Roll no. : 53
Name: Shreya Kamath
Date: 12th September, 2023.

LAB ASSIGNMENT NO. 7

AIM: Study of packet sniffer tools Wireshark and TCPDUMP.

LAB OUTCOME ATTAINED:

LO 3: Explore the different network reconnaissance tools to gather information about networks.

THEORY:

TCPdump is a widely used network packet analyzer command-line tool. It allows users to capture and analyse network traffic on a system. It's particularly valuable for diagnosing network issues, troubleshooting, and monitoring network activities.

Installation of TCPdump:
sudo apt-get install tcpdump

Choosing an interface:
By default, tcpdump captures packets on all interfaces. To view a summary of available interfaces, run the command:
tcpdump -D

Basic command for sniffing
 # tcpdump -n
The -n parameter is given to stop tcpdump from resolving ip addresses to hostnames.
The verbose switch comes in handy to increase the display resolution of this packet. Here is a quick example:
tcpdump -v -n

Selecting packets with specific protocol
 # tcpdump -n tcp
#tcpdump -n icmp

Capturing traffic from particular host or port
Expressions can be used to specify source ip, destination ip, and port numbers. The next example picks up all those packets with source address 172.16.92.1
 # tcpdump -n src 172.16.92.1
 # tcpdump -n dst 172.16.92.1
 # tcpdump -n port 80
 # tcpdump port 80

Specific Packets from specific port
 # tcpdump udp and src port 53

Observing packets within a specific port range
 # tcpdump -n portrange 1-80

Roll no. : 53
Name: Shreya Kamath
Date: 12th September, 2023.

It shows all packets whose source or destination port is between 1 to 80
tcpdump -n src port 443

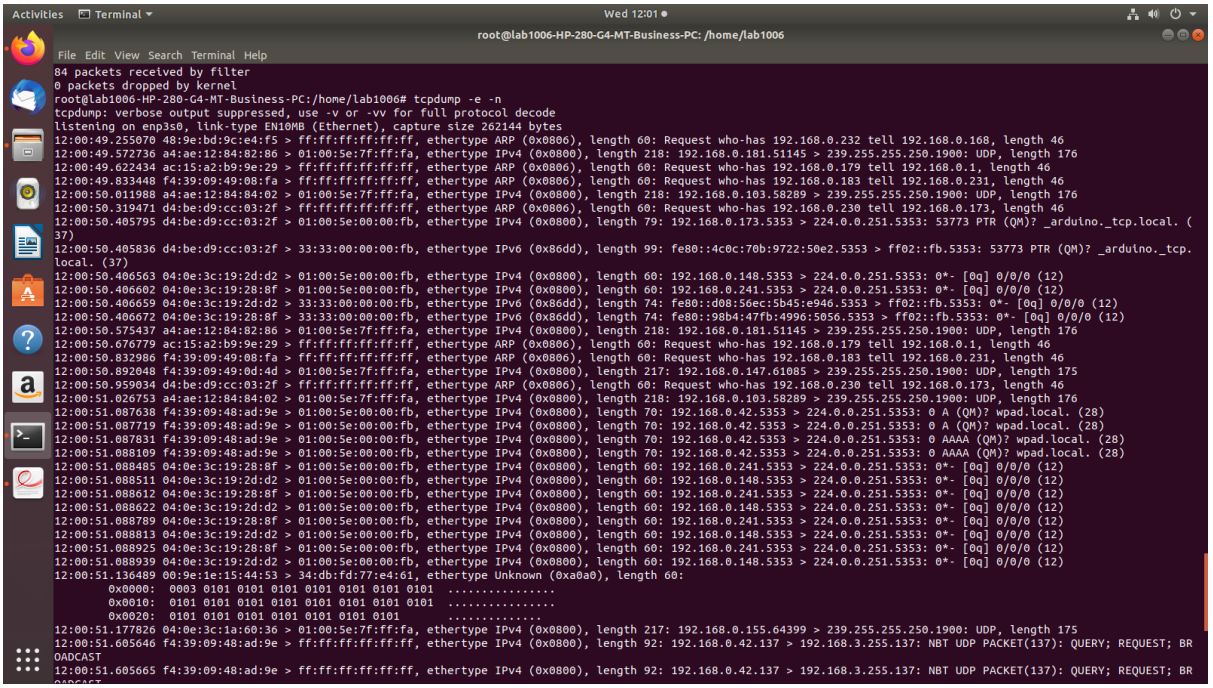
OUTPUT:

```
(socket: Operation not permitted)
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo su
[sudo] password for lab1006:
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:56:26.322051 ARP, Request who-has 192.168.0.183 tell 192.168.0.212, length 46
11:56:26.363690 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 04:0e:3c:1a:5c:74, length 300
11:56:26.546788 IP 192.168.0.234.54309 > 239.255.255.250.1900: UDP, length 176
11:56:26.807417 IP 192.168.0.249.137 > 192.168.0.255.137: NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
11:56:26.868992 ARP, Request who-has 192.168.0.183 tell 192.168.0.212, length 46
11:56:26.958281 ARP, Request who-has 192.168.0.227 tell 192.168.0.125, length 46
11:56:27.547501 IP 192.168.0.242.60818 > 239.255.255.250.1900: UDP, length 175
11:56:27.558155 IP 192.168.0.234.54309 > 239.255.255.250.1900: UDP, length 176
11:56:27.708811 ARP, Request who-has 192.168.0.227 tell 192.168.0.125, length 46
11:56:27.745038 IP 192.168.0.199.5353 > 224.0.0.251.5353: 0 PTR (QU)? _microsoft_mcc._tcp.local. (43)
11:56:27.745081 IP6 fe80::e8f8:c12e:dd5e:4599.5353 > ff02::fb.5353: 0 PTR (QU)? _microsoft_mcc._tcp.local. (43)
11:56:27.745201 IP 192.168.0.241.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
11:56:27.745296 IP6 fe80::98b4:47fb:4996:5056.5353 > ff02::fb.5353: 0*- [0q] 0/0/0 (12)
11:56:27.745655 IP 192.168.0.148.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
11:56:27.745885 IP6 fe80::d08:56ec:5b45:e946.5353 > ff02::fb.5353: 0*- [0q] 0/0/0 (12)
11:56:27.868763 ARP, Request who-has 192.168.0.183 tell 192.168.0.212, length 46
11:56:27.872449 IP6 fe80::3011:4165:bb89:8983 > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
11:56:28.044266 IP6 fe80::3011:4165:bb89:8983 > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
11:56:28.054712 IP 192.168.0.167.55976 > 239.255.255.250.1900: UDP, length 176
11:56:28.556738 IP 192.168.0.242.60818 > 239.255.255.250.1900: UDP, length 175
11:56:28.708674 ARP, Request who-has 192.168.0.227 tell 192.168.0.125, length 46
11:56:28.744389 IP 192.168.0.199.5353 > 224.0.0.251.5353: 0 PTR (QM)? _microsoft_mcc._tcp.local. (43)
11:56:28.744431 IP6 fe80::e8f8:c12e:dd5e:4599.5353 > ff02::fb.5353: 0 PTR (QM)? _microsoft_mcc._tcp.local. (43)
11:56:28.744488 IP 192.168.0.241.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
11:56:28.744556 IP6 fe80::98b4:47fb:4996:5056.5353 > ff02::fb.5353: 0*- [0q] 0/0/0 (12)
11:56:28.745095 IP 192.168.0.148.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
11:56:28.745295 IP6 fe80::d08:56ec:5b45:e946.5353 > ff02::fb.5353: 0*- [0q] 0/0/0 (12)
11:56:28.759744 IP 192.168.0.173.5353 > 224.0.0.251.5353: 25873 PTR (QM)? _arduino._tcp.local. (37)
11:56:28.759801 IP6 fe80::4c0c:70b:9722:50e2.5353 > ff02::fb.5353: 25873 PTR (QM)? _arduino._tcp.local. (37)
11:56:28.759831 IP 192.168.0.241.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
11:56:28.759939 IP6 fe80::98b4:47fb:4996:5056.5353 > ff02::fb.5353: 0*- [0q] 0/0/0 (12)
11:56:28.760491 IP 192.168.0.148.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
11:56:28.760694 IP6 fe80::d08:56ec:5b45:e946.5353 > ff02::fb.5353: 0*- [0q] 0/0/0 (12)
11:56:29.067397 IP 192.168.0.167.55976 > 239.255.255.250.1900: UDP, length 176
11:56:29.568146 IP 192.168.0.242.60818 > 239.255.255.250.1900: UDP, length 175
11:56:29.933505 IP 192.168.0.212.54376 > 239.255.255.250.1900: UDP, length 176
11:56:30.078769 IP 192.168.0.167.55976 > 239.255.255.250.1900: UDP, length 176
11:56:30.251523 IP 192.168.0.149.62299 > 239.255.255.250.1900: UDP, length 175
11:56:30.577083 IP 192.168.0.242.60818 > 239.255.255.250.1900: UDP, length 175
^C
```

```
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -v -n
tcpdump: listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:57:54.634904 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.183 tell 192.168.0.129, length 46
11:57:54.645763 IP (tos 0x0, ttl 64, id 2715, offset 0, flags [DF], proto TCP (6), length 427)
    192.168.0.182.57404 > 142.250.183.142.443: Flags [P.], cksum 0xbd20 (correct), seq 2449946025:2449946400, ack 723247426, win 501, options [nop,nop,TS val 426004561
ecr 1696330276], length 375
11:57:54.645894 IP (tos 0x0, ttl 64, id 2716, offset 0, flags [DF], proto TCP (6), length 179)
    192.168.0.182.57404 > 142.250.183.142.443: Flags [P.], cksum 0x9cb8 (correct), seq 375:502, ack 1, win 501, options [nop,nop,TS val 426004561 ecr 1696330276], lengt
h 127
11:57:54.645947 IP (tos 0x0, ttl 64, id 2717, offset 0, flags [DF], proto TCP (6), length 1452)
    192.168.0.182.57404 > 142.250.183.142.443: Flags [.], cksum 0x725b (correct), seq 502:1902, ack 1, win 501, options [nop,nop,TS val 426004561 ecr 1696330276], lengt
h 1400
11:57:54.645956 IP (tos 0x0, ttl 64, id 2718, offset 0, flags [DF], proto TCP (6), length 1452)
    192.168.0.182.57404 > 142.250.183.142.443: Flags [.], cksum 0x3813 (correct), seq 1902:3302, ack 1, win 501, options [nop,nop,TS val 426004561 ecr 1696330276], leng
th 1400
11:57:54.645963 IP (tos 0x0, ttl 64, id 2719, offset 0, flags [DF], proto TCP (6), length 1452)
    192.168.0.182.57404 > 142.250.183.142.443: Flags [.], cksum 0x9c64 (correct), seq 3302:4702, ack 1, win 501, options [nop,nop,TS val 426004561 ecr 1696330276], leng
th 1400
11:57:54.645969 IP (tos 0x0, ttl 64, id 2720, offset 0, flags [DF], proto TCP (6), length 1452)
    192.168.0.182.57404 > 142.250.183.142.443: Flags [.], cksum 0xaa7b (correct), seq 4702:6102, ack 1, win 501, options [nop,nop,TS val 426004561 ecr 1696330276], leng
th 1400
11:57:54.645976 IP (tos 0x0, ttl 64, id 2721, offset 0, flags [DF], proto TCP (6), length 1452)
    192.168.0.182.57404 > 142.250.183.142.443: Flags [.], cksum 0x5aad (correct), seq 6102:7502, ack 1, win 501, options [nop,nop,TS val 426004561 ecr 1696330276], leng
th 1400
11:57:54.646002 IP (tos 0x0, ttl 64, id 2722, offset 0, flags [DF], proto TCP (6), length 115)
    192.168.0.182.57404 > 142.250.183.142.443: Flags [P.], cksum 0xcd62 (correct), seq 7502:7565, ack 1, win 501, options [nop,nop,TS val 426004561 ecr 1696330276], len
gth 63
11:57:54.647845 IP (tos 0x0, ttl 59, id 44107, offset 0, flags [none], proto TCP (6), length 52)
    142.250.183.142.443 > 192.168.0.182.57404: Flags [.], cksum 0xc086 (correct), ack 502, win 2963, options [nop,nop,TS val 1696340974 ecr 426004561], length 0
11:57:54.647881 IP (tos 0x0, ttl 59, id 44108, offset 0, flags [none], proto TCP (6), length 52)
    142.250.183.142.443 > 192.168.0.182.57404: Flags [.], cksum 0xbb0e (correct), ack 1902, win 2963, options [nop,nop,TS val 1696340974 ecr 426004561], length 0
11:57:54.647887 IP (tos 0x0, ttl 59, id 44109, offset 0, flags [none], proto TCP (6), length 52)
    142.250.183.142.443 > 192.168.0.182.57404: Flags [.], cksum 0xb59b (correct), ack 3302, win 2958, options [nop,nop,TS val 1696340974 ecr 426004561], length 0
11:57:54.647895 IP (tos 0x0, ttl 59, id 44106, offset 0, flags [none], proto TCP (6), length 52)
    142.250.183.142.443 > 192.168.0.182.57404: Flags [.], cksum 0xc105 (correct), ack 375, win 2963, options [nop,nop,TS val 1696340974 ecr 426004561], length 0
11:57:54.647898 IP (tos 0x0, ttl 59, id 44110, offset 0, flags [none], proto TCP (6), length 52)
    142.250.183.142.443 > 192.168.0.182.57404: Flags [.], cksum 0xb028 (correct), ack 4702, win 2953, options [nop,nop,TS val 1696340974 ecr 426004561], length 0
11:57:54.647984 IP (tos 0x0, ttl 59, id 44111, offset 0, flags [none], proto TCP (6), length 52)
    142.250.183.142.443 > 192.168.0.182.57404: Flags [.], cksum 0xaab5 (correct), ack 6102, win 2948, options [nop,nop,TS val 1696340974 ecr 426004561], length 0
11:57:54.648228 IP (tos 0x0, ttl 59, id 44112, offset 0, flags [none], proto TCP (6), length 52)
    142.250.183.142.443 > 192.168.0.182.57404: Flags [.], cksum 0xa542 (correct), ack 7502, win 2943, options [nop,nop,TS val 1696340974 ecr 426004561], length 0
11:57:54.648423 IP (tos 0x0, ttl 59, id 44113, offset 0, flags [none], proto TCP (6), length 52)
```

Roll no. : 53
Name: Shreya Kamath
Date: 12th September, 2023.

```
11:57:55.652394 IP (tos 0x0, ttl 1, id 13855, offset 0, flags [none], proto UDP (17), length 40)
    192.168.0.148.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
11:57:55.668456 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.150 tell 192.168.0.138, length 46
11:57:55.808503 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.226 tell 192.168.0.214, length 46
11:57:55.875091 IP (tos 0x0, ttl 1, id 56459, offset 0, flags [none], proto UDP (17), length 203)
    192.168.0.244.52422 > 239.255.255.250.1900: UDP, length 175
11:57:55.941400 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.179 tell 192.168.0.1, length 46
11:57:56.037519 IP (tos 0x0, ttl 1, id 739, offset 0, flags [none], proto UDP (17), length 204)
    192.168.0.231.63797 > 239.255.255.250.1900: UDP, length 176
11:57:56.041545 IP (tos 0x0, ttl 1, id 25603, offset 0, flags [DF], proto UDP (17), length 201)
    192.168.0.207.52156 > 239.255.255.250.1900: UDP, length 173
11:57:56.141906 IP (tos 0x0, ttl 1, id 44660, offset 0, flags [none], proto UDP (17), length 203)
    192.168.0.175.52366 > 239.255.255.250.1900: UDP, length 175
11:57:56.147798 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.183 tell 192.168.0.129, length 46
11:57:56.228780 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.224 tell 192.168.0.167, length 46
11:57:56.352459 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.224 tell 192.168.0.175, length 46
11:57:56.514920 00:9e:1e:15:44:53 > 34:db:fd:77:e4:61, ethertype Unknown (0xa0a0), length 60:
        0x0000:  0003 0101 0101 0101 0101 0101 0101 0101  ................
        0x0010:  0101 0101 0101 0101 0101 0101 0101 0101  ................
        0x0020:  0101 0101 0101 0101 0101 0101            ............
11:57:56.549537 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.224 tell 192.168.0.101, length 46
11:57:56.587299 IP (tos 0x0, ttl 64, id 56181, offset 0, flags [DF], proto TCP (6), length 98)
    192.168.0.182.40336 > 142.250.67.141.443: Flags [P.], cksum 0x2f62 (correct), seq 144376332:144376378, ack 752583640, win 501, options [nop,nop,TS val 1902569488 ec
r 2327487075], length 46
11:57:56.589288 IP (tos 0x0, ttl 122, id 11714, offset 0, flags [none], proto TCP (6), length 98)
    142.250.67.141.443 > 192.168.0.182.40336: Flags [P.], cksum 0xf7e4 (correct), seq 1:47, ack 46, win 309, options [nop,nop,TS val 2327545079 ecr 1902569488], length
46
11:57:56.589332 IP (tos 0x0, ttl 64, id 56182, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.182.40336 > 142.250.67.141.443: Flags [.], cksum 0x1cb3 (correct), ack 47, win 501, options [nop,nop,TS val 1902569491 ecr 2327545079], length 0
11:57:56.660732 IP (tos 0x0, ttl 1, id 36916, offset 0, flags [none], proto UDP (17), length 68)
    192.168.0.129.5353 > 224.0.0.251.5353: 0 PTR (QM)? _googlecast._tcp.local. (40)
11:57:56.660771 IP (tos 0x0, ttl 1, id 17773, offset 0, flags [none], proto UDP (17), length 40)
    192.168.0.241.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
11:57:56.661298 IP (tos 0x0, ttl 1, id 13856, offset 0, flags [none], proto UDP (17), length 40)
    192.168.0.148.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
11:57:56.729954 IP (tos 0x0, ttl 128, id 19827, offset 0, flags [none], proto UDP (17), length 78)
    192.168.0.168.137 > 192.168.0.255.137: NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
11:57:56.897383 IP (tos 0x0, ttl 1, id 9041, offset 0, flags [none], proto UDP (17), length 204)
    192.168.0.190.57147 > 239.255.255.250.1900: UDP, length 176
11:57:56.937331 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.179 tell 192.168.0.1, length 46
^C
84 packets captured
84 packets received by filter
0 packets dropped by kernel
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006#
```



Roll no. : 53
Name: Shreya Kamath
Date: 12th September, 2023.

```
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -e -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:00:49.255070 48:9e:bd:9c:e4:f5 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 192.168.0.232 tell 192.168.0.168, length 46
12:00:49.572736 a4:ae:12:84:82:86 > 01:00:5e:7f:ff:fa, ethertype IPv4 (0x0800), length 218: 192.168.0.181.51145 > 239.255.255.250.1900: UDP, length 176
12:00:49.622434 ac:15:a2:b9:9e:29 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 192.168.0.179 tell 192.168.0.1, length 46
12:00:49.833448 f4:39:09:49:08:fa > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 192.168.0.183 tell 192.168.0.231, length 46
12:00:50.011988 a4:ae:12:84:84:02 > 01:00:5e:7f:ff:fa, ethertype IPv4 (0x0800), length 218: 192.168.0.103.58289 > 239.255.255.250.1900: UDP, length 176
12:00:50.319471 d4:be:d9:cc:03:2f > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 192.168.0.230 tell 192.168.0.173, length 46
12:00:50.405795 d4:be:d9:cc:03:2f > 01:00:5e:00:00:fb, ethertype IPv4 (0x0800), length 79: 192.168.0.173.5353 > 224.0.0.251.5353: 53773 PTR (QM)? _arduino._tcp.local. (
37)
12:00:50.405836 d4:be:d9:cc:03:2f > 33:33:00:00:00:fb, ethertype IPv6 (0x86dd), length 99: fe80::4c0c:70b:9722:50e2.5353 > ff02::fb.5353: 53773 PTR (QM)? _arduino._tcp.
local. (37)
12:00:50.406563 04:0e:3c:19:2d:d2 > 01:00:5e:00:00:fb, ethertype IPv4 (0x0800), length 60: 192.168.0.148.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
12:00:50.406602 04:0e:3c:19:28:8f > 01:00:5e:00:00:fb, ethertype IPv4 (0x0800), length 60: 192.168.0.241.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
12:00:50.406659 04:0e:3c:19:2d:d2 > 33:33:00:00:00:fb, ethertype IPv6 (0x86dd), length 74: fe80::d08:56ec:5b45:e946.5353 > ff02::fb.5353: 0*- [0q] 0/0/0 (12)
12:00:50.406672 04:0e:3c:19:28:8f > 33:33:00:00:00:fb, ethertype IPv6 (0x86dd), length 74: fe80::98b4:47fb:4996:5056.5353 > ff02::fb.5353: 0*- [0q] 0/0/0 (12)
12:00:50.575437 a4:ae:12:84:82:86 > 01:00:5e:7f:ff:fa, ethertype IPv4 (0x0800), length 218: 192.168.0.181.51145 > 239.255.255.250.1900: UDP, length 176
12:00:50.676779 ac:15:a2:b9:9e:29 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 192.168.0.179 tell 192.168.0.1, length 46
12:00:50.832986 f4:39:09:49:08:fa > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 192.168.0.183 tell 192.168.0.231, length 46
12:00:50.892048 f4:39:09:49:0d:4d > 01:00:5e:7f:ff:fa, ethertype IPv4 (0x0800), length 217: 192.168.0.147.61085 > 239.255.255.250.1900: UDP, length 175
12:00:50.959034 d4:be:d9:cc:03:2f > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 192.168.0.230 tell 192.168.0.173, length 46
12:00:51.026753 a4:ae:12:84:84:02 > 01:00:5e:7f:ff:fa, ethertype IPv4 (0x0800), length 218: 192.168.0.103.58289 > 239.255.255.250.1900: UDP, length 176
12:00:51.087638 f4:39:09:48:ad:9e > 01:00:5e:00:00:fb, ethertype IPv4 (0x0800), length 70: 192.168.0.42.5353 > 224.0.0.251.5353: 0 A (QM)? wpad.local. (28)
12:00:51.087719 f4:39:09:48:ad:9e > 01:00:5e:00:00:fb, ethertype IPv4 (0x0800), length 70: 192.168.0.42.5353 > 224.0.0.251.5353: 0 A (QM)? wpad.local. (28)
12:00:51.087831 f4:39:09:48:ad:9e > 01:00:5e:00:00:fb, ethertype IPv4 (0x0800), length 70: 192.168.0.42.5353 > 224.0.0.251.5353: 0 AAAA (QM)? wpad.local. (28)
12:00:51.088109 f4:39:09:48:ad:9e > 01:00:5e:00:00:fb, ethertype IPv4 (0x0800), length 70: 192.168.0.42.5353 > 224.0.0.251.5353: 0 AAAA (QM)? wpad.local. (28)
12:00:51.088485 04:0e:3c:19:28:8f > 01:00:5e:00:00:fb, ethertype IPv4 (0x0800), length 60: 192.168.0.241.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
12:00:51.088511 04:0e:3c:19:2d:d2 > 01:00:5e:00:00:fb, ethertype IPv4 (0x0800), length 60: 192.168.0.148.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
12:00:51.088612 04:0e:3c:19:28:8f > 01:00:5e:00:00:fb, ethertype IPv4 (0x0800), length 60: 192.168.0.241.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
12:00:51.088622 04:0e:3c:19:2d:d2 > 01:00:5e:00:00:fb, ethertype IPv4 (0x0800), length 60: 192.168.0.148.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
12:00:51.088789 04:0e:3c:19:28:8f > 01:00:5e:00:00:fb, ethertype IPv4 (0x0800), length 60: 192.168.0.241.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
12:00:51.088813 04:0e:3c:19:2d:d2 > 01:00:5e:00:00:fb, ethertype IPv4 (0x0800), length 60: 192.168.0.148.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
12:00:51.088925 04:0e:3c:19:28:8f > 01:00:5e:00:00:fb, ethertype IPv4 (0x0800), length 60: 192.168.0.241.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
12:00:51.088939 04:0e:3c:19:2d:d2 > 01:00:5e:00:00:fb, ethertype IPv4 (0x0800), length 60: 192.168.0.148.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
12:00:51.136489 00:9e:1e:15:44:53 > 34:db:fd:77:e4:61, ethertype Unknown (0xa0a0), length 60:
        0x0000:  0003 0101 0101 0101 0101 0101 0101 0101  ................
        0x0010:  0101 0101 0101 0101 0101 0101 0101 0101  ................
        0x0020:  0101 0101 0101 0101 0101 0101 0101       ..............
12:00:51.177826 04:0e:3c:1a:60:36 > 01:00:5e:7f:ff:fa, ethertype IPv4 (0x0800), length 217: 192.168.0.155.64399 > 239.255.255.250.1900: UDP, length 175
12:00:51.605646 f4:39:09:48:ad:9e > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 92: 192.168.0.42.137 > 192.168.3.255.137: NBT UDP PACKET(137): QUERY; REQUEST; BR
OADCAST
12:00:51.605665 f4:39:09:48:ad:9e > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 92: 192.168.0.42.137 > 192.168.3.255.137: NBT UDP PACKET(137): QUERY; REQUEST; BR
```

```
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -n src  192.168.0.182
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:02:50.363335 ARP, Reply 192.168.0.182 is-at 04:0e:3c:1a:60:28, length 28
12:02:50.363359 ARP, Reply 192.168.0.182 is-at 04:0e:3c:1a:60:28, length 28
12:02:50.522515 IP 192.168.0.182 > 192.168.0.1: ICMP 192.168.0.182 udp port 137 unreachable, length 86
12:02:50.538412 IP 192.168.0.182 > 192.168.0.1: ICMP 192.168.0.182 udp port 137 unreachable, length 86
12:02:52.774977 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], ack 902728857, win 7327, options [nop,nop,TS val 1145898009 ecr 416470929], length 0
12:03:00.311767 IP 192.168.0.182.57404 > 142.250.183.142.443: Flags [P.], seq 2450222053:2450222435, ack 723285217, win 501, options [nop,nop,TS val 426310217 ecr 16966
18757], length 382
12:03:00.311803 IP 192.168.0.182.57404 > 142.250.183.142.443: Flags [.], seq 382:1782, ack 1, win 501, options [nop,nop,TS val 426310217 ecr 1696618757], length 1400
12:03:00.311870 IP 192.168.0.182.57404 > 142.250.183.142.443: Flags [.], seq 1782:3182, ack 1, win 501, options [nop,nop,TS val 426310217 ecr 1696618757], length 1400
12:03:00.311889 IP 192.168.0.182.57404 > 142.250.183.142.443: Flags [.], seq 3182:4582, ack 1, win 501, options [nop,nop,TS val 426310217 ecr 1696618757], length 1400
12:03:00.312010 IP 192.168.0.182.57404 > 142.250.183.142.443: Flags [.], seq 4582:5982, ack 1, win 501, options [nop,nop,TS val 426310217 ecr 1696618757], length 1400
12:03:00.312013 IP 192.168.0.182.57404 > 142.250.183.142.443: Flags [P.], seq 5982:6075, ack 1, win 501, options [nop,nop,TS val 426310217 ecr 1696618757], length 93
12:03:00.313718 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 0:1400, ack 1, win 7327, options [nop,nop,TS val 1145905548 ecr 416470929], length 1400
12:03:00.313735 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 1400:2800, ack 1, win 7327, options [nop,nop,TS val 1145905548 ecr 416470929], length 1400
12:03:00.313737 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 2800:4200, ack 1, win 7327, options [nop,nop,TS val 1145905548 ecr 416470929], length 1400
12:03:00.313846 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 4200:5600, ack 1, win 7327, options [nop,nop,TS val 1145905548 ecr 416470929], length 1400
12:03:00.313850 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 5600:7000, ack 1, win 7327, options [nop,nop,TS val 1145905548 ecr 416470929], length 1400
12:03:00.313852 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 7000:8400, ack 1, win 7327, options [nop,nop,TS val 1145905548 ecr 416470929], length 1400
12:03:00.313946 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [P.], seq 8400:9632, ack 1, win 7327, options [nop,nop,TS val 1145905548 ecr 416470929], length 1232
12:03:00.438454 IP 192.168.0.182.57404 > 142.250.183.142.443: Flags [.], ack 862, win 501, options [nop,nop,TS val 426310344 ecr 1696646759], length 0
12:03:00.440774 IP 192.168.0.182.57404 > 142.250.183.142.443: Flags [.], ack 1061, win 501, options [nop,nop,TS val 426310346 ecr 1696646762], length 0
12:03:00.440839 IP 192.168.0.182.57404 > 142.250.183.142.443: Flags [P.], seq 6075:6121, ack 1061, win 501, options [nop,nop,TS val 426310346 ecr 1696646762], length 46
12:03:00.660391 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], ack 678, win 7327, options [nop,nop,TS val 1145905895 ecr 416478814], length 0
12:03:00.662830 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], ack 716, win 7327, options [nop,nop,TS val 1145905897 ecr 416478817], length 0
12:03:00.662865 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], ack 762, win 7327, options [nop,nop,TS val 1145905897 ecr 416478817], length 0
12:03:00.663201 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [P.], seq 9632:9678, ack 762, win 7327, options [nop,nop,TS val 1145905897 ecr 416478817], length 46
12:03:03.143723 ARP, Reply 192.168.0.182 is-at 04:0e:3c:1a:60:28, length 28
12:03:03.313462 IP 192.168.0.182.57404 > 142.250.183.142.443: Flags [P.], seq 6121:6656, ack 1061, win 501, options [nop,nop,TS val 426313219 ecr 1696646763], length 53
5
12:03:03.313499 IP 192.168.0.182.57404 > 142.250.183.142.443: Flags [.], seq 6656:8056, ack 1061, win 501, options [nop,nop,TS val 426313219 ecr 1696646763], length 140
0
12:03:03.313501 IP 192.168.0.182.57404 > 142.250.183.142.443: Flags [.], seq 8056:9456, ack 1061, win 501, options [nop,nop,TS val 426313219 ecr 1696646763], length 140
0
12:03:03.313575 IP 192.168.0.182.57404 > 142.250.183.142.443: Flags [.], seq 9456:10856, ack 1061, win 501, options [nop,nop,TS val 426313219 ecr 1696646763], length 14
00
```

Roll no. : 53
Name: Shreya Kamath
Date: 12th September, 2023.

```
12:03:03.316865 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 18596:19996, ack 762, win 7327, options [nop,nop,TS val 1145908551 ecr 416478821], length 14
00
12:03:03.317040 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 19996:21396, ack 762, win 7327, options [nop,nop,TS val 1145908551 ecr 416478821], length 14
00
12:03:03.317044 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 21396:22796, ack 762, win 7327, options [nop,nop,TS val 1145908551 ecr 416478821], length 14
00
12:03:03.319238 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 22796:24196, ack 762, win 7327, options [nop,nop,TS val 1145908553 ecr 416481474], length 14
00
12:03:03.319242 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 24196:25596, ack 762, win 7327, options [nop,nop,TS val 1145908553 ecr 416481474], length 14
00
12:03:03.319243 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 25596:26996, ack 762, win 7327, options [nop,nop,TS val 1145908553 ecr 416481474], length 14
00
12:03:03.319246 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 26996:28396, ack 762, win 7327, options [nop,nop,TS val 1145908553 ecr 416481474], length 14
00
12:03:03.319287 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 28396:29796, ack 762, win 7327, options [nop,nop,TS val 1145908553 ecr 416481474], length 14
00
12:03:03.319289 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 29796:31196, ack 762, win 7327, options [nop,nop,TS val 1145908553 ecr 416481474], length 14
00
12:03:03.319290 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 31196:32596, ack 762, win 7327, options [nop,nop,TS val 1145908553 ecr 416481474], length 14
00
12:03:03.319377 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 32596:33996, ack 762, win 7327, options [nop,nop,TS val 1145908553 ecr 416481474], length 14
00
12:03:03.319519 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 33996:35396, ack 762, win 7327, options [nop,nop,TS val 1145908554 ecr 416481474], length 14
00
12:03:03.319551 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 35396:36796, ack 762, win 7327, options [nop,nop,TS val 1145908554 ecr 416481474], length 14
00
12:03:03.319559 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 36796:38196, ack 762, win 7327, options [nop,nop,TS val 1145908554 ecr 416481474], length 14
00
12:03:03.319745 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 38196:39596, ack 762, win 7327, options [nop,nop,TS val 1145908554 ecr 416481474], length 14
00
12:03:03.319839 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 39596:40996, ack 762, win 7327, options [nop,nop,TS val 1145908554 ecr 416481474], length 14
00
12:03:03.319845 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], seq 40996:42396, ack 762, win 7327, options [nop,nop,TS val 1145908554 ecr 416481474], length 14
00
12:03:03.319961 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [P.], seq 42396:43340, ack 762, win 7327, options [nop,nop,TS val 1145908554 ecr 416481474], length 9
44
12:03:03.456370 IP 192.168.0.182.57404 > 142.250.183.142.443: Flags [.], ack 1982, win 501, options [nop,nop,TS val 426313361 ecr 1696649777], length 0
12:03:03.457974 IP 192.168.0.182.57404 > 142.250.183.142.443: Flags [.], ack 2195, win 501, options [nop,nop,TS val 426313363 ecr 1696649779], length 0
12:03:03.458039 IP 192.168.0.182.57404 > 142.250.183.142.443: Flags [P.], seq 28575:28621, ack 2195, win 501, options [nop,nop,TS val 426313363 ecr 1696649779], length
46
^C
71 packets captured
71 packets received by filter
0 packets dropped by kernel
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006#
```

```
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -n icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:04:03.668863 IP 192.168.0.182 > 192.168.0.1: ICMP 192.168.0.182 udp port 137 unreachable, length 86
12:04:03.680528 IP 192.168.0.182 > 192.168.0.1: ICMP 192.168.0.182 udp port 137 unreachable, length 86
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006#
```

```
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -n portrange 1-79
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:06:13.356129 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 04:0e:3c:1a:5c:74, length 300
12:06:20.106423 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 04:0e:3c:1a:5c:74, length 300
12:06:23.051133 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 04:0e:3c:1a:5c:74, length 300
12:06:23.760201 IP 192.168.0.182.58135 > 192.168.0.1.53: 56866+ [1au] A? docs.google.com. (44)
12:06:23.761539 IP 192.168.0.1.53 > 192.168.0.182.58135: 56866 1/0/1 A 142.250.192.78 (60)
^C
5 packets captured
5 packets received by filter
0 packets dropped by kernel
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -n src 192.168.0.182
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:07:36.254761 ARP, Reply 192.168.0.182 is-at 04:0e:3c:1a:60:28, length 28
12:07:36.912758 IP 192.168.0.182.5353 > 224.0.0.251.5353: 0*- [0q] 2/0/0 (Cache flush) AAAA fe80::bbb9:308f:e56e:ecaa, (Cache flush) A 192.168.0.182 (96)
12:07:39.676165 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], ack 902734872, win 7327, options [nop,nop,TS val 1146184901 ecr 416757825], length 0
12:07:44.877925 ARP, Request who-has 192.168.0.1 tell 192.168.0.182, length 28
12:07:51.363081 IP 192.168.0.182.57404 > 142.250.183.142.443: Flags [P.], seq 2450260655:2450260701, ack 723289559, win 501, options [nop,nop,TS val 426601258 ecr 16968
84915], length 46
12:07:51.363433 IP 192.168.0.182.57404 > 142.250.183.142.443: Flags [P.], seq 46:77, ack 1, win 501, options [nop,nop,TS val 426601259 ecr 1696884915], length 31
12:07:51.363462 IP 192.168.0.182.57404 > 142.250.183.142.443: Flags [F.], seq 77, ack 1, win 501, options [nop,nop,TS val 426601259 ecr 1696884915], length 0
12:07:51.365222 IP 192.168.0.182.57404 > 142.250.183.142.443: Flags [.], ack 2, win 501, options [nop,nop,TS val 426601261 ecr 1696937681], length 0
12:07:51.451584 IP 192.168.0.182.5353 > 224.0.0.251.5353: 0 [7q] PTR (QM)? _ftp._tcp.local. PTR (QM)? _nfs._tcp.local. PTR (QM)? _afpovertcp._tcp.local. PTR (QM)? _smb.
_tcp.local. PTR (QM)? _sftp-ssh._tcp.local. PTR (QM)? _webdavs._tcp.local. PTR (QM)? _webdav._tcp.local. (118)
12:07:53.837761 ARP, Reply 192.168.0.182 is-at 04:0e:3c:1a:60:28, length 28
12:07:56.598092 IP 192.168.0.182.34564 > 142.250.67.141.443: Flags [P.], seq 2022881181:2022881227, ack 2578354394, win 501, options [nop,nop,TS val 1903169479 ecr 3613
841975], length 46
12:07:56.600228 IP 192.168.0.182.34564 > 142.250.67.141.443: Flags [.], ack 47, win 501, options [nop,nop,TS val 1903169481 ecr 3613899976], length 0
12:08:05.277928 IP 192.168.0.182.60034 > 142.250.192.78.443: Flags [.], ack 162, win 7327, options [nop,nop,TS val 1146210502 ecr 416783427], length 0
12:08:06.950958 ARP, Reply 192.168.0.182 is-at 04:0e:3c:1a:60:28, length 28
12:08:07.208331 IP 192.168.0.182 > 192.168.0.1: ICMP 192.168.0.182 udp port 137 unreachable, length 86
12:08:07.219993 IP 192.168.0.182 > 192.168.0.1: ICMP 192.168.0.182 udp port 137 unreachable, length 86
12:08:20.876322 IP 192.168.0.182.38464 > 192.168.0.1.53: 33614+ [1au] A? connectivity-check.ubuntu.com. (58)
12:08:20.876584 IP 192.168.0.182.54241 > 192.168.0.1.53: 24423+ [1au] AAAA? connectivity-check.ubuntu.com. (58)
^C
18 packets captured
18 packets received by filter
0 packets dropped by kernel
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006#
```

Roll no. : 53
Name: Shreya Kamath
Date: 12th September, 2023.

```
tcpdump: listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -nnvvS src 192.168.0.182 and dst port 443
tcpdump: listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:13:38.648451 IP (tos 0x0, ttl 64, id 8700, offset 0, flags [DF], proto TCP (6), length 98)
    192.168.0.182.46146 > 142.250.192.132.443: Flags [P.], cksum 0x9392 (correct), seq 1118152770:1118152816, ack 401697757, win 501, options [nop,nop,TS val 1443630945
 ecr 2073072557], length 46
12:13:38.650313 IP (tos 0x0, ttl 64, id 8701, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.182.46146 > 142.250.192.132.443: Flags [.], cksum 0xe798 (correct), seq 1118152816, ack 401697803, win 501, options [nop,nop,TS val 1443630947 ecr 2073130
561], length 0
12:13:41.997806 IP (tos 0x0, ttl 64, id 23323, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.182.41056 > 54.192.111.73.443: Flags [.], cksum 0x30e8 (correct), seq 3415550621, ack 4159023669, win 501, options [nop,nop,TS val 4105395287 ecr 23888370
24], length 0
12:13:42.223861 IP (tos 0x0, ttl 64, id 60338, offset 0, flags [DF], proto TCP (6), length 95)
    192.168.0.182.60034 > 142.250.192.78.443: Flags [P.], cksum 0xe6c0 (correct), seq 2221851728:2221851771, ack 902743322, win 7327, options [nop,nop,TS val 1146547455
 ecr 417114454], length 43
12:13:42.507644 IP (tos 0x0, ttl 64, id 23324, offset 0, flags [DF], proto TCP (6), length 495)
    192.168.0.182.41056 > 54.192.111.73.443: Flags [P.], cksum 0x4e2f (correct), seq 3415550622:3415551065, ack 4159023669, win 501, options [nop,nop,TS val 4105395797
ecr 2388847264], length 443
12:13:42.606177 IP (tos 0x0, ttl 64, id 23325, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.182.41056 > 54.192.111.73.443: Flags [.], cksum 0x0068 (correct), seq 3415551065, ack 4159024281, win 501, options [nop,nop,TS val 4105395895 ecr 23888477
76], length 0
12:13:49.746703 IP (tos 0x0, ttl 64, id 23326, offset 0, flags [DF], proto TCP (6), length 495)
    192.168.0.182.41056 > 54.192.111.73.443: Flags [P.], cksum 0x914e (correct), seq 3415551065:3415551508, ack 4159024281, win 501, options [nop,nop,TS val 4105403036
ecr 2388847776], length 443
12:13:49.845135 IP (tos 0x0, ttl 64, id 23327, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.182.41056 > 54.192.111.73.443: Flags [.], cksum 0xc3ba (correct), seq 3415551508, ack 4159024893, win 501, options [nop,nop,TS val 4105403134 ecr 23888550
15], length 0
12:13:58.867388 IP (tos 0x0, ttl 64, id 55118, offset 0, flags [DF], proto TCP (6), length 98)
    192.168.0.182.54162 > 142.250.183.142.443: Flags [P.], cksum 0x044e (correct), seq 3780532617:3780532663, ack 1856904268, win 501, options [nop,nop,TS val 426968770
 ecr 3504007057], length 46
12:13:58.913806 IP (tos 0x0, ttl 64, id 55119, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.182.54162 > 142.250.183.142.443: Flags [.], cksum 0x14c7 (correct), seq 3780532663, ack 1856904314, win 501, options [nop,nop,TS val 426968816 ecr 3504065
366], length 0
12:13:59.917760 IP (tos 0x0, ttl 64, id 23328, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.182.41056 > 54.192.111.73.443: Flags [.], cksum 0x9c62 (correct), seq 3415551507, ack 4159024893, win 501, options [nop,nop,TS val 4105413207 ecr 23888550
15], length 0
12:14:01.306581 IP (tos 0x0, ttl 64, id 55120, offset 0, flags [DF], proto TCP (6), length 425)
    192.168.0.182.54162 > 142.250.183.142.443: Flags [P.], cksum 0xeaec (correct), seq 3780532663:3780533036, ack 1856904314, win 501, options [nop,nop,TS val 426971209
 ecr 3504065366], length 373
12:14:01.306644 IP (tos 0x0, ttl 64, id 55121, offset 0, flags [DF], proto TCP (6), length 1452)
    192.168.0.182.54162 > 142.250.183.142.443: Flags [.], cksum 0x61ca (correct), seq 3780533036:3780534436, ack 1856904314, win 501, options [nop,nop,TS val 426971209
ecr 3504065366], length 1400
```

```
0412], length 0
12:14:14.029133 IP (tos 0x0, ttl 64, id 59269, offset 0, flags [DF], proto TCP (6), length 90)
    192.168.0.182.43934 > 103.102.166.224.443: Flags [P.], cksum 0x1150 (correct), seq 3777618545:3777618583, ack 3182039794, win 501, options [nop,nop,TS val 148497424
6 ecr 1808780412], length 38
12:14:16.135515 IP (tos 0x0, ttl 64, id 60351, offset 0, flags [DF], proto TCP (6), length 95)
    192.168.0.182.60034 > 142.250.192.78.443: Flags [P.], cksum 0x509e (correct), seq 2221860918:2221860961, ack 902744258, win 7327, options [nop,nop,TS val 1146581367
 ecr 417142086], length 43
12:14:20.909604 IP (tos 0x0, ttl 64, id 23332, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.182.41056 > 54.192.111.73.443: Flags [.], cksum 0xf4a8 (correct), seq 3415551950, ack 4159025505, win 501, options [nop,nop,TS val 4105434199 ecr 23888759
05], length 0
12:14:27.747550 IP (tos 0x0, ttl 64, id 60352, offset 0, flags [DF], proto TCP (6), length 95)
    192.168.0.182.60034 > 142.250.192.78.443: Flags [P.], cksum 0x9274 (correct), seq 2221860961:2221861004, ack 902744258, win 7327, options [nop,nop,TS val 1146592979
 ecr 417154301], length 43
12:14:28.080112 IP (tos 0x0, ttl 64, id 23333, offset 0, flags [DF], proto TCP (6), length 495)
    192.168.0.182.41056 > 54.192.111.73.443: Flags [P.], cksum 0xb938 (correct), seq 3415551951:3415552394, ack 4159025505, win 501, options [nop,nop,TS val 4105441370
ecr 2388886177], length 443
12:14:28.178586 IP (tos 0x0, ttl 64, id 23334, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.182.41056 > 54.192.111.73.443: Flags [.], cksum 0x8ffe (correct), seq 3415552394, ack 4159026117, win 501, options [nop,nop,TS val 4105441468 ecr 23888933
50], length 0
12:14:28.735516 IP (tos 0x0, ttl 64, id 60353, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.182.60034 > 142.250.192.78.443: Flags [.], cksum 0x7b58 (correct), seq 2221861004, ack 902744319, win 7327, options [nop,nop,TS val 1146593967 ecr 4171668
99], length 0
12:14:32.978136 IP (tos 0x0, ttl 64, id 8702, offset 0, flags [DF], proto TCP (6), length 98)
    192.168.0.182.46146 > 142.250.192.132.443: Flags [P.], cksum 0x9192 (correct), seq 1118152816:1118152862, ack 401697803, win 501, options [nop,nop,TS val 1443685276
 ecr 2073130561], length 46
12:14:32.978341 IP (tos 0x0, ttl 64, id 8703, offset 0, flags [DF], proto TCP (6), length 83)
    192.168.0.182.46146 > 142.250.192.132.443: Flags [P.], cksum 0x91ab (correct), seq 1118152862:1118152893, ack 401697803, win 501, options [nop,nop,TS val 1443685276
 ecr 2073130561], length 31
12:14:32.978358 IP (tos 0x0, ttl 64, id 8704, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.182.46146 > 142.250.192.132.443: Flags [F.], cksum 0x1311 (correct), seq 1118152893, ack 401697803, win 501, options [nop,nop,TS val 1443685276 ecr 207313
0561], length 0
12:14:32.980650 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.182.46146 > 142.250.192.132.443: Flags [.], cksum 0x3ed0 (correct), seq 1118152894, ack 401697804, win 501, options [nop,nop,TS val 1443685279 ecr 2073184
893], length 0
12:14:35.475572 IP (tos 0x0, ttl 64, id 23335, offset 0, flags [DF], proto TCP (6), length 495)
    192.168.0.182.41056 > 54.192.111.73.443: Flags [P.], cksum 0x818f (correct), seq 3415552394:3415552837, ack 4159026117, win 501, options [nop,nop,TS val 4105448766
ecr 2388893350], length 443
12:14:35.575270 IP (tos 0x0, ttl 64, id 23336, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.182.41056 > 54.192.111.73.443: Flags [.], cksum 0x5217 (correct), seq 3415552837, ack 4159026729, win 501, options [nop,nop,TS val 4105448865 ecr 23889007
45], length 0
^C
58 packets captured
58 packets received by filter
0 packets dropped by kernel
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006#
```

CONCLUSION:

Hence, I have learnt the fundamentals of Wireshark and sniffing tool tcpdump and executed commands to capture packets in different ways.