## NETWORKING & SYSTEM ADMINISTRATION LAB

**Name: Justin v kalappura**

**Roll No: 10**

**Batch: MCA b batch**

**Date: 23-05-2022**

## Experiment No.: 27

## Aim:

Analyzing network packet stream using tcpdump and wireshark. Perform basic network service tests using nc.

## Procedure:

### 1.How to Install tcpdump in Linux

Many Linux distributions already shipped with the tcpdump tool, if in case you don't have it on a system, you can install it using the command.

- $ sudo apt-get install tcpdump [On Debian, Ubuntu and Mint]

```
mca@S66:~$ sudo apt update && sudo apt install tcpdump
[sudo] password for mca:
Hit:1 http://in.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 https://dl.google.com/linux/chrome/deb stable InRelease
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
Hit:5 http://ppa.launchpad.net/webupd8team/java/ubuntu bionic InRelease
Get:6 https://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.6 Release [2,495 B]
Get:7 https://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.6 Release.gpg [801 B]
Err:7 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 not 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>
```

```
mca@S66:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:48:30.969742 IP 192.168.6.246.52211 > 239.255.255.250.1900: UDP, length 175
14:48:30.971138 IP S66.40918 > dns.google.domain: 60522+ [1au] PTR? 250.255.255.239.in-addr.arpa. (57)
14:48:30.985296 IP 192.168.6.246.52212 > 239.255.255.250.1900: UDP, length 174
14:48:30.988376 IP dns.google.domain > S66.40918: 60522 NXDomain 0/1/1 (114)
14:48:30.990300 IP S66.54927 > dns.google.domain: 11341+ [1au] PTR? 246.6.168.192.in-addr.arpa. (55)
14:48:31.005219 IP dns.google.domain > S66.54927: 11341 NXDomain 0/0/1 (55)
14:48:31.006636 IP S66.34150 > dns.google.domain: 42956+ [1au] PTR? 8.8.8.8.in-addr.arpa. (49)
14:48:31.021106 IP dns.google.domain > S66.34150: 42956 1/0/1 PTR dns.google. (73)
14:48:31.068544 ARP, Reply 192.168.1.1 is-at 04:09:73:99:e3:b0 (oui Unknown), length 46
14:48:31.068565 ARP, Reply 192.168.1.1 is-at 04:09:73:99:63:ac (oui Unknown), length 46
14:48:31.068638 ARP, Reply 192.168.1.1 is-at 04:09:73:fd:e4:7c (oui Unknown), length 46
14:48:31.069003 IP S66.42631 > dns.google.domain: 47416+ [1au] PTR? 1.1.168.192.in-addr.arpa. (53)
14:48:31.084563 IP dns.google.domain > S66.42631: 47416 NXDomain 0/0/1 (53)
14:48:31.245978 IP 172.17.0.2 > igmp.mcast.net: igmp v3 report, 1 group record(s)
14:48:31.246432 IP S66.36570 > dns.google.domain: 30119+ [1au] PTR? 22.0.0.224.in-addr.arpa. (52)
14:48:31.264380 IP dns.google.domain > S66.36570: 30119 1/0/1 PTR igmp.mcast.net. (80)
14:48:31.265021 IP S66.55163 > dns.google.domain: 38474+ [1au] PTR? 2.0.17.172.in-addr.arpa. (52)
14:48:31.279813 IP dns.google.domain > S66.55163: 38474 NXDomain 0/0/1 (52)
14:48:31.330747 IP 172.17.0.2.mdns > 224.0.0.251.mdns: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
14:48:31.331076 IP S66.38948 > dns.google.domain: 51777+ [1au] PTR? 251.0.0.224.in-addr.arpa. (53)
14:48:31.334792 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 78:24:af:ba:c4:90 (oui Unknown), length 300
14:48:31.373031 IP dns.google.domain > S66.38948: 51777 NXDomain 0/1/1 (110)
14:48:31.470020 ARP, Request who-has 192.168.6.92 tell 192.168.6.91, length 46
14:48:31.470572 IP S66.47475 > dns.google.domain: 59001+ [1au] PTR? 92.6.168.192.in-addr.arpa. (54)
14:48:31.487289 IP dns.google.domain > S66.47475: 59001 NXDomain 0/0/1 (54)
14:48:31.488456 IP S66.52466 > dns.google.domain: 50210+ [1au] PTR? 91.6.168.192.in-addr.arpa. (54)
14:48:31.502951 IP dns.google.domain > S66.52466: 50210 NXDomain 0/0/1 (54)
14:48:31.527632 IP 172.17.0.2.mdns > 224.0.0.251.mdns: 0 [3q] [4n] ANY (QM)? 1.6.0.3.8.1.4.9.9.a.9.4.d.d.b.c.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.i
p6.arpa. ANY (QM)? U37.local. ANY (QM)? 2.0.17.172.in-addr.arpa. (202)
14:48:31.539168 IP 192.168.6.76.63390 > 239.255.255.250.1900: UDP, length 174
14:48:31.539738 IP S66.46892 > dns.google.domain: 49578+ [1au] PTR? 76.6.168.192.in-addr.arpa. (54)
14:48:31.556973 IP dns.google.domain > S66.46892: 49578 NXDomain 0/0/1 (54)
14:48:31.608159 IP 192.168.6.76.63391 > 239.255.255.250.1900: UDP, length 175
14:48:31.652817 IP 169.254.12.69.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 44:31:92:f1:0c:46 (oui Unknown), length 334
```

### 2.Display Available Interfaces

To list the number of available interfaces on the system, run the following command with -D option.

```
mca@S66:~$ sudo tcpdump -D
1.enp3s0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.docker0 [Up]
5.nflog (Linux netfilter log (NFLOG) interface)
6.nfqueue (Linux netfilter queue (NFQUEUE) interface)
7.usbmon1 (USB bus number 1)
8.usbmon2 (USB bus number 2)
9.usbmon3 (USB bus number 3)
10.usbmon4 (USB bus number 4)
```

### 3.Capture Packets from Specific Interface

The command screen will scroll up until you interrupt and when we execute the tcpdump command it will captures from all the interfaces, however with -i switch only capture from the desired interface.

```
mca@S66:~$ sudo tcpdump -i enp3s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:50:51.049423 ARP, Request who-has 192.168.6.129 tell _gateway, length 46
14:50:51.050719 IP S66.58959 > dns.google.domain: 65361+ [1au] PTR? 129.6.168.192.in-addr.arpa. (55)
14:50:51.065706 IP dns.google.domain > S66.58959: 65361 NXDomain 0/0/1 (55)
14:50:51.067564 IP S66.57195 > dns.google.domain: 55961+ [1au] PTR? 100.6.168.192.in-addr.arpa. (55)
14:50:51.082544 IP dns.google.domain > S66.57195: 55961 NXDomain 0/0/1 (55)
14:50:51.084331 IP S66.51765 > dns.google.domain: 42819+ [1au] PTR? 66.6.168.192.in-addr.arpa. (54)
14:50:51.100902 IP dns.google.domain > S66.51765: 42819 NXDomain 0/0/1 (54)
14:50:51.172312 ARP, Request who-has 192.168.6.92 tell 192.168.6.91, length 46
14:50:51.172719 IP S66.54283 > dns.google.domain: 31086+ [1au] PTR? 92.6.168.192.in-addr.arpa. (54)
14:50:51.187599 IP dns.google.domain > S66.54283: 31086 NXDomain 0/0/1 (54)
14:50:51.188298 IP S66.46752 > dns.google.domain: 62750+ [1au] PTR? 91.6.168.192.in-addr.arpa. (54)
14:50:51.202418 IP dns.google.domain > S66.46752: 62750 NXDomain 0/0/1 (54)
14:50:51.255146 IP 192.168.6.59.49717 > 239.255.255.250.1900: UDP, length 172
14:50:51.256240 IP S66.33091 > dns.google.domain: 44586+ [1au] PTR? 59.6.168.192.in-addr.arpa. (54)
14:50:51.258319 IP 192.168.6.83.60366 > 239.255.255.250.1900: UDP, length 174
14:50:51.272796 IP dns.google.domain > S66.33091: 44586 NXDomain 0/0/1 (54)
14:50:51.273877 IP S66.39602 > dns.google.domain: 4567+ [1au] PTR? 83.6.168.192.in-addr.arpa. (54)
14:50:51.288554 IP dns.google.domain > S66.39602: 4567 NXDomain 0/0/1 (54)
14:50:51.412232 IP 192.168.6.236.52332 > 239.255.255.250.1900: UDP, length 174
14:50:51.412253 IP 192.168.6.236.52329 > 239.255.255.250.1900: UDP, length 175
14:50:51.412563 IP S66.38699 > dns.google.domain: 52710+ [1au] PTR? 236.6.168.192.in-addr.arpa. (55)
14:50:51.429559 IP dns.google.domain > S66.38699: 52710 NXDomain 0/0/1 (55)
14:50:51.496305 IP 192.168.6.236.50872 > 192.168.6.255.6866: UDP, length 395
14:50:51.496757 IP S66.54608 > dns.google.domain: 37534+ [1au] PTR? 255.6.168.192.in-addr.arpa. (55)
14:50:51.512693 IP dns.google.domain > S66.54608: 37534 NXDomain 0/0/1 (55)
14:50:51.552703 ARP, Request who-has 192.168.6.168 tell _gateway, length 46
14:50:51.553036 IP S66.42661 > dns.google.domain: 29228+ [1au] PTR? 168.6.168.192.in-addr.arpa. (55)
14:50:51.569979 IP dns.google.domain > S66.42661: 29228 NXDomain 0/0/1 (55)
```

### 4.Capture Only N Number of Packets

When you run the tcpdump command it will capture all the packets for the specified interface, until you hit the cancel button. But using `-c` option, you can capture a specified number of packets.

# tcpdump –c 5 –i enp3s0

```
mca@S66:~$ sudo tcpdump -c 4 -i enp3s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:52:06.492213 IP 192.168.6.91.netbios-ns > 192.168.6.255.netbios-ns: NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
14:52:06.492753 IP S66.45675 > dns.google.domain: 62104+ [1au] PTR? 255.6.168.192.in-addr.arpa. (55)
14:52:06.507376 IP dns.google.domain > S66.45675: 62104 NXDomain 0/0/1 (55)
14:52:06.508369 IP S66.35678 > dns.google.domain: 32209+ [1au] PTR? 91.6.168.192.in-addr.arpa. (54)
4 packets captured
7 packets received by filter
0 packets dropped by kernel
```

### 5.Display Captured Packets in HEX and ASCII

The following command with option -XX capture the data of each packet, including its link level header in HEX and ASCII format

```
mca@S66:~$ sudo tcpdump -XX -i enp3s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:53:25.604279 ARP, Request who-has 192.168.6.92 tell 192.168.6.91, length 46
        0x0000:  ffff ffff ffff 0c9d 920e 8dea 0806 0001  ..............
        0x0010:  0800 0604 0001 0c9d 920e 8dea c0a8 065b  ...............[
        0x0020:  0000 0000 0000 c0a8 065c 0000 0000 0000  .........\......
        0x0030:  0000 0000 0000 0000 0000 0000            ............
14:53:25.605431 IP S66.39677 > dns.google.domain: 37631+ [1au] PTR? 92.6.168.192.in-addr.arpa. (54)
        0x0000:  001a 8c6b 54cf 1c87 2c71 893e 0800 4500  ...kT...,q.>..E.
        0x0010:  0052 5e7c 4000 4011 0525 c0a8 0642 0808  .R^|@.@..%...B..
        0x0020:  0808 9afd 0035 003e 7457 92ff 0100 0001  .....5.>tW......
        0x0030:  0000 0000 0001 0239 3201 3603 3136 3803  .......92.6.168.
        0x0040:  3139 3207 696e 2d61 6464 7204 6172 7061  192.in-addr.arpa
        0x0050:  0000 0c00 0100 0029 0200 0000 0000 0000  .......)........
14:53:25.620006 IP dns.google.domain > S66.39677: 37631 NXDomain 0/0/1 (54)
        0x0000:  1c87 2c71 893e 001a 8c6b 54cf 0800 4500  ..,q.>...kT...E.
        0x0010:  0052 2a86 0000 3c11 7d1b 0808 0808 c0a8  .R*...<.}.......
        0x0020:  0642 0035 9afd 003e f3d3 92ff 8183 0001  .B.5...>........
        0x0030:  0000 0000 0001 0239 3201 3603 3136 3803  .......92.6.168.
        0x0040:  3139 3207 696e 2d61 6464 7204 6172 7061  192.in-addr.arpa
        0x0050:  0000 0c00 0100 0029 0200 0000 0000 0000  .......)........
14:53:25.621529 IP S66.34818 > dns.google.domain: 37952+ [1au] PTR? 91.6.168.192.in-addr.arpa. (54)
        0x0000:  001a 8c6b 54cf 1c87 2c71 893e 0800 4500  ...kT...,q.>..E.
        0x0010:  0052 5e7e 4000 4011 0523 c0a8 0642 0808  .R^~@.@..#...B..
        0x0020:  0808 8802 0035 003e 8711 9440 0100 0001  .....5.>...@....
        0x0030:  0000 0000 0001 0239 3101 3603 3136 3803  .......91.6.168.
        0x0040:  3139 3207 696e 2d61 6464 7204 6172 7061  192.in-addr.arpa
        0x0050:  0000 0c00 0100 0029 0200 0000 0000 0000  .......)........
14:53:25.638802 IP dns.google.domain > S66.34818: 37952 NXDomain 0/0/1 (54)
        0x0000:  1c87 2c71 893e 001a 8c6b 54cf 0800 4500  ..,q.>...kT...E.
        0x0010:  0052 18dc 0000 3c11 8ec5 0808 0808 c0a8  .R....<.........
        0x0020:  0642 0035 8802 003e 068e 9440 8183 0001  .B.5...>...@....
        0x0030:  0000 0000 0001 0239 3101 3603 3136 3803  .......91.6.168.
```

## 6.Capture and Save Packets in a File

As we said, that tcpdump has a feature to capture and save the file in a .pcap format, to do this just execute the command with -w option.

```
mca@S66:~$ sudo tcpdump -i enp3s0 -c 10 -w icmp.pcap
tcpdump: listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
10 packets captured
12 packets received by filter
0 packets dropped by kernel
```

## 7.Capture Packet from Specific Port

Let's say you want to capture packets for specific port 80, execute the below command by specifying port number 80 as shown below.

```
mca@S66:~$ sudo tcpdump -i enp3s0 -c 5 port 80
[sudo] password for mca:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:18:09.213493 IP S66.59252 > 32.121.122.34.bc.googleusercontent.com.http: Flags [S], seq 18809714, win 29200, options [mss 1460,sackOK,TS va
l 1175571752 ecr 0,nop,wscale 7], length 0
14:18:10.244247 IP S66.59252 > 32.121.122.34.bc.googleusercontent.com.http: Flags [S], seq 18809714, win 29200, options [mss 1460,sackOK,TS va
l 1175572783 ecr 0,nop,wscale 7], length 0
14:18:10.489618 IP 32.121.122.34.bc.googleusercontent.com.http > S66.59252: Flags [S.], seq 131097005, ack 18809715, win 64768, options [mss 1
420,sackOK,TS val 3319464738 ecr 1175572783,nop,wscale 7], length 0
14:18:10.489703 IP S66.59252 > 32.121.122.34.bc.googleusercontent.com.http: Flags [.], ack 1, win 229, options [nop,nop,TS val 1175573028 ecr
3319464738], length 0
14:18:10.489864 IP S66.59252 > 32.121.122.34.bc.googleusercontent.com.http: Flags [P.], seq 1:88, ack 1, win 229, options [nop,nop,TS val 1175
573028 ecr 3319464738], length 87: HTTP: GET / HTTP/1.1
5 packets captured
5 packets received by filter
0 packets dropped by kernel
```

## 8.Read Captured Packets File

To read and analyze captured packet 0001.pcap file use the command with -r option.

```
mca@S66:~$ sudo tcpdump -r icmp.pcap
reading from file icmp.pcap, link-type EN10MB (Ethernet)
14:19:22.189957 ARP, Reply 192.168.1.1 is-at 04:09:73:99:63:ac (oui Unknown), length 46
14:19:22.190160 ARP, Reply 192.168.1.1 is-at 04:09:73:fd:e4:7c (oui Unknown), length 46
14:19:22.195693 ARP, Reply 192.168.1.1 is-at 04:09:73:99:e3:b0 (oui Unknown), length 46
14:19:22.216587 IP 192.168.6.204.32925 > 239.255.255.250.1900: UDP, length 172
14:19:22.586506 ARP, Request who-has 192.168.6.185 tell _gateway, length 46
14:19:22.595038 STP 802.1w, Rapid STP, Flags [Forward], bridge-id 8000.44:31:92:f1:0c:45.8012, length 47
14:19:23.157167 ARP, Reply 192.168.1.1 is-at 04:09:73:fd:e4:7c (oui Unknown), length 46
14:19:23.157170 ARP, Reply 192.168.1.1 is-at 04:09:73:99:e3:b0 (oui Unknown), length 46
14:19:23.157196 ARP, Reply 192.168.1.1 is-at 04:09:73:99:63:ac (oui Unknown), length 46
14:19:23.169605 IP 192.168.6.236.57786 > 192.168.6.255.6866: UDP, length 395
```

## Wire shark:

Installing Wireshark on Ubuntu 20.04

The Wireshark utility is available on all major desktop platforms, i.e., Linux, Microsoft Windows, FreeBSD, MacOS, Solaris, and many more. Follow the steps below to install Wireshark on Ubuntu 20.04.

**STEP1** : Update APT

First, as always, update and upgrade your APT through the following command.

**Syntax:** **$ sudo apt update**

```
mca@S66:~$ 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]
Ign:3 https://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.6 InRelease
Err:4 http://ppa.launchpad.net/jonathonf/python-3.6/ubuntu bionic InRelease
  403  Forbidden [IP: 185.125.190.52 80]
Get:5 https://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1,097 B]
Hit:6 http://ppa.launchpad.net/webupd8team/java/ubuntu bionic InRelease
Get:7 https://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.6 Release [2,495 B]
Get:8 https://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.6 Release.gpg [801 B]
Err:8 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 not 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:** Download and Install Wireshark

Now that Wireshark's latest version has been added to the APT, you can download and install it with the following command.

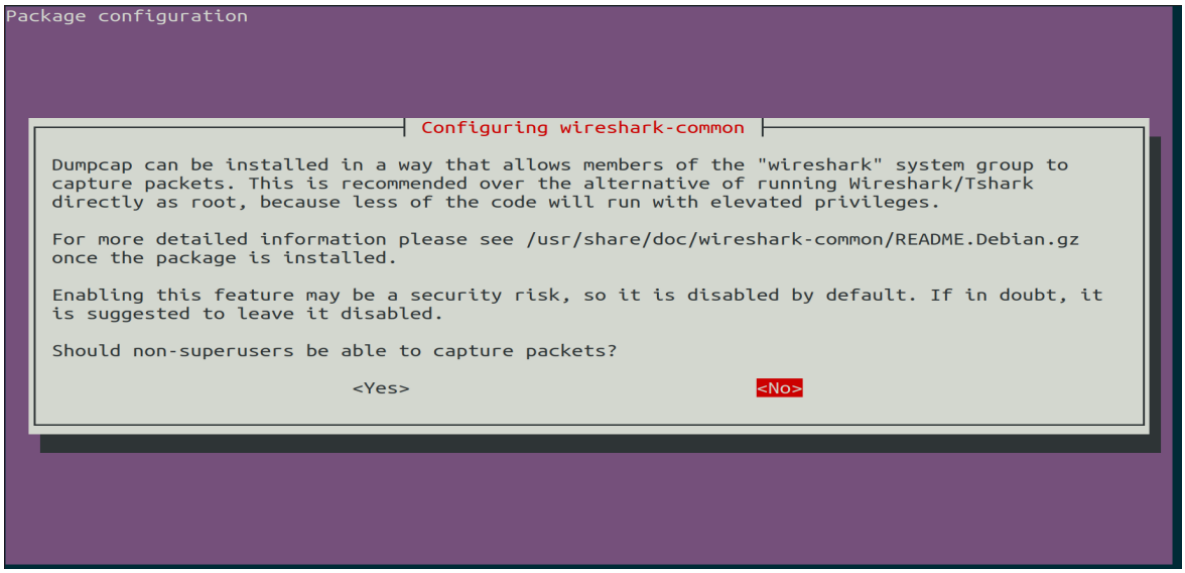
**Syntax:** **$ sudo apt install wireshark**

```
mca@S66:~$ sudo apt install wireshark
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  geoip-database-extra javascript-common libc-ares2 libjs-openlayers libnl-route-3-200 libqt5multimedia5 libsmi2ldbl libsnappy1v5
  libspandsp2 libssh-gcrypt-4 libwireshark-data 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 javascript-common libc-ares2 libjs-openlayers libnl-route-3-200 libqt5multimedia5 libsmi2ldbl libsnappy1v5
  libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark10 libwiretap7 libwscodecs1 libwsutil8 wireshark wireshark-common wireshark-qt
0 upgraded, 18 newly installed, 0 to remove and 1 not upgraded.
2 not fully installed or removed.
Need to get 31.3 MB of archives.
After this operation, 139 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]
0% [1 geoip-database-extra 14.2 kB/11.1 MB 0%]


Get:2 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 javascript-common all 11 [6,066 B]
Get:3 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 libnl-route-3-200 amd64 3.2.29-0ubuntu3 [146 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libqt5multimedia5 amd64 5.9.5-0ubuntu1 [293 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 libsmi2ldbl amd64 0.4.8+dfsg2-15 [100 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libspandsp2 amd64 0.0.6+dfsg-0.1 [273 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 libssh-gcrypt-4 amd64 0.8.0~20170825.94fa1e38-1build1 [171 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libwireshark-data all 2.4.5-1 [958 kB]
Get:9 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 libc-ares2 amd64 1.14.0-1 [37.1 kB]
Get:10 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 libsnappy1v5 amd64 1.1.7-1 [16.0 kB]
Get:11 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libwsutil8 amd64 2.4.5-1 [50.2 kB]
Get:12 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libwiretap7 amd64 2.4.5-1 [172 kB]
Get:13 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libwscodecs1 amd64 2.4.5-1 [16.6 kB]
Get:14 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libwireshark10 amd64 2.4.5-1 [13.5 MB]
Get:15 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 wireshark-common amd64 2.4.5-1 [369 kB]
Get:16 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 wireshark-qt amd64 2.4.5-1 [3,357 kB]
Get:17 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 wireshark amd64 2.4.5-1 [4,484 B]
```

**Step 3:** Enable Root Privileges

When Wireshark installs on your system, you will be prompted by the following window. As Wireshark requires superuser/root privileges to operate, this option asks to enable or disable permissions for all every user on the system. Press the “Yes” button to allow other users, or press the “No” button to restrict other users from using Wireshark.




**Step 4:**

You must add a username to the Wireshark group so that this user can use Wireshark. To do this, execute the following command, adding your required username after “wireshark” in the command.

**Syntax:** **$ sudo adduser $user wireshark**

```
mca@S66:~$ sudo adduser $mca wireshark
adduser: The group `wireshark' already exists.
```

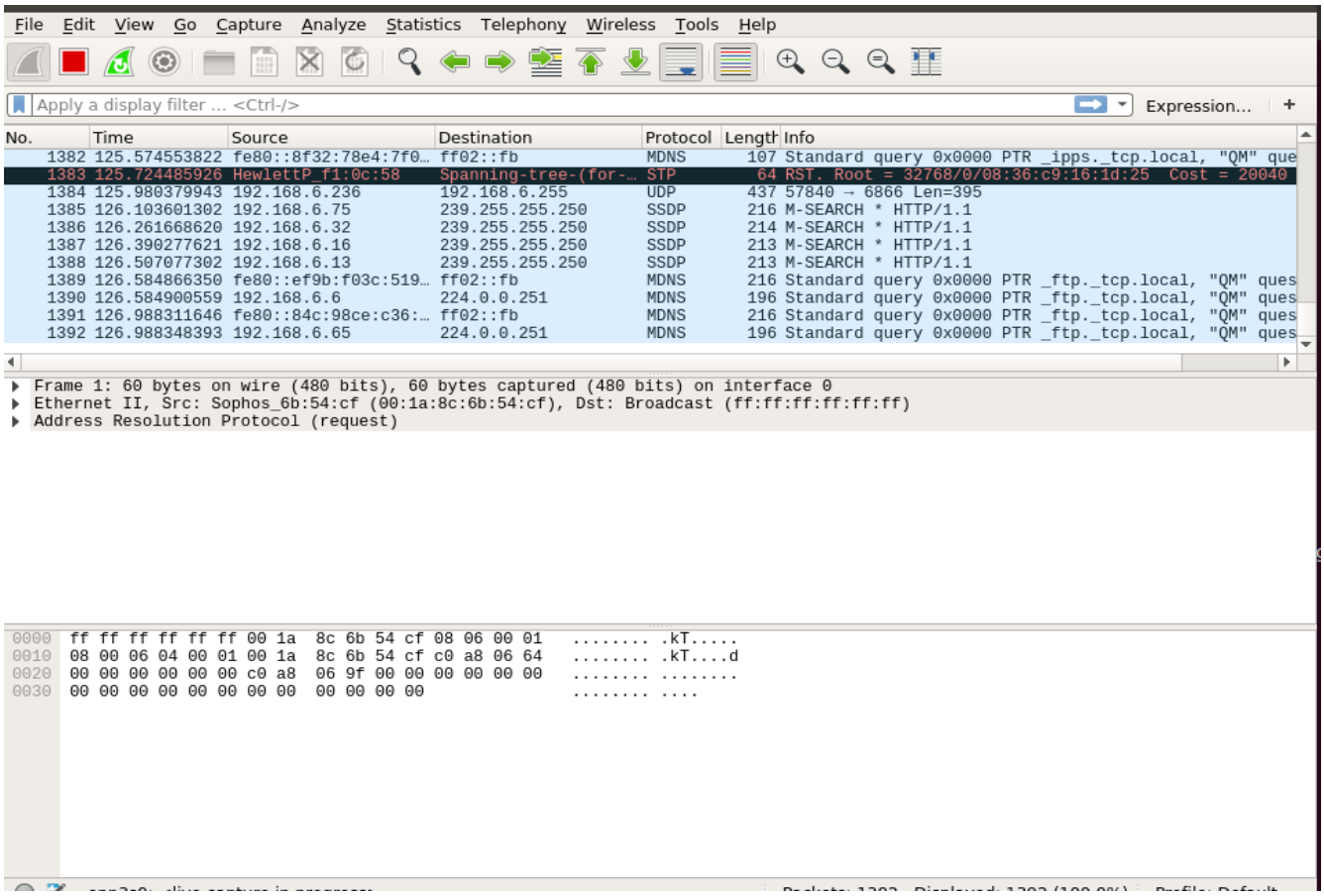
**Step 5:** Launch Wireshark

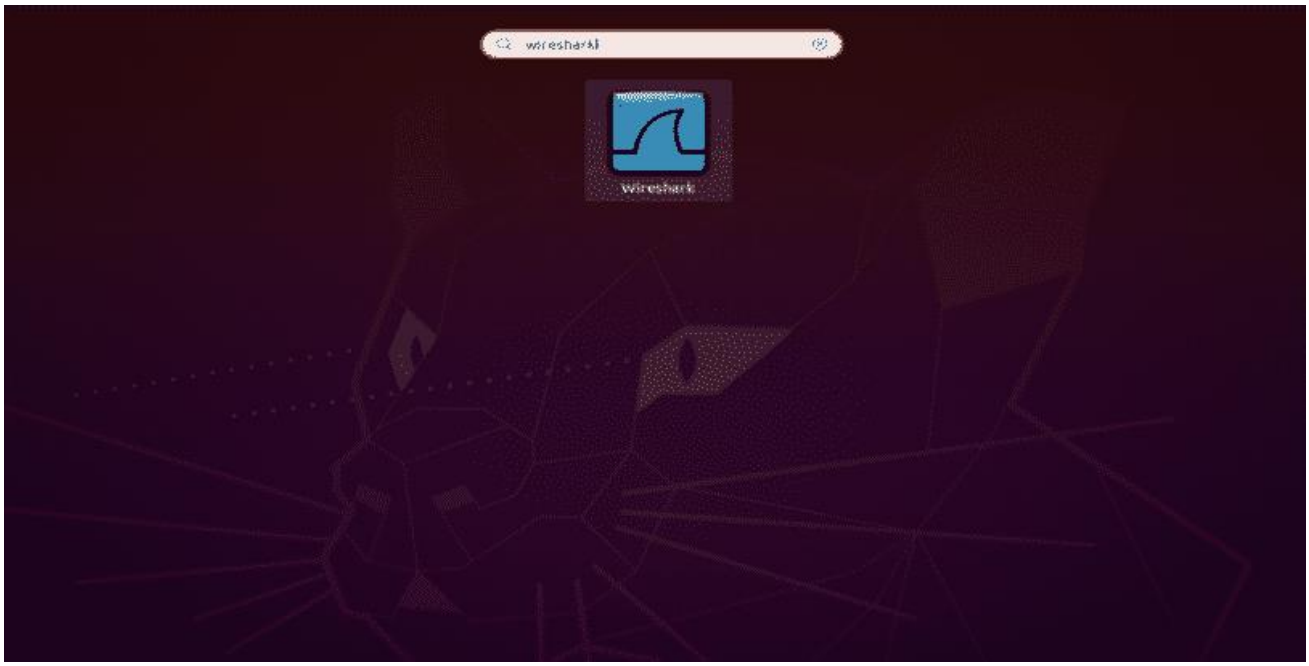
In the terminal window, type the following command to start the Wireshark application.

**Syntax:** **$ sudo wireshark**

You can also open Wireshark through the Graphical User Interface (GUI) by opening the activities on the Ubuntu desktop, and in the search bar, type "Wireshark," and click on the application result.

```
mca@S66:~$ sudo wireshark
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```






**STEP1:** Update APT

First, as always, update and upgrade your APT through the following command.

**Syntax:** **$ sudo apt update**

```
mca@U23:~$ sudo apt-get update
[sudo] password for mca:
Hit:1 http://ppa.launchpad.net/codeblocks-devs/release/ubuntu bionic InRelease
Get:2 https://dl.google.com/linux/chrome/deb stable InRelease [1,811 B]
Hit:3 http://archive.ubuntu.com/ubuntu bionic InRelease
Err:4 http://ppa.launchpad.net/jonathonf/python-3.6/ubuntu bionic InRelease
  403  Forbidden [IP: 185.125.190.52 80]
Get:5 https://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1,097 B]
Hit:6 http://ppa.launchpad.net/pasgui/ppa/ubuntu bionic InRelease
Hit:7 http://ppa.launchpad.net/webupd8team/java/ubuntu bionic InRelease
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.
```

**Step 2:** Install netcat

```
mca@U23:~$ sudo apt-get install netcat
Reading package lists... Done
Building dependency tree
Reading state information... Done
netcat is already the newest version (1.10-41.1).
The following packages were automatically installed and are no longer required:
  debhelper dh-autoreconf dh-strip-nondeterminism libarchive-cpio-perl
  libfile-stripnondeterminism-perl libmail-sendmail-perl libpcre16-3
  libpcre3-dev libpcre32-3 libpcrecpp0v5 libssl-dev libssl-doc
  libsys-hostname-long-perl po-debconf shtool
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 6 not upgraded.
```

## Working with netcat security tool:

To start listening on a port, first open 2 window terminals

Terminal 1 for listening…….

```
mca@U23:~$ nc -l -p 1234
Hi buddy how are
nice to meet u
```

Terminal 2 sending requesting……

```
mca@U23:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:60:8b:1f:bd  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp5s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.6.193  netmask 255.255.255.0  broadcast 192.168.6.255
        inet6 fe80::a0fd:1fa9:856d:5ce1  prefixlen 64  scopeid 0x20<link>
        ether 0c:9d:92:0e:92:12  txqueuelen 1000  (Ethernet)
        RX packets 142103  bytes 176542175 (176.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 36029  bytes 13803699 (13.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 620  bytes 48633 (48.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 620  bytes 48633 (48.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
mca@U23:~$ nc 192.168.6.193 1234
Hi buddy how are
nice to meet u
```