PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)

Academic Year: 2025-26
Semester: V
Class / Branch: TE IT-C
Subject: Security Lab
Name of Instructor: Prof. Vishal Badgujar

Name of Student: Suyash Y Mane
Student ID: 24204008
Date of Performance: 13/08/2025
Date of Submission: 13/08/2025

Experiment No. 4

Aim: To study analysis of network packets by sing open source sniffing tools like tcpdump and Wireshark in promiscuous and non-promiscuous mode.

Screenshots:

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ tcpdump -D
1.enp1s0 [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)
```

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo tcpdump -i enp1s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp1s0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:51:02.737309 IP 192.168.104.10.43478 > 239.255.255.250.1900: UDP, length 167
10:51:02.740909 IP apsit-HP-280-Pro-G6-Microtower-PC.45834 > _gateway.domain: 8316+ PTR? 250.255.255.239.in-addr.arpa. (46)
10:51:02.742556 ARP, Request who-has 192.168.7.89 tell 192.168.5.22, length 46
10:51:02.743005 ARP, Request who-has 192.168.3.120 tell 192.168.5.22, length 46
10:51:02.744478 IP _gateway.domain > apsit-HP-280-Pro-G6-Microtower-PC.45834: 8316 NXDomain* 0/0/0 (46)
10:51:02.746108 IP apsit-HP-280-Pro-G6-Microtower-PC.55775 > _gateway.domain: 18370+ PTR? 10.104.168.192.in-addr.arpa. (45)
10:51:02.748141 ARP, Request who-has 192.168.110.8 tell 192.168.4.137, length 46
10:51:05.756961 IP apsit-HP-280-Pro-G6-Microtower-PC.58422 > _gateway.domain: 22569+ PTR? 193.192.168.192.in-addr.arpa. (46)
10:51:11.776000 IP apsit-HP-280-Pro-G6-Microtower-PC.36393 > _gateway.domain: 6235+ PTR? 89.7.168.192.in-addr.arpa. (43)
10:51:17.797985 ARP, Request who-has 192.168.3.120 tell 192.168.3.241, length 46
10:51:20.818221 IP apsit-HP-280-Pro-G6-Microtower-PC.47039 > _gateway.domain: 26017+ PTR? 8.110.168.192.in-addr.arpa. (44)
10:51:20.826371 ARP, Request who-has 192.168.100.247 tell 192.168.3.118, length 46
10:51:20.826374 ARP, Request who-has 192.168.100.248 tell 192.168.3.118, length 46
10:51:26.843485 IP6 fe80::677e:e066:e1c0:ea38.53263 > ff02::c.3702: UDP, length 656
10:51:26.843933 IP apsit-HP-280-Pro-G6-Microtower-PC.35942 > _gateway.domain: 24879+ PTR? 241.3.168.192.in-addr.arpa. (44)
10:51:26.852160 ARP, Request who-has 192.168.9.75 tell 192.168.10.37, length 46
10:51:29.867619 IP apsit-HP-280-Pro-G6-Microtower-PC.45320 > _gateway.domain: 13145+ PTR? 247.100.168.192.in-addr.arpa. (46)
10:51:29.880116 IP6 fe80::b4db:6829:6226:7bdf.53688 > ff02::c.3702: UDP, length 656
10:51:35.894404 IP apsit-HP-280-Pro-G6-Microtower-PC.35933 > _gateway.domain: 51865+ PTR? 248.100.168.192.in-addr.arpa. (46)
10:51:38.912958 IP apsit-HP-280-Pro-G6-Microtower-PC.55722 > _gateway.domain: 30850+ PTR? c.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.
0.0.2.0.f.f.ip6.arpa. (90)
10:51:44.949144 IP apsit-HP-280-Pro-G6-Microtower-PC.54407 > _gateway.domain: 25531+ PTR? 75.9.168.192.in-addr.arpa. (43)
10:51:44.952243 ARP, Request who-has 192.168.79.2 tell 192.168.4.180, length 46
10:51:50.996199 IP apsit-HP-280-Pro-G6-Microtower-PC.43755 > _gateway.domain: 41752+ PTR? f.d.b.7.6.2.2.6.9.2.8.6.b.d.4.b.0.0.0.0.0.0.0.0.0.0.
0.0.0.8.e.f.ip6.arpa. (90)
10:51:50.997221 ARP, Request who-has 192.168.4.194 tell 192.168.4.76, length 46
10:51:54.010289 IP apsit-HP-280-Pro-G6-Microtower-PC.57050 > _gateway.domain: 14031+ PTR? 2.79.168.192.in-addr.arpa. (43)
^C10:51:54.015005 IP 192.168.4.199.54915 > 192.168.255.255.54915: UDP, length 263

26 packets captured
27308 packets received by filter
27276 packets dropped by kernel
```

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo tcpdump -i any
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
10:53:22.500761 ARP, Request who-has 192.168.3.115 tell 192.168.3.187, length 46
10:53:22.501711 IP localhost.42023 > localhost.domain: 57649+ [1au] PTR? 115.3.168.192.in-addr.arpa. (55)
10:53:22.502229 IP apsit-HP-280-Pro-G6-Microtower-PC.43643 > _gateway.domain: 36489+ PTR? 115.3.168.192.in-addr.arpa. (44)
10:53:22.513309 IP 192.168.69.197 > mdns.mcast.net: igmp v2 report mdns.mcast.net
10:53:22.519200 ARP, Request who-has 192.168.15.186 tell 192.168.4.148, length 46
10:53:22.526999 ARP, Request who-has 192.168.100.236 tell 192.168.3.94, length 46
10:53:28.527118 IP localhost.60086 > localhost.domain: 20656+ [1au] PTR? 53.0.0.127.in-addr.arpa. (52)
10:53:52.673782 ARP, Request who-has 192.168.110.8 tell 192.168.4.160, length 46
10:53:52.674057 IP localhost.34620 > localhost.domain: 31654+ [1au] PTR? 8.110.168.192.in-addr.arpa. (55)
10:53:52.674453 IP apsit-HP-280-Pro-G6-Microtower-PC.45208 > _gateway.domain: 20024+ PTR? 8.110.168.192.in-addr.arpa. (44)
10:53:52.676546 IP 192.168.8.120.mdns > mdns.mcast.net.mdns: 0*- [0q] 1/0/4 (Cache flush) SRV Android-4.local.:8009 0 0 (166)
10:53:52.676859 IP6 fe80::c18c:853b:dbcf:4407.mdns > ff02::fb.mdns: 0*- [0q] 1/0/4 (Cache flush) SRV Android-4.local.:8009 0 0 (166)
10:53:52.686180 IP 192.168.2.219.mdns > mdns.mcast.net.mdns: 0 SRV (QM)? BytelloShare1146._googlecast._tcp.local. (57)
10:53:58.711938 IP localhost.59504 > localhost.domain: 54513+ [1au] PTR? 120.8.168.192.in-addr.arpa. (55)
10:53:58.712274 IP apsit-HP-280-Pro-G6-Microtower-PC.50924 > _gateway.domain: 1088+ PTR? 120.8.168.192.in-addr.arpa. (44)
10:53:58.714015 IP 192.168.3.184.mdns > mdns.mcast.net.mdns: 0*- [0q] 1/0/4 (Cache flush) SRV Android-90.local.:8009 0 0 (167)
10:54:07.770939 IP localhost.49859 > localhost.domain: 4161+ [1au] PTR? 184.3.168.192.in-addr.arpa. (55)
10:54:07.771273 IP apsit-HP-280-Pro-G6-Microtower-PC.40649 > _gateway.domain: 30603+ PTR? 184.3.168.192.in-addr.arpa. (44)
^C10:54:07.774403 IP 192.168.91.11.mdns > mdns.mcast.net.mdns: 0 [4a] [4q] SRV (QM)? HP LaserJet Tank 1020w (F4D819)._ipps._tcp.local. AAAA (Q
M)? NPIF4D819.local. A (QM)? NPIF4D819.local. TXT (QM)? HP LaserJet Tank 1020w (F4D819)._ipps._tcp.local. (718)

19 packets captured
13750 packets received by filter
13714 packets dropped by kernel
```

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo tcpdump -i enp1s0 -c5
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp1s0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:02:01.466936 ARP, Request who-has 192.168.7.98 tell 192.168.3.126, length 46
11:02:01.468269 ARP, Request who-has 192.168.7.120 tell 192.168.5.122, length 46
11:02:01.468295 IP apsit-HP-280-Pro-G6-Microtower-PC.51013 > _gateway.domain: 62139+ PTR? 98.7.168.192.in-addr.arpa. (43)
11:02:01.468988 ARP, Request who-has 192.168.7.121 tell 192.168.5.122, length 46
11:02:01.475242 ARP, Request who-has 192.168.80.16 tell 192.168.3.230, length 46
5 packets captured
8429 packets received by filter
8418 packets dropped by kernel
```

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo tcpdump -i enp1s0 tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp1s0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:03:37.828438 IP apsit-HP-280-Pro-G6-Microtower-PC.43364 > _gateway.8090: Flags [F.], seq 4145486300, ack 3842155602, win 501, length 0
11:03:43.545751 IP 11.206.47.34.bc.googleusercontent.com.5223 > 192.168.5.107.58935: Flags [.], ack 2845892326, win 494, options [nop,nop,TS v
al 2265231004 ecr 1436493573], length 0
11:03:47.026815 IP 129.227.192.35.http-alt > 192.168.6.245.40738: Flags [F.], seq 247703502, ack 284710934, win 33, length 0
11:03:51.140701 IP apsit-HP-280-Pro-G6-Microtower-PC.43364 > _gateway.8090: Flags [F.], seq 0, ack 1, win 501, length 0
11:04:13.756496 IP 11.206.47.34.bc.googleusercontent.com.5223 > 192.168.5.107.58935: Flags [R.], seq 1, ack 1, win 494, options [nop,nop,TS va
l 2265261213 ecr 1436493573], length 0
11:04:19.300730 IP apsit-HP-280-Pro-G6-Microtower-PC.43304 > sl-in-f188.1e100.net.5228: Flags [.], ack 2763095602, win 501, options [nop,nop,T
S val 213616246 ecr 2884211588], length 0
11:04:19.300753 IP apsit-HP-280-Pro-G6-Microtower-PC.43364 > _gateway.8090: Flags [F.], seq 0, ack 1, win 501, length 0
11:04:19.300756 IP apsit-HP-280-Pro-G6-Microtower-PC.43302 > sl-in-f188.1e100.net.5228: Flags [.], ack 354421413, win 501, options [nop,nop,TS
 val 213616246 ecr 3302764561], length 0
11:04:19.361197 IP sl-in-f188.1e100.net.5228 > apsit-HP-280-Pro-G6-Microtower-PC.43304: Flags [.], ack 1, win 1043, options [nop,nop,TS val 28
84258635 ecr 213207462], length 0
11:04:19.361199 IP sl-in-f188.1e100.net.5228 > apsit-HP-280-Pro-G6-Microtower-PC.43302: Flags [.], ack 1, win 1044, options [nop,nop,TS val 33
02811608 ecr 213207305], length 0
11:04:24.848803 IP _gateway.8090 > apsit-HP-280-Pro-G6-Microtower-PC.53182: Flags [F.], seq 2573759027, ack 3786873375, win 237, length 0
11:04:24.892491 IP apsit-HP-280-Pro-G6-Microtower-PC.53182 > _gateway.8090: Flags [.], ack 1, win 501, length 0
11:04:26.892676 IP pnbomb-az-in-f14.1e100.net.https > 192.168.3.241.59108: Flags [P.], seq 1543060196:1543060269, ack 1761447985, win 332, len
gth 73
11:04:28.940673 IP dns.google.https > 192.168.3.241.58850: Flags [P.], seq 2770933859:2770933932, ack 3106369251, win 1502, length 73
^C
14 packets captured
14 packets received by filter
0 packets dropped by kernel
1 packet dropped by interface
```

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo tcpdump -i enp1s0 src 192.168.86.29
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp1s0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:08:01.873842 IP apsit-HP-280-Pro-G6-Microtower-PC.netbios-dgm > 192.168.255.255.netbios-dgm: UDP, length 216
11:08:01.875211 IP apsit-HP-280-Pro-G6-Microtower-PC.34940 > _gateway.domain: 40812+ PTR? 255.255.168.192.in-addr.arpa. (46)
11:08:02.651689 IP apsit-HP-280-Pro-G6-Microtower-PC.34940 > _gateway.domain: 40812+ PTR? 255.255.168.192.in-addr.arpa. (46)
11:08:03.876719 IP apsit-HP-280-Pro-G6-Microtower-PC.netbios-dgm > 192.168.255.255.netbios-dgm: UDP, length 216
11:08:04.401840 IP apsit-HP-280-Pro-G6-Microtower-PC.34940 > _gateway.domain: 40812+ PTR? 255.255.168.192.in-addr.arpa. (46)
11:08:04.620498 IP apsit-HP-280-Pro-G6-Microtower-PC.43304 > sl-in-f188.1e100.net.5228: Flags [.], ack 2763095602, win 501, options [nop,nop,T
S val 213841566 ecr 2884438888], length 0
11:08:04.620508 IP apsit-HP-280-Pro-G6-Microtower-PC.43302 > sl-in-f188.1e100.net.5228: Flags [.], ack 354421413, win 501, options [nop,nop,TS
 val 213841566 ecr 3302991862], length 0
11:08:07.904585 IP apsit-HP-280-Pro-G6-Microtower-PC.52803 > _gateway.domain: 26584+ PTR? 193.192.168.192.in-addr.arpa. (46)
11:08:10.924003 IP apsit-HP-280-Pro-G6-Microtower-PC.55058 > _gateway.domain: 18373+ PTR? 188.118.253.172.in-addr.arpa. (46)
11:08:14.567038 IP apsit-HP-280-Pro-G6-Microtower-PC.mdns > mdns.mcast.net.mdns: 0 [1a] [2q] SRV (QM)? Canon iR2224 (fe:bd:c3)._ipp._tcp.local
. TXT (QM)? Canon iR2224 (fe:bd:c3)._ipp._tcp.local. (644)
11:08:15.568019 IP apsit-HP-280-Pro-G6-Microtower-PC.mdns > mdns.mcast.net.mdns: 0 [1a] TXT (QM)? Canon iR2224 (fe:bd:c3)._ipp._tcp.local. (63
8)
^C
11 packets captured
17 packets received by filter
4 packets dropped by kernel
```

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo tcpdump -i enp1s0 dst 192.168.86.29
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp1s0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:09:24.443843 IP _gateway.8090 > apsit-HP-280-Pro-G6-Microtower-PC.36684: Flags [S.], seq 1262061952, ack 3890927406, win 29200, options [ms
s 1460,nop,nop,sackOK,nop,wscale 7], length 0
11:09:24.444669 IP _gateway.8090 > apsit-HP-280-Pro-G6-Microtower-PC.36684: Flags [.], ack 378, win 237, length 0
11:09:24.445611 IP _gateway.8090 > apsit-HP-280-Pro-G6-Microtower-PC.36684: Flags [P.], seq 1:259, ack 378, win 237, length 258
11:09:27.468352 IP _gateway.domain > apsit-HP-280-Pro-G6-Microtower-PC.42414: 22169 NXDomain* 0/0/0 (44)
11:09:30.492451 IP _gateway.domain > apsit-HP-280-Pro-G6-Microtower-PC.54415: 47988 NXDomain* 0/0/0 (46)
11:09:34.809141 IP sl-in-f188.1e100.net.5228 > apsit-HP-280-Pro-G6-Microtower-PC.43302: Flags [.], ack 148288467, win 1044, options [nop,nop,T
S val 3303127054 ecr 213207305], length 0
11:09:34.809151 IP sl-in-f188.1e100.net.5228 > apsit-HP-280-Pro-G6-Microtower-PC.43304: Flags [.], ack 1924106587, win 1043, options [nop,nop,
TS val 2884574080 ecr 213207462], length 0
^C
7 packets captured
8 packets received by filter
0 packets dropped by kernel
```

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo tcpdump -i enp1s0 "tcp[tcpflags] & (tcp-syn) != 0" >/home/apsit/Desktop/syn.txt
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp1s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C4 packets captured
7 packets received by filter
0 packets dropped by kernel
```

syn.txt | ack.txt | fin.txt

```
1 11:12:57.530744 IP 192.168.3.243.64124 > 192.168.3.131.7680: Flags [S], seq 2553154322, win 65535, options [mss 1460,nop,wscale
  8,nop,nop,sackOK], length 0
2 11:12:58.515966 IP 192.168.3.243.64124 > 192.168.3.131.7680: Flags [S], seq 2553154322, win 65535, options [mss 1460,nop,wscale
  8,nop,nop,sackOK], length 0
3 11:13:00.518184 IP 192.168.3.243.64124 > 192.168.3.131.7680: Flags [S], seq 2553154322, win 65535, options [mss 1460,nop,wscale
  8,nop,nop,sackOK], length 0
4 11:13:04.532076 IP 192.168.3.243.64124 > 192.168.3.131.7680: Flags [S], seq 2553154322, win 65535, options [mss 1460,nop,wscale
  8,nop,nop,sackOK], length 0
5
```

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo tcpdump -i enp1s0 "tcp[tcpflags] & (tcp-ack) != 0" >/home/apsit/Desktop/ack.txt
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp1s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C13 packets captured
13 packets received by filter
0 packets dropped by kernel
```

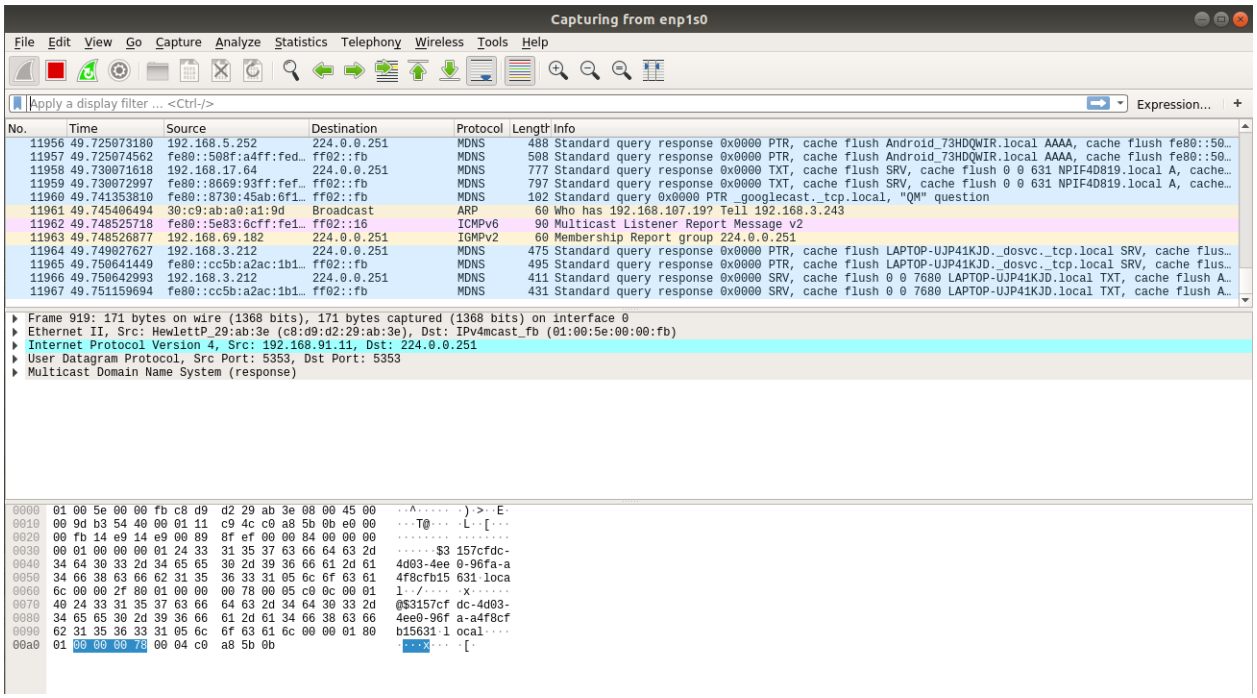
```
1 11:14:46.004441 IP apsit-HP-280-Pro-G6-Microtower-PC.43302 > sl-in-f188.1e100.net.5228: Flags [.], ack 354421439, win 501, options
  [nop,nop,TS val 214242950 ecr 3303393247], length 0
2 11:14:46.008462 IP apsit-HP-280-Pro-G6-Microtower-PC.43304 > sl-in-f188.1e100.net.5228: Flags [.], ack 2763095628, win 501, options
  [nop,nop,TS val 214242954 ecr 2884840278], length 0
3 11:14:46.068193 IP sl-in-f188.1e100.net.5228 > apsit-HP-280-Pro-G6-Microtower-PC.43302: Flags [.], ack 1, win 1044, options [nop,nop,TS val
  3303438314 ecr 214107367], length 0
4 11:14:46.072419 IP sl-in-f188.1e100.net.5228 > apsit-HP-280-Pro-G6-Microtower-PC.43304: Flags [.], ack 1, win 1043, options [nop,nop,TS val
  2884885345 ecr 214107524], length 0
5 11:14:51.635604 IP 192.168.192.194.ssh > 192.168.5.213.58726: Flags [P.], seq 912088650:912088810, ack 2437054235, win 501, length 160
6 11:14:51.895606 IP 192.168.192.194.ssh > 192.168.5.213.58726: Flags [P.], seq 0:160, ack 1, win 501, length 160
7 11:14:52.013482 IP 192.168.192.194.ssh > 192.168.5.213.58726: Flags [P.], seq 160:560, ack 1, win 501, length 400
8 11:14:52.013483 IP 192.168.192.194.ssh > 192.168.5.213.58726: Flags [P.], seq 560:768, ack 1, win 501, length 208
9 11:14:52.013605 IP 192.168.192.194.ssh > 192.168.5.213.58726: Flags [P.], seq 768:896, ack 1, win 501, length 128
10 11:14:52.155597 IP 192.168.192.194.ssh > 192.168.5.213.58726: Flags [P.], seq 0:896, ack 1, win 501, length 896
11 11:14:52.695569 IP 192.168.192.194.ssh > 192.168.5.213.58726: Flags [P.], seq 0:896, ack 1, win 501, length 896
12 11:14:53.751536 IP 192.168.192.194.ssh > 192.168.5.213.58726: Flags [P.], seq 0:896, ack 1, win 501, length 896
13 11:14:55.959480 IP 192.168.192.194.ssh > 192.168.5.213.58726: Flags [P.], seq 0:896, ack 1, win 501, length 896
14
```

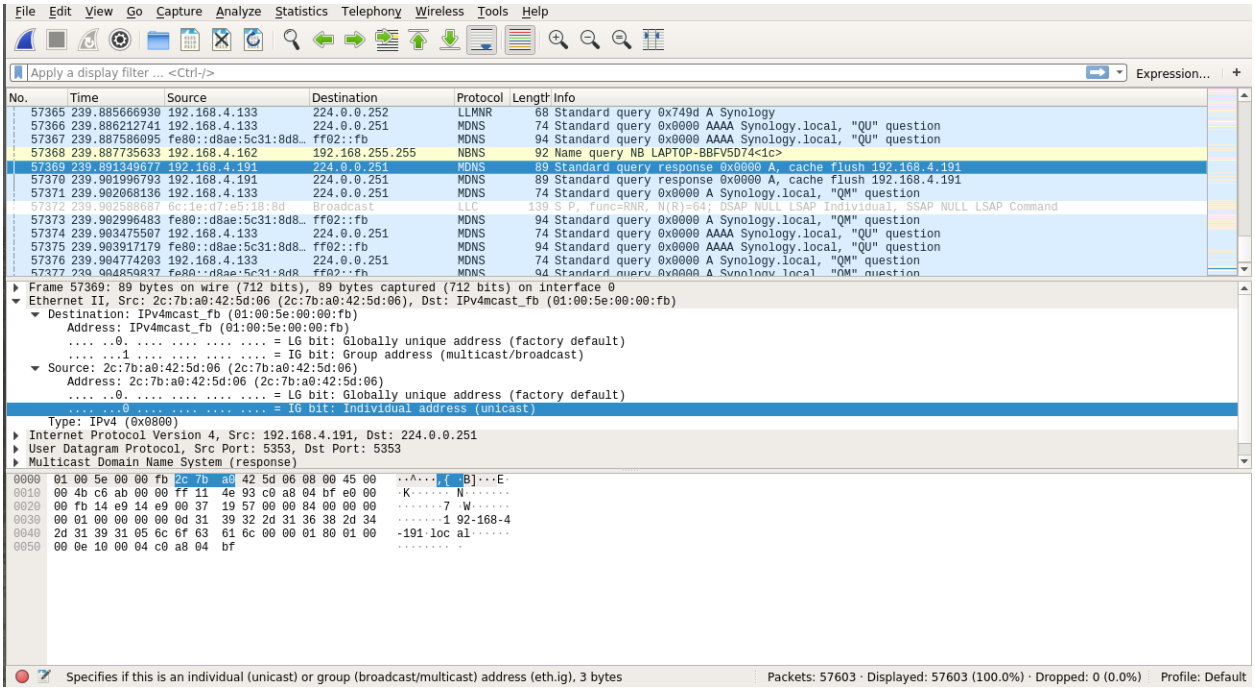
```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo tcpdump -i enp1s0 "tcp[tcpflags] & (tcp-fin) != 0" >/home/apsit/Desktop/fin.txt
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp1s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C2 packets captured
3 packets received by filter
0 packets dropped by kernel
```

```
1 11:19:18.372549 IP apsit-HP-280-Pro-G6-Microtower-PC.39364 > _gateway.8090: Flags [F.], seq 918158082, ack 3843971460, win 501, length 0
2 11:19:25.473366 IP _gateway.8090 > apsit-HP-280-Pro-G6-Microtower-PC.49312: Flags [F.], seq 978076490, ack 3935043836, win 237, length 0
3
```

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo tcpdump -i enp1s0 -x -X -A -nvvv port 22 > ssh.txt
tcpdump: listening on enp1s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C0 packets captured
2 packets received by filter
0 packets dropped by kernel
```

Wireshark





```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo ip link set enp1s0 promisc on
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
docker0   1500        0      0      0 0             0      0      0      0 BMU
enp1s0    1500  1465371      0   5148 0         23036      0      0      0 BMPRU
lo       65536     2852      0      0 0          2852      0      0      0 LRU
```

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo ip link set enp1s0 promisc off
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
docker0   1500        0      0      0 0             0      0      0      0 BMU
enp1s0    1500  1477296      0   5214 0         23103      0      0      0 BMRU
lo       65536     2866      0      0 0          2866      0      0      0 LRU
```

Conclusion:

In this experiment, we learnt and understood to study analysis of network packets by sing open source sniffing tools like tcpdump and Wireshark in promiscuous and non-promiscuous mode.