Q. Execute tcpdump and its options on your own system, and submit the output screenshot as a document.

Install tcpdump sudo apt update && sudo apt

install tcpdump

```
sujith@LAPTOP-4DJBAO1Q:~$ sudo apt update && sudo apt install tcpdump
Get:1 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Hit:2 http://archive.ubuntu.com/ubuntu focal InRelease
Get:3 http://archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:4 http://archive.ubuntu.com/ubuntu focal-backports InRelease [101 kB]
Fetched 328 kB in 4s (86.0 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
55 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree
Reading state information... Done
tcpdump is already the newest version (4.9.3-4).
0 upgraded, 0 newly installed, 0 to remove and 55 not upgraded.
```

Execute tcpdump

```
sujith@LAPTOP-4DJBAO1Q:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:34:40.105302 IP LAPTOP-4DJBAO1Q.mshome.net.netbios-ns > 172.18.175.255.netbios-ns: UDP, length 50
12:34:40.105747 IP 172.18.169.231.38546 > LAPTOP-4DJBAO1Q.mshome.net.domain: 63073+ PTR? 255.175.18.172.in-addr.arpa. (45)
12:34:40.106889 IP LAPTOP-4DJBAO1Q.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 255.175.18.172.in-addr.arpa.local. (51)
12:34:40.107261 IP6 LAPTOP-4DJBAO1Q.mdns > ff02::fb.mdns: 0 PTR (QM)? 255.175.18.172.in-addr.arpa.local. (51)
12:34:40.855488 IP LAPTOP-4DJBAO1Q.mshome.net.netbios-ns > 172.18.175.255.netbios-ns: UDP, length 50
12:34:40.891418 IP LAPTOP-4DJBAO1Q.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 255.175.18.172.in-addr.arpa.local. (51)
12:34:40.892118 IP6 LAPTOP-4DJBAO1Q.mdns > ff02::fb.mdns: 0 PTR (QM)? 255.175.18.172.in-addr.arpa.local. (51)
12:34:41.105938 IP LAPTOP-4DJBAO1Q.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 255.175.18.172.in-addr.arpa.local. (51)
12:34:41.106744 IP6 LAPTOP-4DJBAO1Q.mdns > ff02::fb.mdns: 0 PTR (QM)? 255.175.18.172.in-addr.arpa.local. (51)
12:34:41.606775 IP LAPTOP-4DJBAO1Q.mshome.net.netbios-ns > 172.18.175.255.netbios-ns: UDP, length 50
12:34:41.888354 IP LAPTOP-4DJBAO1Q.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 255.175.18.172.in-addr.arpa.local. (51)
12:34:41.888970 IP6 LAPTOP-4DJBAO1Q.mdns > ff02::fb.mdns: 0 PTR (QM)? 255.175.18.172.in-addr.arpa.local. (51)
12:34:41.895623 IP LAPTOP-4DJBAO1Q.mshome.net.domain > 172.18.169.231.38546: 63073 NXDomain 0/0/0 (45)
12:34:41.896082 IP 172.18.169.231.35000 > LAPTOP-4DJBAO1Q.mshome.net.domain: 23834+ PTR? 1.160.18.172.in-addr.arpa. (43)
12:34:41.897378 IP LAPTOP-4DJBAO1Q.mshome.net.domain > 172.18.169.231.35000: 23834- 1/0/0 PTR LAPTOP-4DJBAO1Q.mshome.net. (108)
12:34:41.898038 IP 172.18.169.231.44789 > LAPTOP-4DJBAO1Q.mshome.net.domain: 44649+ PTR? 231.169.18.172.in-addr.arpa. (45)
12:34:41.899948 IP LAPTOP-4DJBAO1Q.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 231.169.18.172.in-addr.arpa.local. (51)
12:34:41.900487 IP6 LAPTOP-4DJBAO1Q.mdns > ff02::fb.mdns: 0 PTR (QM)? 231.169.18.172.in-addr.arpa.local. (51)
12:34:42.176257 IP LAPTOP-4DJBAO1Q.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 231.169.18.172.in-addr.arpa.local. (51)
12:34:42.176909 IP6 LAPTOP-4DJBAO1Q.mdns > ff02::fb.mdns: 0 PTR (QM)? 231.169.18.172.in-addr.arpa.local. (51)
12:34:42.890184 IP LAPTOP-4DJBAO1Q.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 231.169.18.172.in-addr.arpa.local. (51)
12:34:42.891068 IP6 LAPTOP-4DJBAO1Q.mdns > ff02::fb.mdns: 0 PTR (QM)? 231.169.18.172.in-addr.arpa.local. (51)
12:34:43.172228 IP LAPTOP-4DJBAO1Q.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 231.169.18.172.in-addr.arpa.local. (51)
12:34:43.172857 IP6 LAPTOP-4DJBAO1Q.mdns > ff02::fb.mdns: 0 PTR (QM)? 231.169.18.172.in-addr.arpa.local. (51)
12:34:43.176838 IP LAPTOP-4DJBAO1Q.mshome.net.domain > 172.18.169.231.44789: 44649 NXDomain 0/0/0 (45)
12:34:43.177237 IP 172.18.169.231.34382 > LAPTOP-4DJBAO1Q.mshome.net.domain: 21190+ PTR? 251.0.0.224.in-addr.arpa. (42)
12:34:43.179187 IP LAPTOP-4DJBAO1Q.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 251.0.0.224.in-addr.arpa.local. (48)
12:34:43.179732 IP6 LAPTOP-4DJBAO1Q.mdns > ff02::fb.mdns: 0 PTR (QM)? 251.0.0.224.in-addr.arpa.local. (48)
12:34:43.245402 IP LAPTOP-4DJBAO1Q.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 251.0.0.224.in-addr.arpa.local. (48)
12:34:43.245993 IP6 LAPTOP-4DJBAO1Q.mdns > ff02::fb.mdns: 0 PTR (QM)? 251.0.0.224.in-addr.arpa.local. (48)
12:34:44.189575 IP LAPTOP-4DJBAO1Q.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 251.0.0.224.in-addr.arpa.local. (48)
12:34:44.190351 IP6 LAPTOP-4DJBAO1Q.mdns > ff02::fb.mdns: 0 PTR (QM)? 251.0.0.224.in-addr.arpa.local. (48)
12:34:44.251943 IP LAPTOP-4DJBAO1Q.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 251.0.0.224.in-addr.arpa.local. (48)
12:34:44.252691 IP6 LAPTOP-4DJBAO1Q.mdns > ff02::fb.mdns: 0 PTR (QM)? 251.0.0.224.in-addr.arpa.local. (48)
```

tcpdump –D

```
sujith@LAPTOP-4DJBAO1Q:~$ tcpdump -D
1.eth0 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7.dummy0 [none]
8.tunl0 [none]
9.sit0 [none]
10.bond0 [none]
```

```
sujith@LAPTOP-4DJBAO1Q:~$ sudo tcpdump -i enp2s0
tcpdump: enp2s0: No such device exists
(SIOCGIFHWADDR: No such device)
sujith@LAPTOP-4DJBAO1Q:~$
```

Sudo tcpdump -c 5

```
sujith@LAPTOP-4DJBAO1Q:~$ sudo tcpdump -c 5
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:39:29.377292 IP LAPTOP-4DJBAO1Q.mshome.net.49545 > 239.255.255.250.1900: UDP, length 173
12:39:29.377768 IP 172.18.109.231.42220 > LAPTOP-4DJBAO1Q.mshome.net.domain: 9149+ PTR? 250.255.255.239.in-addr.arpa. (46)
12:39:29.379026 IP LAPTOP-4DJBAO1Q.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa.local. (52)
12:39:29.379293 IP6 LAPTOP-4DJBAO1Q.mdns > ff02::fb.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa.local. (52)
12:39:29.895810 IP LAPTOP-4DJBAO1Q.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa.local. (52)
5 packets captured
96 packets received by filter
61 packets dropped by kernel
```