NETWORKING & SYSTEM ADMINISTRATION LAB

Name: SWETHA PRAKASH

Roll No: 46

Batch: B

Date: 06/06/2022

Experiment No.: 22

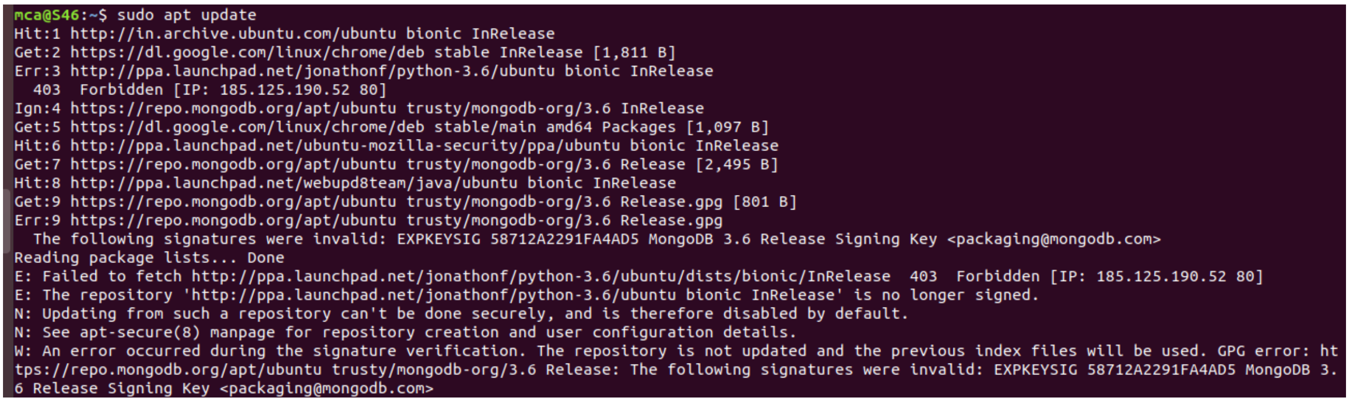
Aim

Install and use the latest version of Wireshark on Ubuntu.

Procedure

Step 1 : First update the APT package repository cache with the following command.

- **sudo apt update**

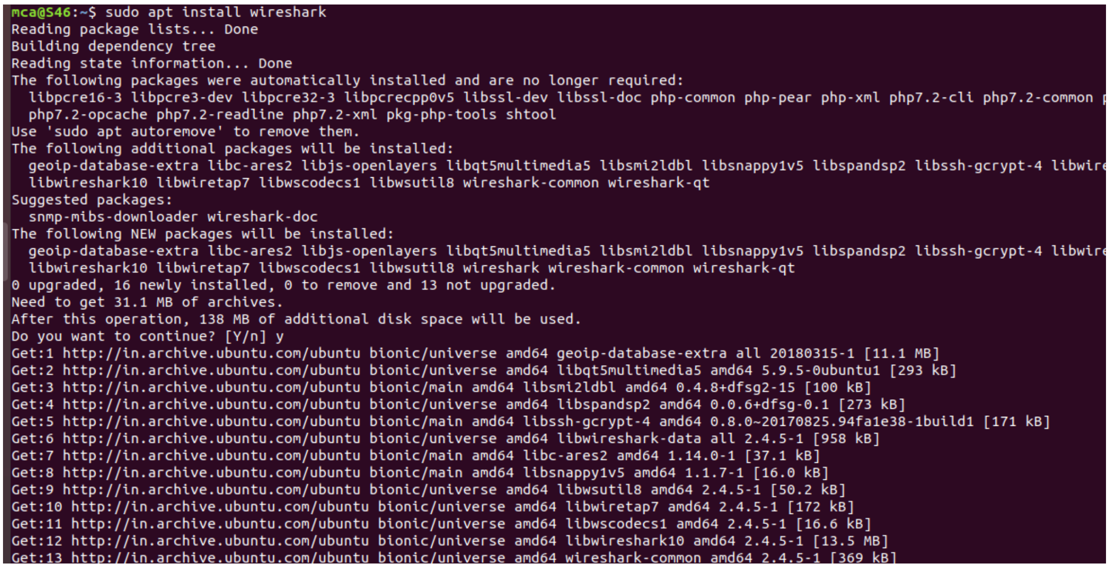


```
mca@S46:~$ sudo apt update
Hit:1 http://in.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 https://dl.google.com/linux/chrome/deb stable InRelease [1,811 B]
Err:3 http://ppa.launchpad.net/jonathonf/python-3.6/ubuntu bionic InRelease
  403  Forbidden [IP: 185.125.190.52 80]
Ign:4 https://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.6 InRelease
Get:5 https://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1,097 B]
Hit:6 http://ppa.launchpad.net/ubuntu-mozilla-security/ppa/ubuntu bionic InRelease
Get:7 https://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.6 Release [2,495 B]
Hit:8 http://ppa.launchpad.net/webupd8team/java/ubuntu bionic InRelease
Get:9 https://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.6 Release.gpg [801 B]
Err:9 https://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.6 Release.gpg
  The following signatures were invalid: EXPKEYSIG 58712A2291FA4AD5 MongoDB 3.6 Release Signing Key <packaging@mongodb.com>
Reading package lists... Done
E: Failed to fetch http://ppa.launchpad.net/jonathonf/python-3.6/ubuntu/dists/bionic/InRelease  403  Forbidden [IP: 185.125.190.52 80]
E: The repository 'http://ppa.launchpad.net/jonathonf/python-3.6/ubuntu bionic InRelease' is no longer signed.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
W: An error occurred during the signature verification. The repository is not updated and the previous index files will be used. GPG error: ht
tps://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.6 Release: The following signatures were invalid: EXPKEYSIG 58712A2291FA4AD5 MongoDB 3.
6 Release Signing Key <packaging@mongodb.com>
```

Step 2 : Now, run the following command to install Wireshark on the Ubuntu machine

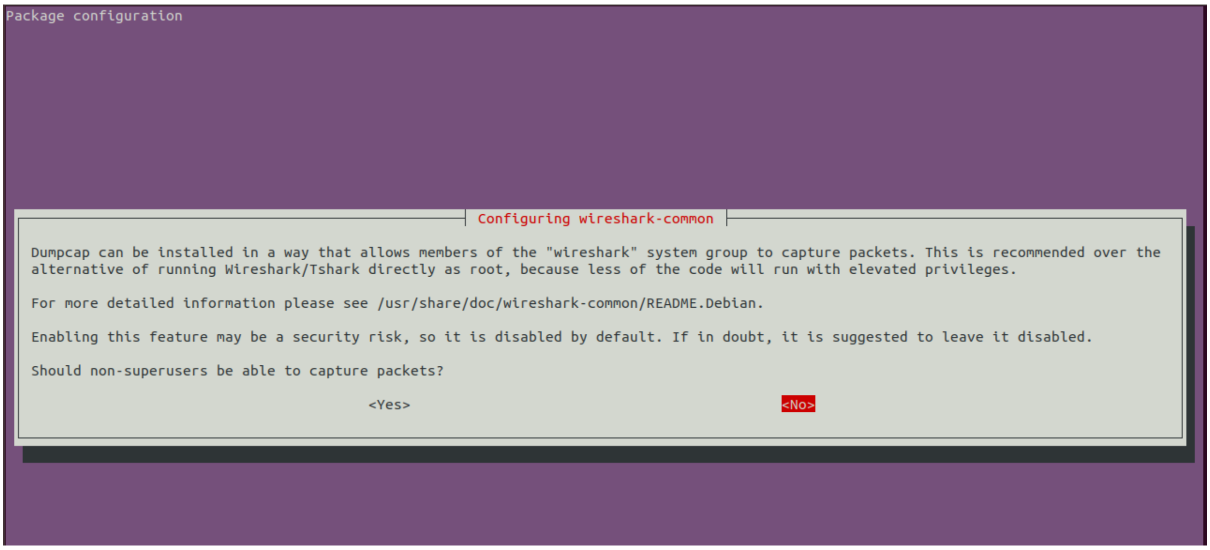
- **sudo apt install wireshark**

Now press **y** and then press **Enter.**



```
mca@S46:~$ sudo apt install wireshark
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libpcre16-3 libpcre3-dev libpcre32-3 libpcrecpp0v5 libssl-dev libssl-doc php-common php-pear php-xml php7.2-cli php7.2-common p
  php7.2-opcache php7.2-readline php7.2-xml pkg-php-tools shtool
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  geoip-database-extra libc-ares2 libjs-openlayers libqt5multimedia5 libsmi2ldbl libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwire
  libwireshark10 libwiretap7 libwscodecs1 libwsutil8 wireshark-common wireshark-qt
Suggested packages:
  snmp-mibs-downloader wireshark-doc
The following NEW packages will be installed:
  geoip-database-extra libc-ares2 libjs-openlayers libqt5multimedia5 libsmi2ldbl libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwire
  libwireshark10 libwiretap7 libwscodecs1 libwsutil8 wireshark wireshark-common wireshark-qt
0 upgraded, 16 newly installed, 0 to remove and 13 not upgraded.
Need to get 31.1 MB of archives.
After this operation, 138 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 geoip-database-extra all 20180315-1 [11.1 MB]
Get:2 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libqt5multimedia5 amd64 5.9.5-0ubuntu1 [293 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 libsmi2ldbl amd64 0.4.8+dfsg2-15 [100 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libspandsp2 amd64 0.0.6+dfsg-0.1 [273 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 libssh-gcrypt-4 amd64 0.8.0~20170825.94fa1e38-1build1 [171 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libwireshark-data all 2.4.5-1 [958 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 libc-ares2 amd64 1.14.0-1 [37.1 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 libsnappy1v5 amd64 1.1.7-1 [16.0 kB]
Get:9 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libwsutil8 amd64 2.4.5-1 [50.2 kB]
Get:10 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libwiretap7 amd64 2.4.5-1 [172 kB]
Get:11 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libwscodecs1 amd64 2.4.5-1 [16.6 kB]
Get:12 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libwireshark10 amd64 2.4.5-1 [13.5 MB]
Get:13 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 wireshark-common amd64 2.4.5-1 [369 kB]
```

Step 3 : By default, Wireshark must be started as root privileges in order to work. If you want to run Wireshark without root privileges or without sudo, then select **Yes** and press **Enter**.

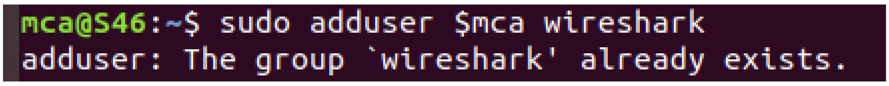


```
Dumpcap can be installed in a way that allows members of the "wireshark" system group to capture packets. This is recommended over the
alternative of running Wireshark/Tshark directly as root, because less of the code will run with elevated privileges.

For more detailed information please see /usr/share/doc/wireshark-common/README.Debian.

Enabling this feature may be a security risk, so it is disabled by default. If in doubt, it is suggested to leave it disabled.

Should non-superusers be able to capture packets?
```

Wireshark should be installed.

Step 4 : Now run the following command to add user to the **wireshark** group:

- **sudo adduser $mca wireshark**



```
mca@S46:~$ sudo adduser $mca wireshark
adduser: The group `wireshark' already exists.
```

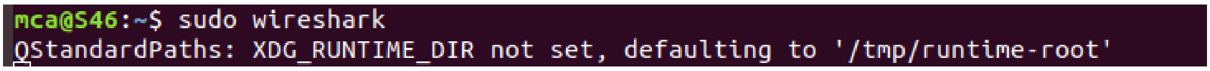
Step 5 : Finally, reboot our computer with the following command:

- **sudo reboot**

Step 6 : Now that Wireshark is installed, you can start Wireshark from the Application Menu of Ubuntu.

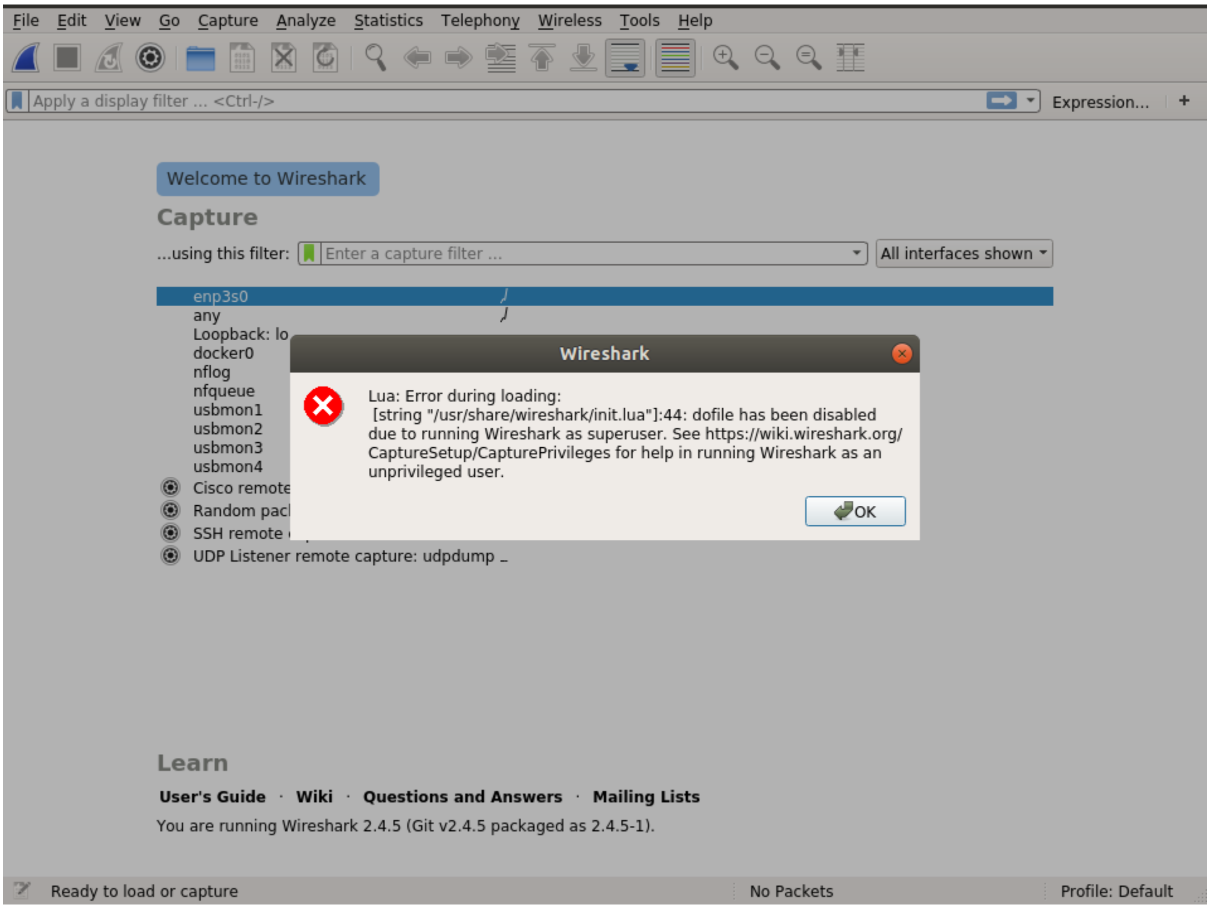
If you did not enable Wireshark to run without **root** privileges or **sudo**, then the command should be:

- **sudo wireshark**



```
mca@S46:~$ sudo wireshark
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

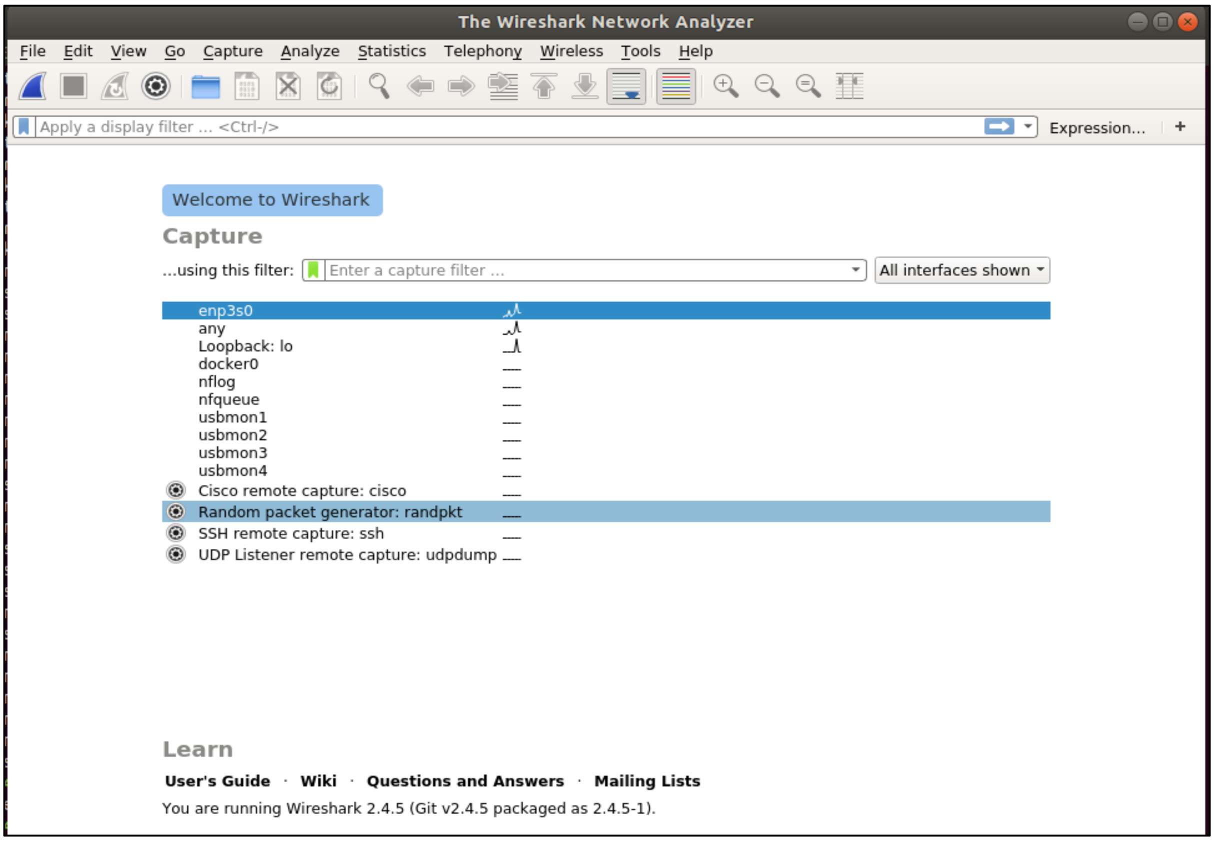
Wireshark should start.



Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:44: dofile has been disabled due to running Wireshark as superuser. See https://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark as an unprivileged user.

You are running Wireshark 2.4.5 (Git v2.4.5 packaged as 2.4.5-1).

Step 7 : When we start Wireshark, you will see a list of interfaces that you can capture packets to and from.


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

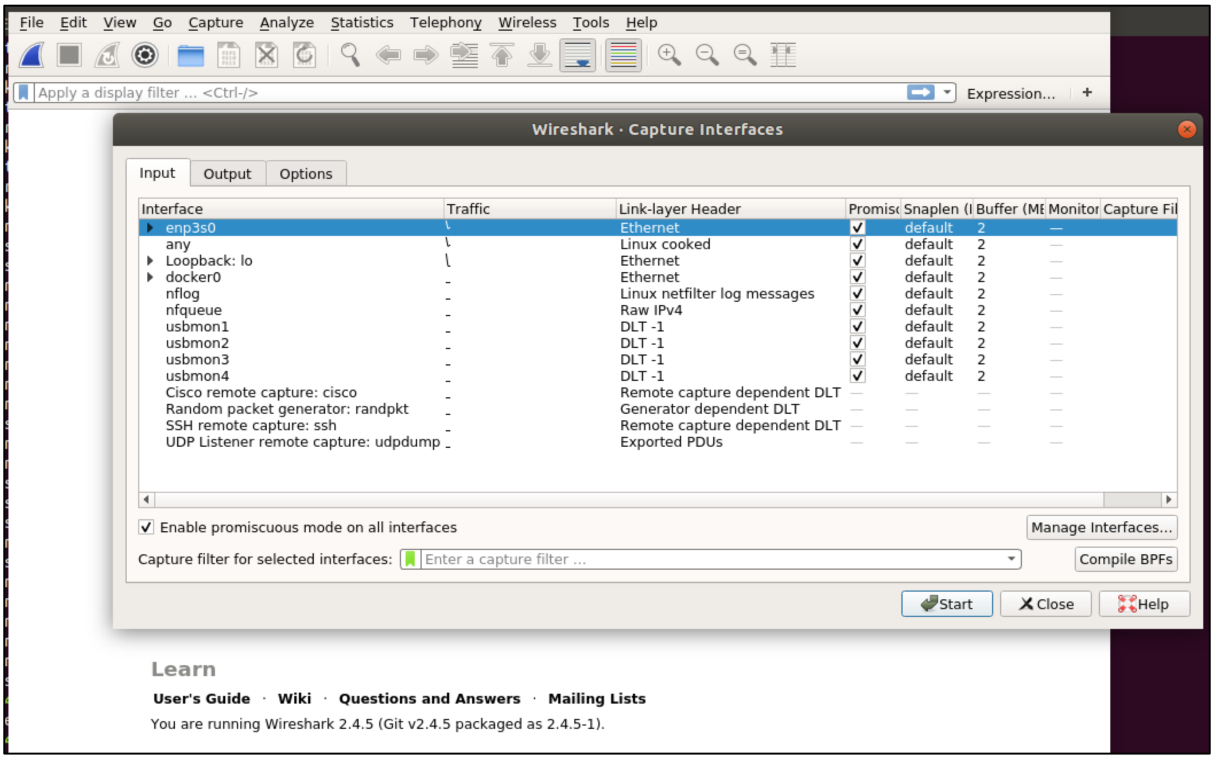
enp3s0
any
Loopback: lo
docker0
nflog
nfqueue
usbmon1
usbmon2
usbmon3
usbmon4
Cisco remote capture: cisco
Random packet generator: randpkt
SSH remote capture: ssh
UDP Listener remote capture: udpdump

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.4.5 (Git v2.4.5 packaged as 2.4.5-1).

Step 8 : Now to start capturing packets, just select the interface and click on the **Start capturing packets** icon above.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+
Wireshark · Capture Interfaces
Input
Output
Options
Manage Interfaces…
Compile BPFs
Start
Close
Help

Interface	Traffic	Link-layer Header	Promisc	Snaplen (l	Buffer (ME	Monitor	Capture Fil
enp3s0		Ethernet	☑	default	2	—	
any		Linux cooked	☑	default	2	—	
Loopback: lo		Ethernet	☑	default	2	—	
docker0		Ethernet	☑	default	2	—	
nflog		Linux netfilter log messages	☑	default	2	—	
nfqueue		Raw IPv4	☑	default	2	—	
usbmon1		DLT -1	☑	default	2	—	
usbmon2		DLT -1	☑	default	2	—	
usbmon3		DLT -1	☑	default	2	—	
usbmon4		DLT -1	☑	default	2	—	
Cisco remote capture: cisco		Remote capture dependent DLT	—	—	—	—	
Random packet generator: randpkt		Generator dependent DLT	—	—	—	—	
SSH remote capture: ssh		Remote capture dependent DLT	—	—	—	—	
UDP Listener remote capture: udpdump		Exported PDUs	—	—	—	—	

☑ Enable promiscuous mode on all interfaces

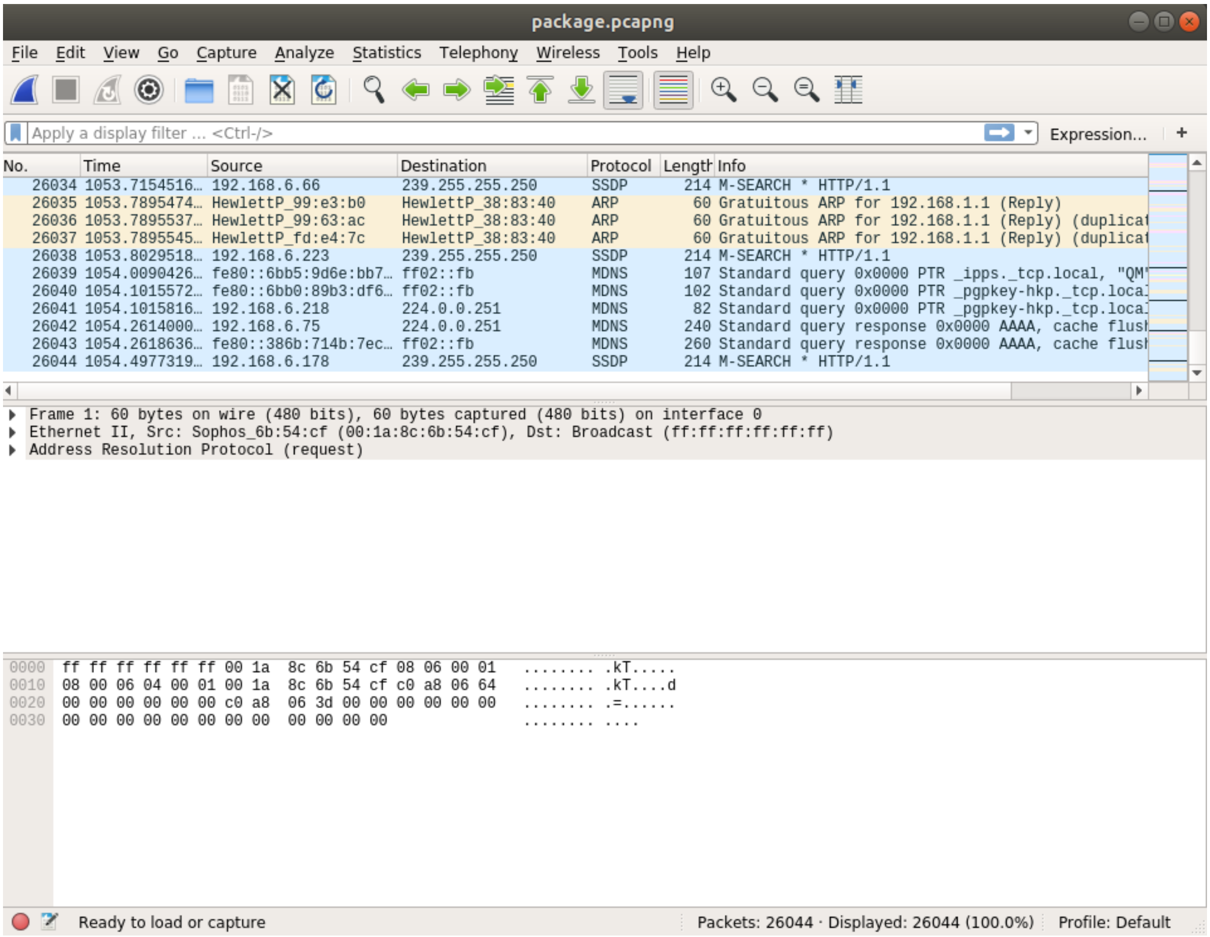
Capture filter for selected interfaces: Enter a capture filter …

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.4.5 (Git v2.4.5 packaged as 2.4.5-1).

Step 9 : We can capture packets on any network interface.


package.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

No.	Time	Source	Destination	Protocol	Length	Info
26034	1053.7154516…	192.168.6.66	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
26035	1053.7895474…	HewlettP_99:e3:b0	HewlettP_38:83:40	ARP	60	Gratuitous ARP for 192.168.1.1 (Reply)
26036	1053.7895537…	HewlettP_99:63:ac	HewlettP_38:83:40	ARP	60	Gratuitous ARP for 192.168.1.1 (Reply) (duplicat
26037	1053.7895545…	HewlettP_fd:e4:7c	HewlettP_38:83:40	ARP	60	Gratuitous ARP for 192.168.1.1 (Reply) (duplicat
26038	1053.8029518…	192.168.6.223	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
26039	1054.0090426…	fe80::6bb5:9d6e:bb7…	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM"
26040	1054.1015572…	fe80::6bb0:89b3:df6…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _pgpkey-hkp._tcp.local
26041	1054.1015816…	192.168.6.218	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _pgpkey-hkp._tcp.local
26042	1054.2614000…	192.168.6.75	224.0.0.251	MDNS	240	Standard query response 0x0000 AAAA, cache flush
26043	1054.2618636…	fe80::386b:714b:7ec…	ff02::fb	MDNS	260	Standard query response 0x0000 AAAA, cache flush
26044	1054.4977319…	192.168.6.178	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1

```
▸ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: Sophos_6b:54:cf (00:1a:8c:6b:54:cf), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 1a  8c 6b 54 cf 08 06 00 01   ........ .kT.....
0010  08 00 06 04 00 01 00 1a  8c 6b 54 cf c0 a8 06 64   ........ .kT....d
0020  00 00 00 00 00 00 c0 a8  06 3d 00 00 00 00 00 00   ........ .=......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Ready to load or capture

Packets: 26044 · Displayed: 26044 (100.0%)

Profile: Default