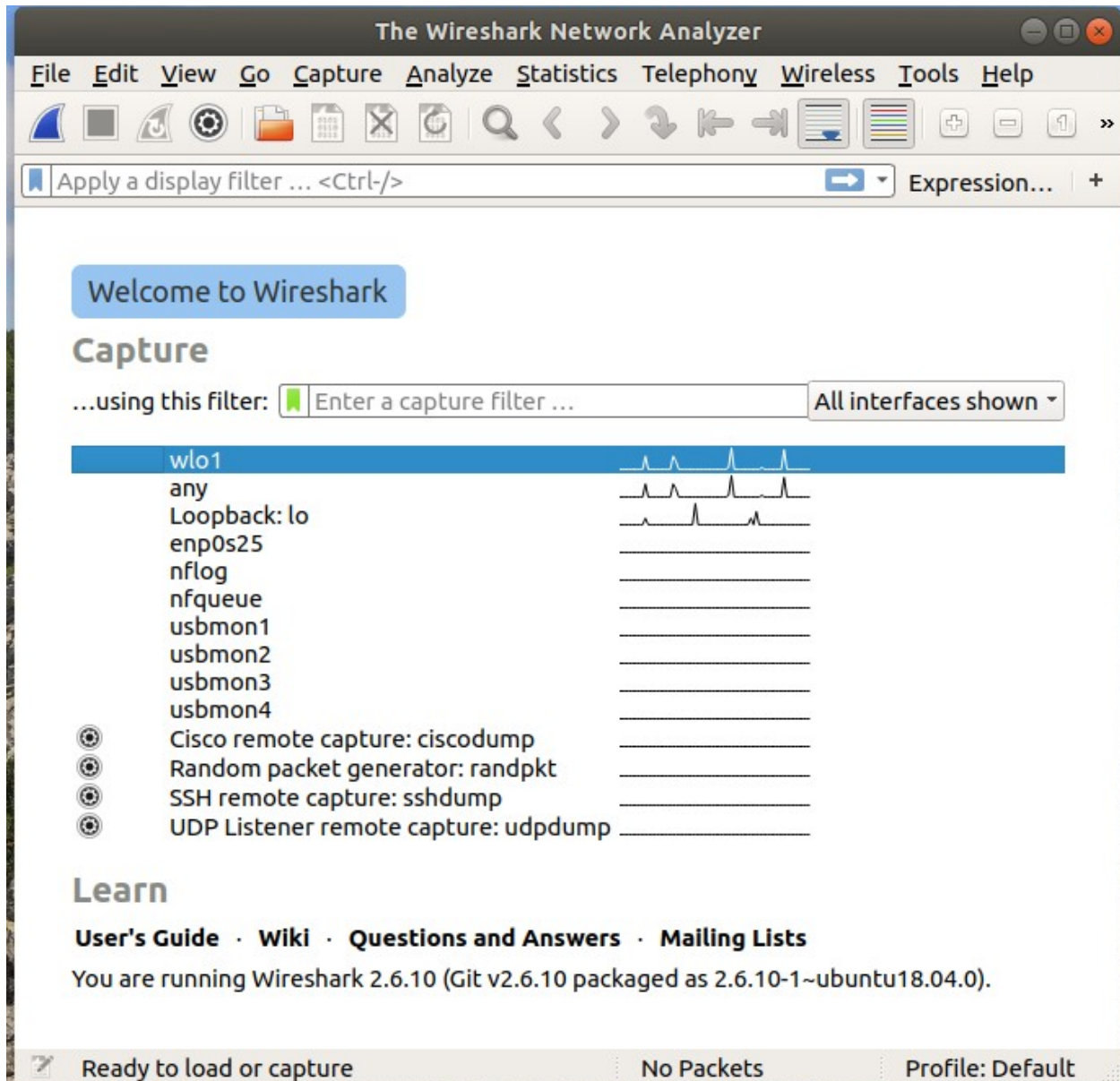
Step 2:

The terminal window shows the command 'sudo usermod -aG wireshark \$(whoami)' being entered at the prompt.

```
binodon@binodon-HP-EliteBook-8470p:~$ sudo usermod -aG wireshark $(whoami)
```

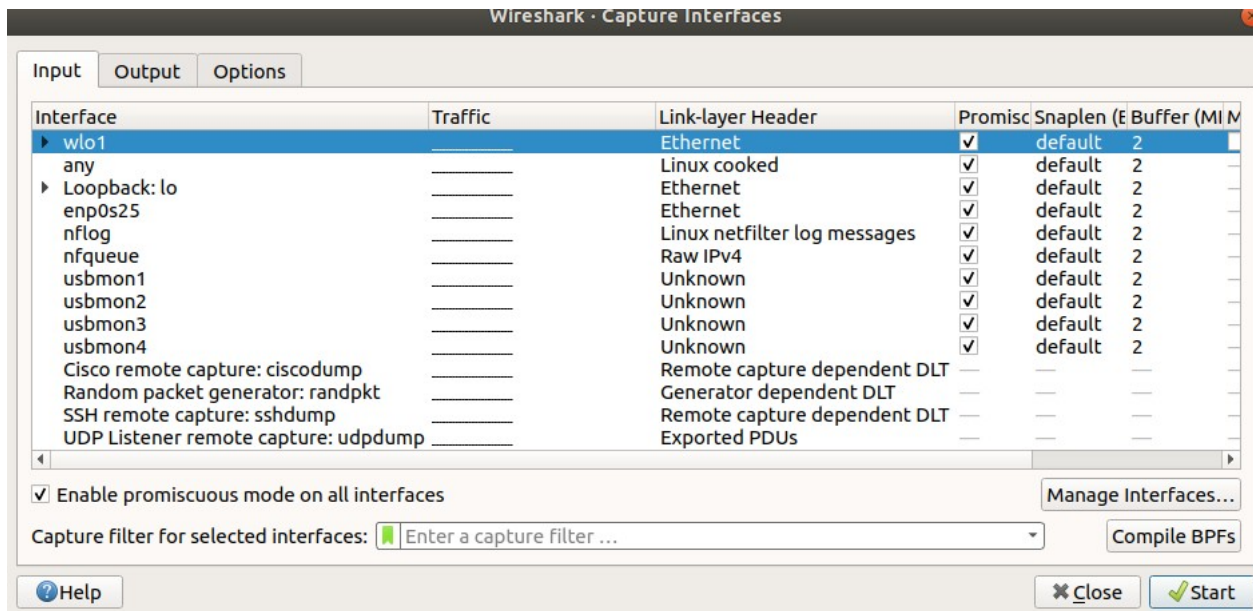
Now The process has been completed successfully.

## Wireshark Main window:

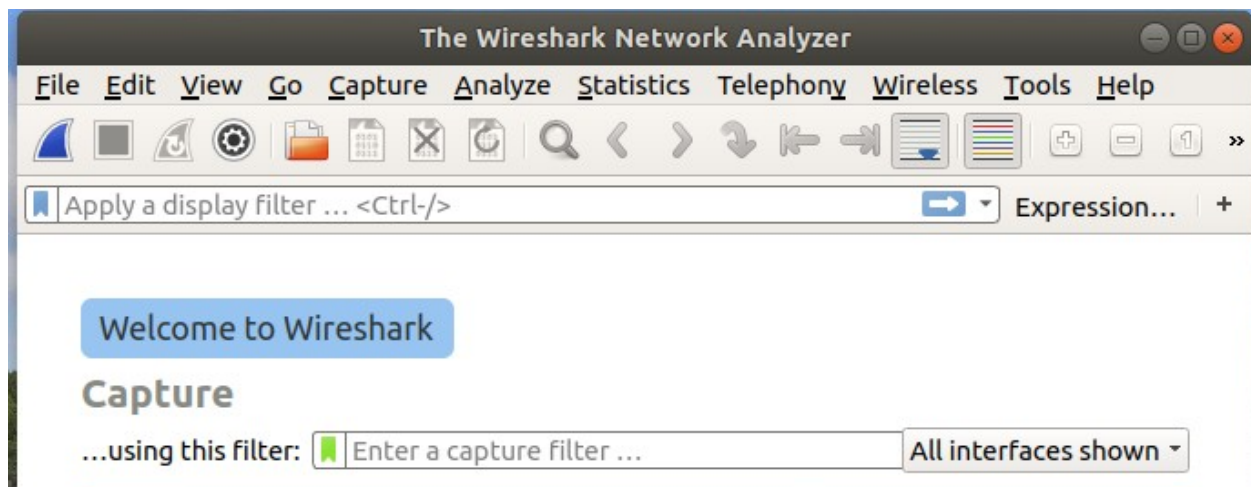


## Capturing :

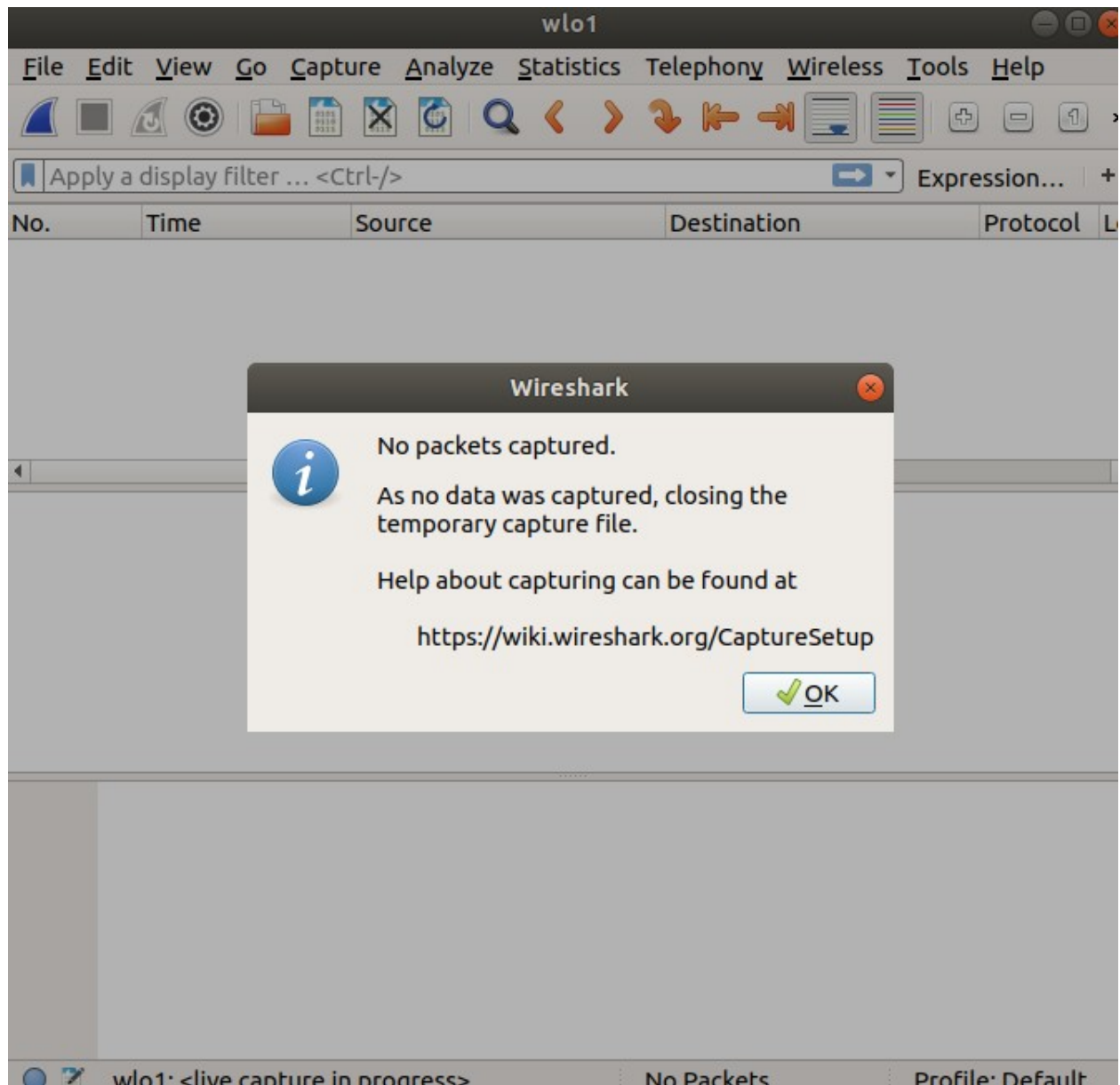
To capture go to capture Option. Capturing window will be appeared. Then select capture menu select option. Start capturing on interface that has IP address.



Select this option then start Capturing



When Capturing is started in the meantime a blank screen will appear like this.



It will be blank until the data will exchange through NIC.

When package exchanged on NIC. Then it turns on a new window

The image shows a Wireshark network traffic capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. A filter bar at the top of the packet list shows "Apply a display filter ... <Ctrl-/>" and "Expression...".

The packet list table shows the following data:

No.	Time	Source	Destination	Protocol
348	26.213203220	192.168.0.101	224.0.0.251	MDNS
349	33.143507801	172.217.194.189	192.168.0.104	TLSv1.2
350	33.143567708	192.168.0.104	172.217.194.189	TCP
351	39.283392989	192.168.0.104	74.125.68.139	TLSv1.2
352	39.343006494	74.125.68.139	192.168.0.104	TCP
353	39.343064035	74.125.68.139	192.168.0.104	TLSv1.2
354	39.343096050	192.168.0.104	74.125.68.139	TCP

The packet details pane shows the following information for the selected packet (Frame 1):

- Frame 1: 317 bytes on wire (2536 bits), 317 bytes captured (2536 bits) on
- Ethernet II, Src: Tp-LinkT\_4e:7d:24 (f4:f2:6d:4e:7d:24), Dst: IPv4mcast\_7
- Internet Protocol Version 4, Src: 192.168.0.1, Dst: 239.255.255.250
- User Datagram Protocol, Src Port: 52370, Dst Port: 1900
- Simple Service Discovery Protocol

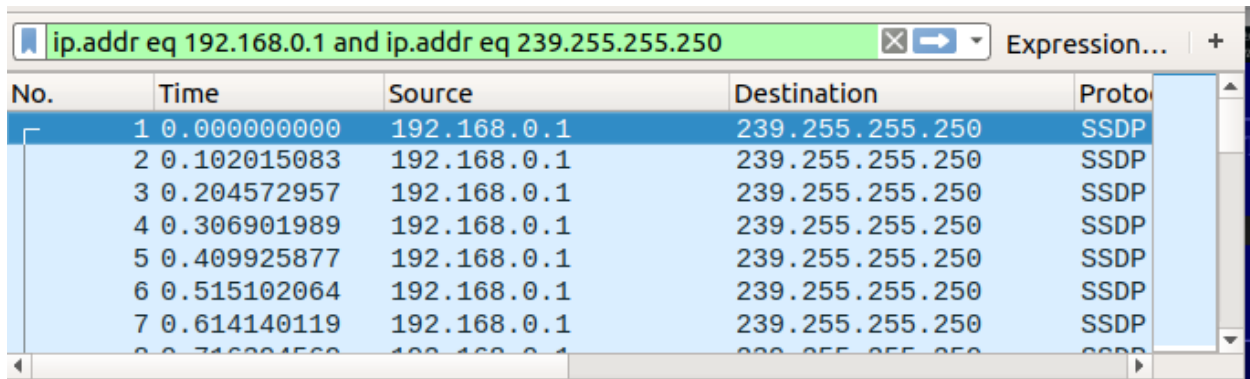
The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 01 00 5e 7f ff fa f4 f2 6d 4e 7d 24 08 00 45 00 ..^.... mN}$..E
0010 01 2f 00 00 40 00 04 11 c5 1a c0 a8 00 01 ef ff ./...@... ..
0020 ff fa cc 92 07 6c 01 1b b4 5f 4e 4f 54 49 46 59 ....1.. _NOTIF
0030 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 4f 53 * HTTP/ 1.1..HC
0040 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 2e 32 T: 239.2 55.255.
0050 35 30 3a 31 39 30 30 0d 0a 43 41 43 48 45 2d 43 50:1900.. CACHE-
0060 4f 4e 54 52 4f 4c 3a 20 6d 61 78 2d 61 67 65 3d ONTROL: max-age
0070 31 30 30 0d 0a 4c 4f 43 41 54 49 4f 4e 3a 20 68 100..LOC ATION:
0080 74 74 70 3a 2f 2f 31 39 32 2e 31 36 38 2e 30 2e ttp://19 2.168.0
```

The status bar at the bottom shows "wlo1: <live c... in progress> Packets: 354 · Displayed: 354 (100.0%) Profile: Default".



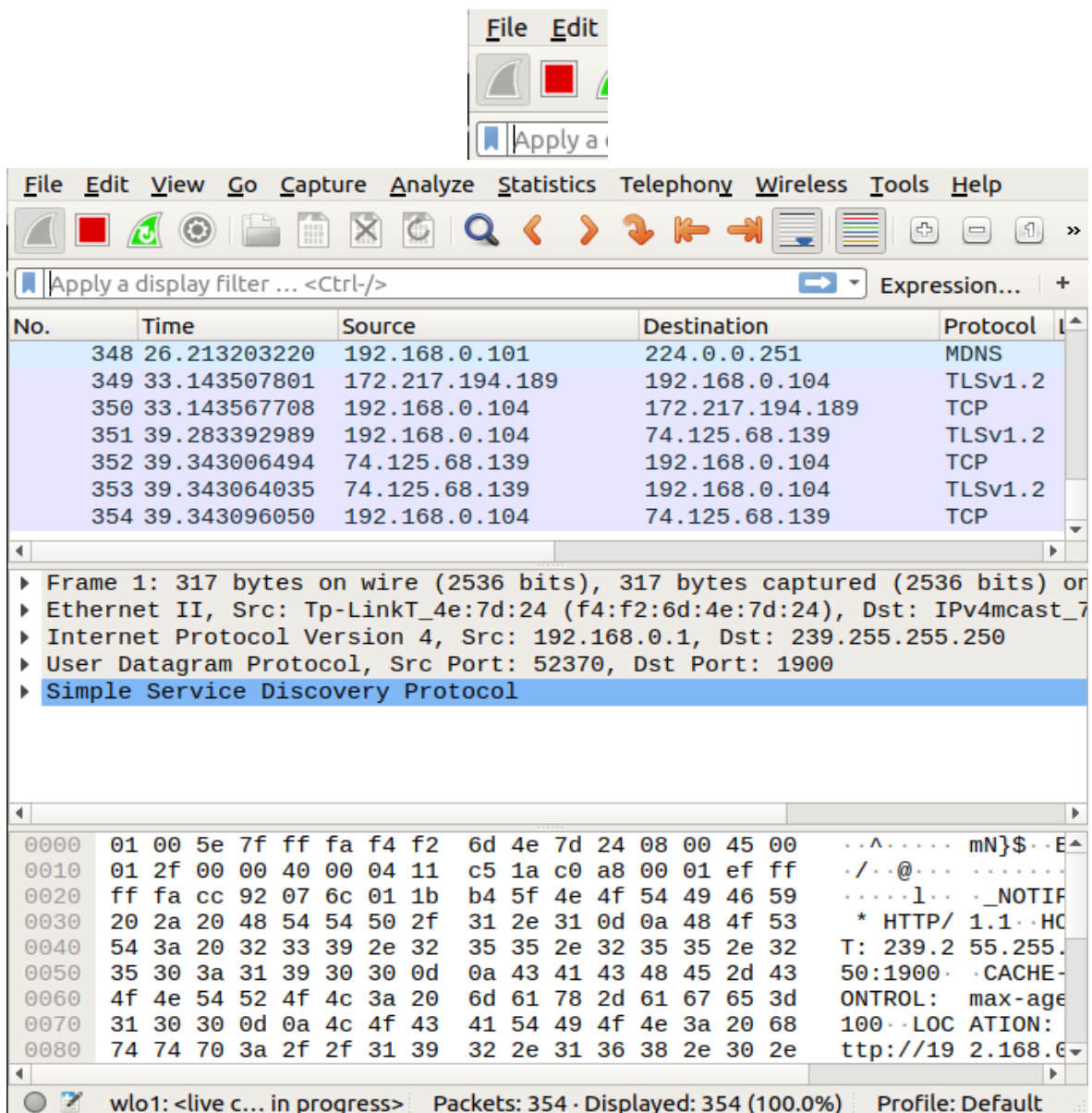
It will show The IP address also.



No.	Time	Source	Destination	Protocol
1	0.000000000	192.168.0.1	239.255.255.250	SSDP
2	0.102015083	192.168.0.1	239.255.255.250	SSDP
3	0.204572957	192.168.0.1	239.255.255.250	SSDP
4	0.306901989	192.168.0.1	239.255.255.250	SSDP
5	0.409925877	192.168.0.1	239.255.255.250	SSDP
6	0.515102064	192.168.0.1	239.255.255.250	SSDP
7	0.614140119	192.168.0.1	239.255.255.250	SSDP

### Stopping capture:

Capture can be stopped by clicking stop



The image shows the Wireshark interface with the 'File' and 'Edit' menus at the top. The toolbar includes a red square stop button. The main window displays a packet capture with a display filter 'ip.addr eq 192.168.0.1 and ip.addr eq 239.255.255.250'. The packet list shows several packets, including an SSDP packet (No. 348) and a TCP packet (No. 354). The packet details pane shows the structure of the selected packet (No. 348), which is an SSDP packet. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol
348	26.213203220	192.168.0.101	224.0.0.251	MDNS
349	33.143507801	172.217.194.189	192.168.0.104	TLSv1.2
350	33.143567708	192.168.0.104	172.217.194.189	TCP
351	39.283392989	192.168.0.104	74.125.68.139	TLSv1.2
352	39.343006494	74.125.68.139	192.168.0.104	TCP
353	39.343064035	74.125.68.139	192.168.0.104	TLSv1.2
354	39.343096050	192.168.0.104	74.125.68.139	TCP

Frame 1: 317 bytes on wire (2536 bits), 317 bytes captured (2536 bits) on  
Ethernet II, Src: Tp-LinkT\_4e:7d:24 (f4:f2:6d:4e:7d:24), Dst: IPv4mcast\_7  
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 239.255.255.250  
User Datagram Protocol, Src Port: 52370, Dst Port: 1900  
Simple Service Discovery Protocol

0000 01 00 5e 7f ff fa f4 f2 6d 4e 7d 24 08 00 45 00 ..^.... mN}\$..E  
0010 01 2f 00 00 40 00 04 11 c5 1a c0 a8 00 01 ef ff ./..@... ..  
0020 ff fa cc 92 07 6c 01 1b b4 5f 4e 4f 54 49 46 59 ....1.. \_NOTIF  
0030 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 4f 53 \* HTTP/ 1.1..HC  
0040 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 2e 32 T: 239.2 55.255.  
0050 35 30 3a 31 39 30 30 0d 0a 43 41 43 48 45 2d 43 50:1900.. CACHE-  
0060 4f 4e 54 52 4f 4c 3a 20 6d 61 78 2d 61 67 65 3d ONTROL: max-age  
0070 31 30 30 0d 0a 4c 4f 43 41 54 49 4f 4e 3a 20 68 100..LOC ATION:  
0080 74 74 70 3a 2f 2f 31 39 32 2e 31 36 38 2e 30 2e ttp://19 2.168.6

## Protocol analysis with examples:

The image shows a Wireshark packet capture of a Simple Service Discovery Protocol (SSDP) message. The packet list on the left shows a packet of type 'HTTP' with a length of 130 bytes. The packet details pane on the right shows the structure of the message, including the 'NOTIFY' action, the host address, cache control, location, and the server information.

**Simple Service Discovery Protocol**

- NOTIFY \* HTTP/1.1\r\n
- HOST: 239.255.255.250:1900\r\n
- CACHE-CONTROL: max-age=100\r\n
- LOCATION: http://192.168.0.1:1900/igd.xml\r\n
- NT: upnp:rootdevice\r\n
- NTS: ssdp:alive\r\n
- SERVER: ipos/7.0 UPnP/1.0 TL-WR740N/TL-WR741ND/6.0\r\n
- USN: uuid:060b7353-fca6-4070-85f4-1fbfb9add62c::upnp:rootdevice\r\n

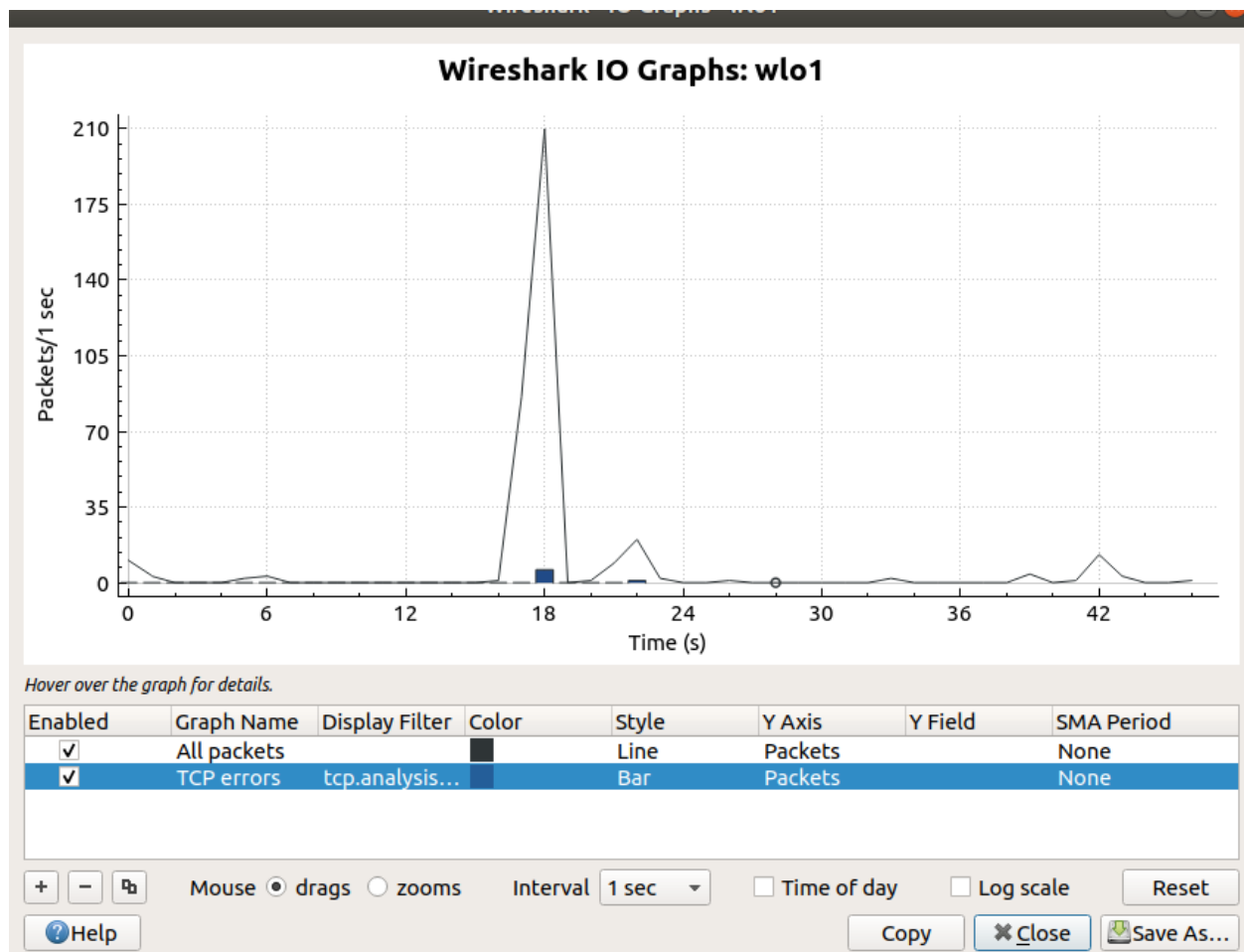
**Packet 130 (00c0):**

Offset	Hex	ASCII
00c0	6c 69 76 65 0d 0a 53 45 52 56 45 52 3a 20 69 70	live..SE RVER: i
00d0	6f 73 2f 37 2e 30 20 55 50 6e 50 2f 31 2e 30 20	os/7.0 U PnP/1.0
00e0	54 4c 2d 57 52 37 34 30 4e 2f 54 4c 2d 57 52 37	TL-WR740 N/TL-WR
00f0	34 31 4e 44 2f 36 2e 30 0d 0a 55 53 4e 3a 20 75	41ND/6.0 ..USN:
0100	75 69 64 3a 30 36 30 62 37 33 35 33 2d 66 63 61	uid:060b 7353-fc
0110	36 2d 34 30 37 30 2d 38 35 66 34 2d 31 66 62 66	6-4070-8 5f4-1fb
0120	62 39 61 64 64 36 32 63 3a 3a 75 70 6e 70 3a 72	b9add62c ::upnp:
0130	6f 6f 74 64 65 76 69 63 65 0d 0a 0d 0a	ootdevic e....

HTTP...ytes: Packets: 372 · Displayed: 39 (10.5%) · Dropped: 0 (0.0%) Profile: Default

Graph and plots are also available on statistics menu.

Wireshark I/O graph:



**Conclusion:** In this lab we come to learn about Installation of wireshark in Ubuntu,Capturing as well as statistics. To do this lab we did not face any problem.