Roll No: 09
Name: Shreya Bagade
Date: 18/08/2023

LAB ASSIGNMENT NO:07

Aim: Study of packet sniffer tools Wireshark and TCPDUMP.

Lab Outcome Attained: Explore the different network reconnaissance tools to gather information about networks.

Theory:

> What is TCPDUMP and how to install it?

tcpdump is a command-line packet analyzer tool used to capture and display network packets. It's commonly used for network troubleshooting, monitoring, and security analysis. tcpdump can capture packets from various network interfaces and display their content, allowing you to inspect the data being transmitted over the network. It provides a detailed view of packet headers, payload, and other relevant information.

To install tcpdump on different operating systems:

Linux (Debian/Ubuntu): sudo apt-get install tcpdump

Linux (Red Hat/CentOS): sudo yum install tcpdump

macOS: brew install tcpdump

> Explain varous commands in tcpdump to capture different types of packets.

```
# tcpdump -n tcp
```

```
#tcpdump -n icmp
```

```
# tcpdump -n src 172.16.92.1
```

```
# tcpdump -n dst 172.16.92.1
```

```
# tcpdump -n port 80
```

```
# tcpdump port 80
```

```
# tcpdump udp and src port 53
```

observing packets within a specific port range

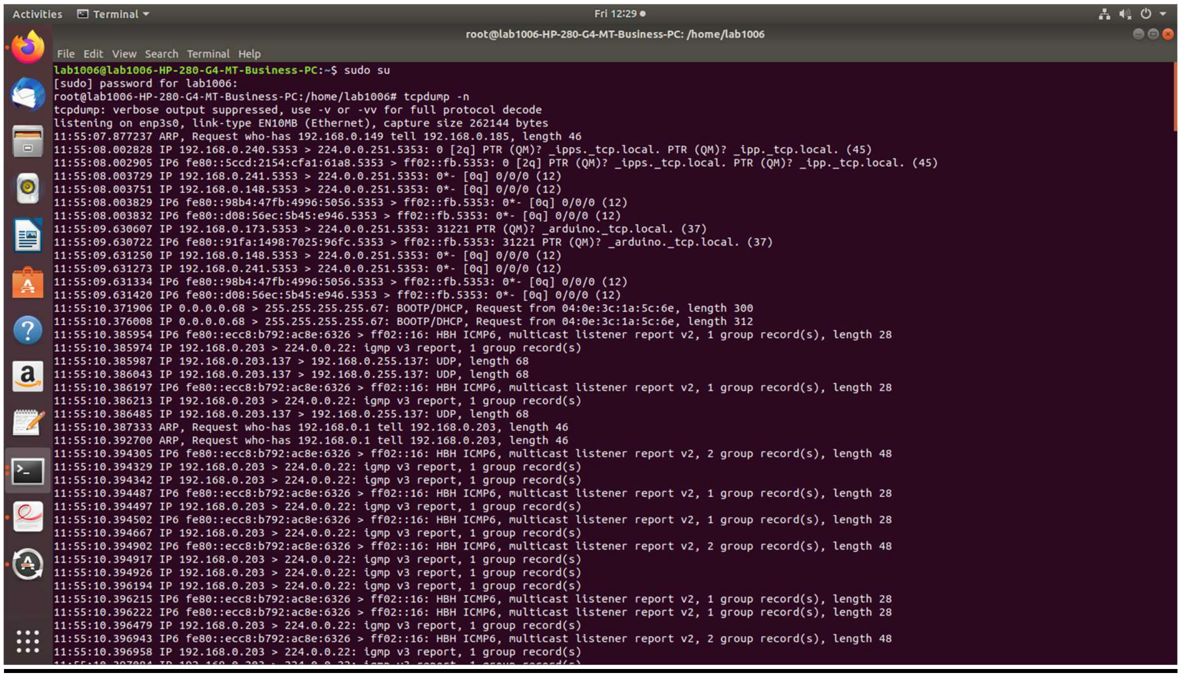
```
# tcpdump -n portrange 1-80
```

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

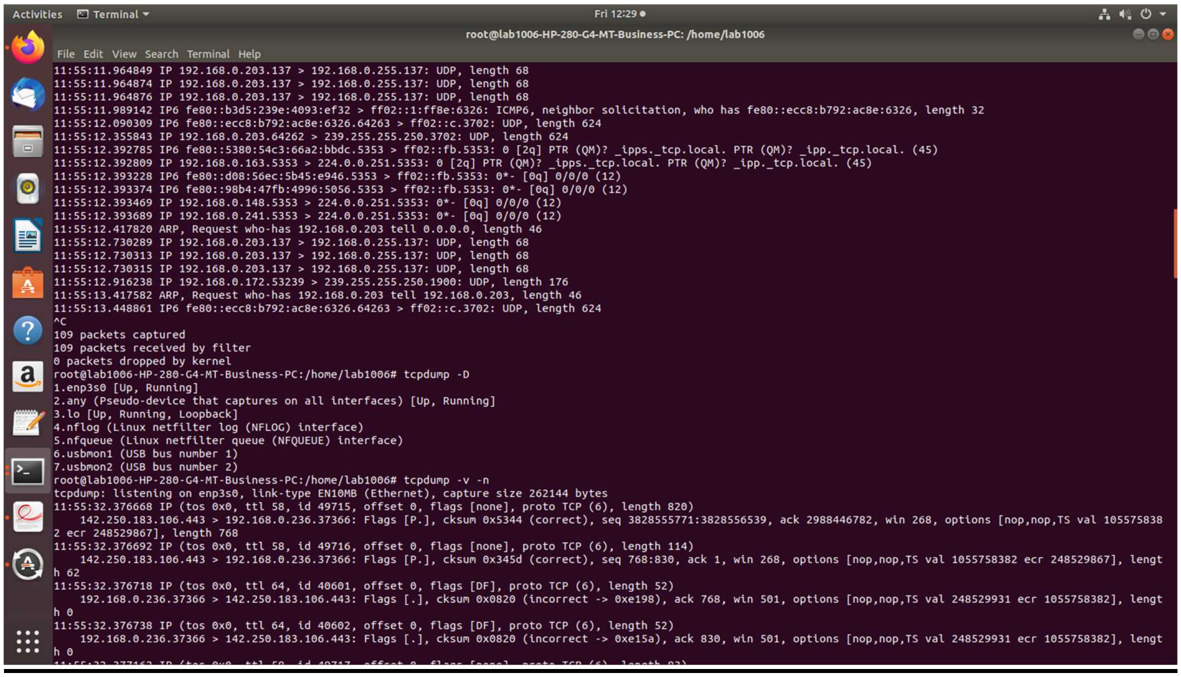
tcpdump -nnvvS src 10.5.2.3 and dst port 3389

tcpdump -nvX src net 192.168.0.0/16 and dst net 10.0.0.0/8 or 172.16.0.0/16

Output Screenshots:

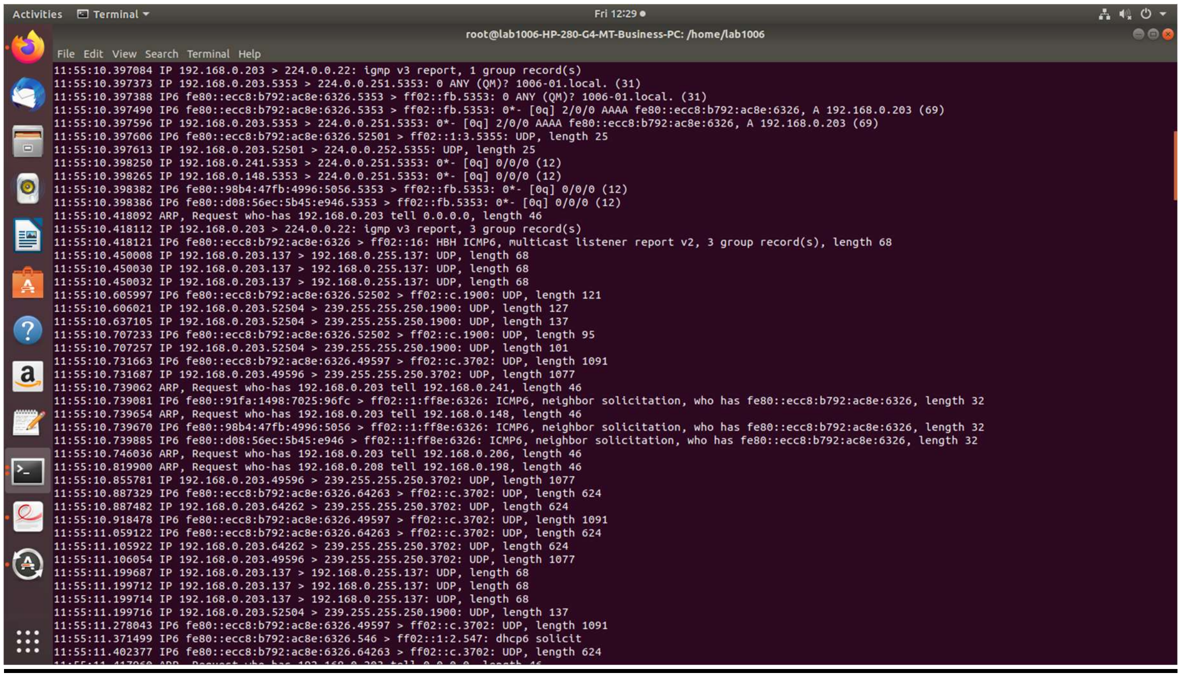

Activities
Terminal
Fri 12:29
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

```
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
11:55:07.877237 ARP, Request who-has 192.168.0.149 tell 192.168.0.185, length 46
11:55:08.002828 IP 192.168.0.240.5353 > 224.0.0.251.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
11:55:08.002905 IP6 fe80::5ccd:2154:cfa1:61a8.5353 > ff02::fb.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
11:55:08.003729 IP 192.168.0.241.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
11:55:08.003751 IP 192.168.0.148.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
11:55:08.003829 IP6 fe80::98b4:47fb:4996:5056.5353 > ff02::fb.5353: 0*- [0q] 0/0/0 (12)
11:55:08.003832 IP6 fe80::d08:56ec:5b45:e946.5353 > ff02::fb.5353: 0*- [0q] 0/0/0 (12)
11:55:09.630607 IP 192.168.0.173.5353 > 224.0.0.251.5353: 31221 PTR (QM)? _arduino._tcp.local. (37)
11:55:09.630722 IP6 fe80::91fa:1498:7025:96fc.5353 > ff02::fb.5353: 31221 PTR (QM)? _arduino._tcp.local. (37)
11:55:09.631250 IP 192.168.0.148.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
11:55:09.631273 IP 192.168.0.241.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
11:55:09.631334 IP6 fe80::98b4:47fb:4996:5056.5353 > ff02::fb.5353: 0*- [0q] 0/0/0 (12)
11:55:09.631420 IP6 fe80::d08:56ec:5b45:e946.5353 > ff02::fb.5353: 0*- [0q] 0/0/0 (12)
11:55:10.371906 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 04:0e:3c:1a:5c:6e, length 300
11:55:10.376008 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 04:0e:3c:1a:5c:6e, length 312
11:55:10.385954 IP6 fe80::ecc8:b792:ac8e:6326 > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
11:55:10.385974 IP 192.168.0.203 > 224.0.0.22: igmp v3 report, 1 group record(s)
11:55:10.385987 IP 192.168.0.203.137 > 192.168.0.255.137: UDP, length 68
11:55:10.386043 IP 192.168.0.203.137 > 192.168.0.255.137: UDP, length 68
11:55:10.386197 IP6 fe80::ecc8:b792:ac8e:6326 > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
11:55:10.386213 IP 192.168.0.203 > 224.0.0.22: igmp v3 report, 1 group record(s)
11:55:10.386485 IP 192.168.0.203.137 > 192.168.0.255.137: UDP, length 68
11:55:10.387333 ARP, Request who-has 192.168.0.1 tell 192.168.0.203, length 46
11:55:10.392700 ARP, Request who-has 192.168.0.1 tell 192.168.0.203, length 46
11:55:10.394305 IP6 fe80::ecc8:b792:ac8e:6326 > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
11:55:10.394329 IP 192.168.0.203 > 224.0.0.22: igmp v3 report, 1 group record(s)
11:55:10.394342 IP 192.168.0.203 > 224.0.0.22: igmp v3 report, 1 group record(s)
11:55:10.394487 IP6 fe80::ecc8:b792:ac8e:6326 > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
11:55:10.394497 IP 192.168.0.203 > 224.0.0.22: igmp v3 report, 1 group record(s)
11:55:10.394502 IP6 fe80::ecc8:b792:ac8e:6326 > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
11:55:10.394667 IP 192.168.0.203 > 224.0.0.22: igmp v3 report, 1 group record(s)
11:55:10.394902 IP6 fe80::ecc8:b792:ac8e:6326 > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
11:55:10.394917 IP 192.168.0.203 > 224.0.0.22: igmp v3 report, 1 group record(s)
11:55:10.394926 IP 192.168.0.203 > 224.0.0.22: igmp v3 report, 1 group record(s)
11:55:10.396194 IP 192.168.0.203 > 224.0.0.22: igmp v3 report, 1 group record(s)
11:55:10.396215 IP6 fe80::ecc8:b792:ac8e:6326 > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
11:55:10.396222 IP6 fe80::ecc8:b792:ac8e:6326 > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
11:55:10.396479 IP 192.168.0.203 > 224.0.0.22: igmp v3 report, 1 group record(s)
11:55:10.396943 IP6 fe80::ecc8:b792:ac8e:6326 > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
11:55:10.396958 IP 192.168.0.203 > 224.0.0.22: igmp v3 report, 1 group record(s)
11:55:10.397084 IP 192.168.0.203 > 224.0.0.22: igmp v3 report, 1 group record(s)
```

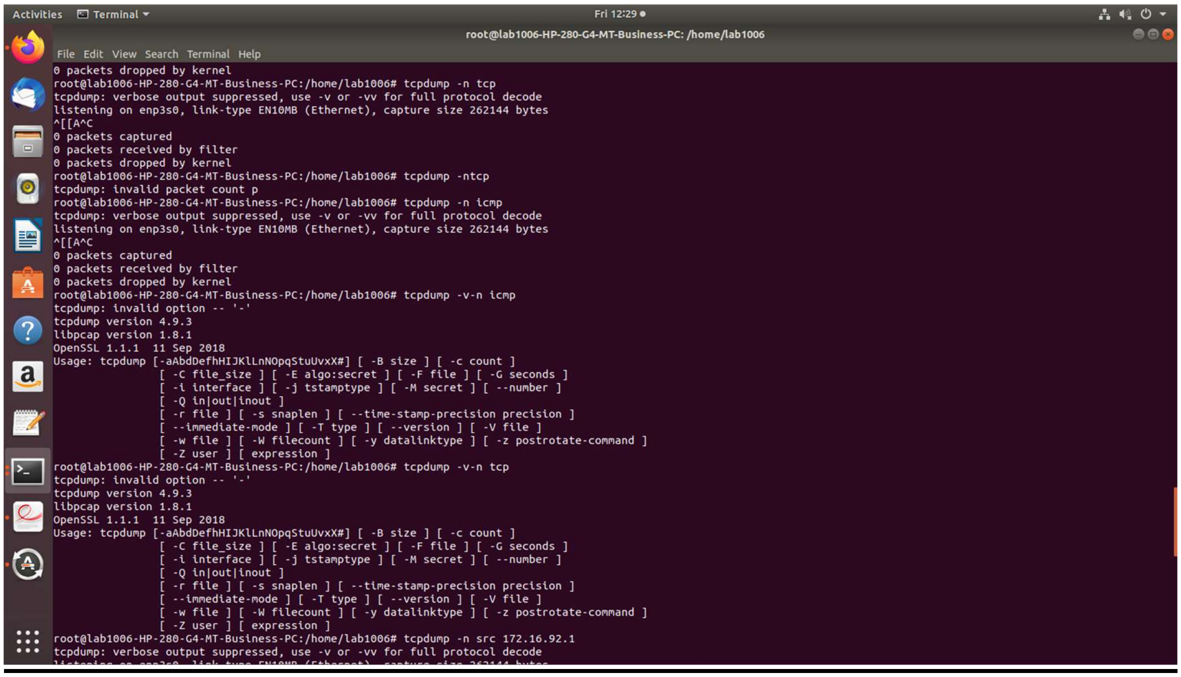

Activities
Terminal
Fri 12:29
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

```
11:55:11.964849 IP 192.168.0.203.137 > 192.168.0.255.137: UDP, length 68
11:55:11.964874 IP 192.168.0.203.137 > 192.168.0.255.137: UDP, length 68
11:55:11.964876 IP 192.168.0.203.137 > 192.168.0.255.137: UDP, length 68
11:55:11.989142 IP6 fe80::b3d5:239e:4093:ef32 > ff02::1:ff8e:6326: ICMP6, neighbor solicitation, who has fe80::ecc8:b792:ac8e:6326, length 32
11:55:12.090309 IP6 fe80::ecc8:b792:ac8e:6326.64263 > ff02::c.3702: UDP, length 624
11:55:12.355843 IP 192.168.0.203.64262 > 239.255.255.250.3702: UDP, length 624
11:55:12.392785 IP6 fe80::5380:54c3:66a2:bbdc.5353 > ff02::fb.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
11:55:12.392809 IP 192.168.0.163.5353 > 224.0.0.251.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
11:55:12.393228 IP6 fe80::d08:56ec:5b45:e946.5353 > ff02::fb.5353: 0*- [0q] 0/0/0 (12)
11:55:12.393374 IP6 fe80::98b4:47fb:4996:5056.5353 > ff02::fb.5353: 0*- [0q] 0/0/0 (12)
11:55:12.393469 IP 192.168.0.148.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
11:55:12.393689 IP 192.168.0.241.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
11:55:12.417820 ARP, Request who-has 192.168.0.203 tell 0.0.0.0, length 46
11:55:12.730289 IP 192.168.0.203.137 > 192.168.0.255.137: UDP, length 68
11:55:12.730313 IP 192.168.0.203.137 > 192.168.0.255.137: UDP, length 68
11:55:12.730315 IP 192.168.0.203.137 > 192.168.0.255.137: UDP, length 68
11:55:12.916238 IP 192.168.0.172.53239 > 239.255.255.250.1900: UDP, length 176
11:55:13.417582 ARP, Request who-has 192.168.0.203 tell 192.168.0.203, length 46
11:55:13.448861 IP6 fe80::ecc8:b792:ac8e:6326.64263 > ff02::c.3702: UDP, length 624
^C
109 packets captured
109 packets received by filter
0 packets dropped by kernel
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -D
1.enp3s0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.nflog (Linux netfilter log (NFLOG) interface)
5.nfqueue (Linux netfilter queue (NFQUEUE) interface)
6.usbmon1 (USB bus number 1)
7.usbmon2 (USB bus number 2)
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
11:55:32.376668 IP (tos 0x0, ttl 58, id 49715, offset 0, flags [none], proto TCP (6), length 820)
    142.250.183.106.443 > 192.168.0.236.37366: Flags [P.], cksum 0x5344 (correct), seq 3828555771:3828556539, ack 2988446782, win 268, options [nop,nop,TS val 105575838
2 ecr 248529867], length 768
11:55:32.376692 IP (tos 0x0, ttl 58, id 49716, offset 0, flags [none], proto TCP (6), length 114)
    142.250.183.106.443 > 192.168.0.236.37366: Flags [P.], cksum 0x345d (correct), seq 768:830, ack 1, win 268, options [nop,nop,TS val 1055758382 ecr 248529867], lengt
h 62
11:55:32.376718 IP (tos 0x0, ttl 64, id 40601, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.236.37366 > 142.250.183.106.443: Flags [.], cksum 0x0820 (incorrect -> 0xe198), ack 768, win 501, options [nop,nop,TS val 248529931 ecr 1055758382], lengt
h 0
11:55:32.376738 IP (tos 0x0, ttl 64, id 40602, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.236.37366 > 142.250.183.106.443: Flags [.], cksum 0x0820 (incorrect -> 0xe15a), ack 830, win 501, options [nop,nop,TS val 248529931 ecr 1055758382], lengt
h 0
11:55:32.377162 IP (tos 0x0, ttl 58, id 49717, offset 0, flags [none], proto TCP (6), length 83)
```

Roll No: 09
Name: Shreya Bagade
Date: 18/08/2023

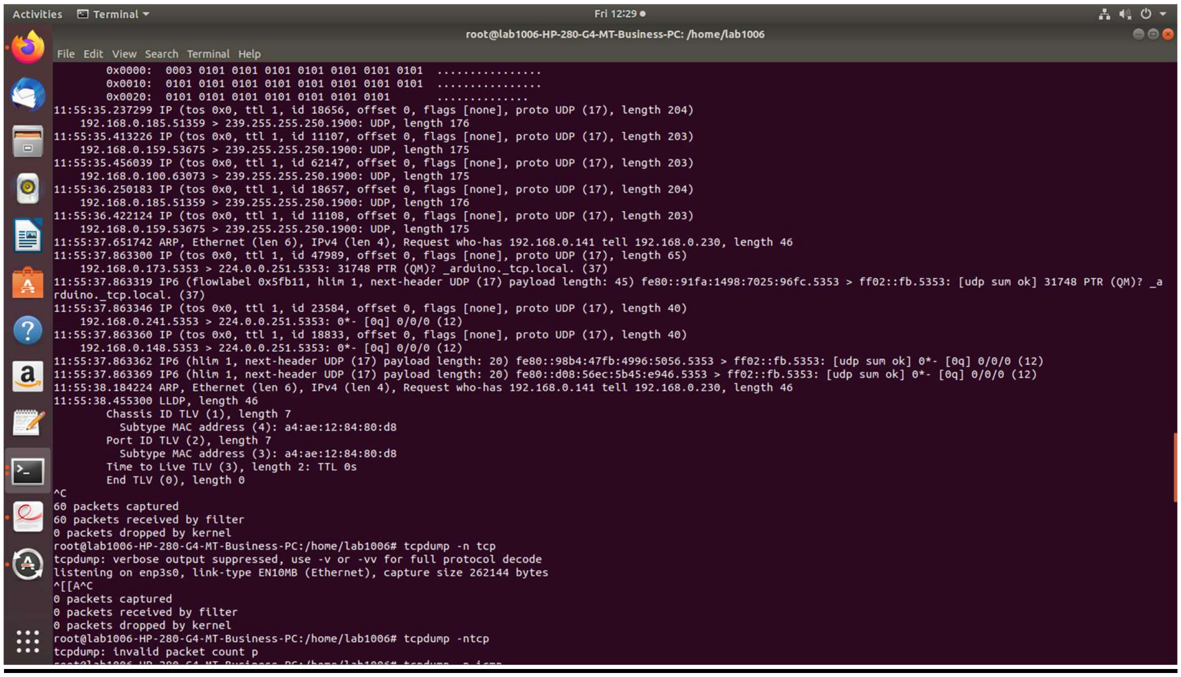

Activities
Terminal
Fri 12:29
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

```
11:55:10.397084 IP 192.168.0.203 > 224.0.0.22: igmp v3 report, 1 group record(s)
11:55:10.397373 IP 192.168.0.203.5353 > 224.0.0.251.5353: 0 ANY (QM)? 1006-01.local. (31)
11:55:10.397388 IP6 fe80::ecc8:b792:ac8e:6326.5353 > ff02::fb.5353: 0 ANY (QM)? 1006-01.local. (31)
11:55:10.397490 IP6 fe80::ecc8:b792:ac8e:6326.5353 > ff02::fb.5353: 0*- [0q] 2/0/0 AAAA fe80::ecc8:b792:ac8e:6326, A 192.168.0.203 (69)
11:55:10.397596 IP 192.168.0.203.5353 > 224.0.0.251.5353: 0*- [0q] 2/0/0 AAAA fe80::ecc8:b792:ac8e:6326, A 192.168.0.203 (69)
11:55:10.397606 IP6 fe80::ecc8:b792:ac8e:6326.52501 > ff02::1:3.5355: UDP, length 25
11:55:10.397613 IP 192.168.0.203.52501 > 224.0.0.252.5355: UDP, length 25
11:55:10.398250 IP 192.168.0.241.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
11:55:10.398265 IP 192.168.0.148.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
11:55:10.398382 IP6 fe80::98b4:47fb:4996:5056.5353 > ff02::fb.5353: 0*- [0q] 0/0/0 (12)
11:55:10.398386 IP6 fe80::d08:56ec:5b45:e946.5353 > ff02::fb.5353: 0*- [0q] 0/0/0 (12)
11:55:10.418092 ARP, Request who-has 192.168.0.203 tell 0.0.0.0, length 46
11:55:10.418112 IP 192.168.0.203 > 224.0.0.22: igmp v3 report, 3 group record(s)
11:55:10.418121 IP6 fe80::ecc8:b792:ac8e:6326 > ff02::16: HBH ICMP6, multicast listener report v2, 3 group record(s), length 68
11:55:10.450008 IP 192.168.0.203.137 > 192.168.0.255.137: UDP, length 68
11:55:10.450030 IP 192.168.0.203.137 > 192.168.0.255.137: UDP, length 68
11:55:10.450032 IP 192.168.0.203.137 > 192.168.0.255.137: UDP, length 68
11:55:10.605997 IP6 fe80::ecc8:b792:ac8e:6326.52502 > ff02::c.1900: UDP, length 121
11:55:10.606021 IP 192.168.0.203.52504 > 239.255.255.250.1900: UDP, length 127
11:55:10.637105 IP 192.168.0.203.52504 > 239.255.255.250.1900: UDP, length 137
11:55:10.707233 IP6 fe80::ecc8:b792:ac8e:6326.52502 > ff02::c.1900: UDP, length 95
11:55:10.707257 IP 192.168.0.203.52504 > 239.255.255.250.1900: UDP, length 101
11:55:10.731663 IP6 fe80::ecc8:b792:ac8e:6326.49597 > ff02::c.3702: UDP, length 1091
11:55:10.731687 IP 192.168.0.203.49596 > 239.255.255.250.3702: UDP, length 1077
11:55:10.739062 ARP, Request who-has 192.168.0.203 tell 192.168.0.241, length 46
11:55:10.739081 IP6 fe80::91fa:1498:7025:96fc > ff02::1:ff8e:6326: ICMP6, neighbor solicitation, who has fe80::ecc8:b792:ac8e:6326, length 32
11:55:10.739654 ARP, Request who-has 192.168.0.203 tell 192.168.0.148, length 46
11:55:10.739670 IP6 fe80::98b4:47fb:4996:5056 > ff02::1:ff8e:6326: ICMP6, neighbor solicitation, who has fe80::ecc8:b792:ac8e:6326, length 32
11:55:10.739885 IP6 fe80::d08:56ec:5b45:e946 > ff02::1:ff8e:6326: ICMP6, neighbor solicitation, who has fe80::ecc8:b792:ac8e:6326, length 32
11:55:10.746036 ARP, Request who-has 192.168.0.203 tell 192.168.0.206, length 46
11:55:10.819900 ARP, Request who-has 192.168.0.208 tell 192.168.0.198, length 46
11:55:10.855781 IP 192.168.0.203.49596 > 239.255.255.250.3702: UDP, length 1077
11:55:10.887329 IP6 fe80::ecc8:b792:ac8e:6326.64263 > ff02::c.3702: UDP, length 624
11:55:10.887482 IP 192.168.0.203.64262 > 239.255.255.250.3702: UDP, length 624
11:55:10.918478 IP6 fe80::ecc8:b792:ac8e:6326.49597 > ff02::c.3702: UDP, length 1091
11:55:11.059122 IP6 fe80::ecc8:b792:ac8e:6326.64263 > ff02::c.3702: UDP, length 624
11:55:11.105922 IP 192.168.0.203.64262 > 239.255.255.250.3702: UDP, length 624
11:55:11.106054 IP 192.168.0.203.49596 > 239.255.255.250.3702: UDP, length 1077
11:55:11.199687 IP 192.168.0.203.137 > 192.168.0.255.137: UDP, length 68
11:55:11.199712 IP 192.168.0.203.137 > 192.168.0.255.137: UDP, length 68
11:55:11.199714 IP 192.168.0.203.137 > 192.168.0.255.137: UDP, length 68
11:55:11.199716 IP 192.168.0.203.52504 > 239.255.255.250.1900: UDP, length 137
11:55:11.278043 IP6 fe80::ecc8:b792:ac8e:6326.49597 > ff02::c.3702: UDP, length 1091
11:55:11.371499 IP6 fe80::ecc8:b792:ac8e:6326.546 > ff02::1:2.547: dhcp6 solicit
11:55:11.402377 IP6 fe80::ecc8:b792:ac8e:6326.64263 > ff02::c.3702: UDP, length 624
11:55:11.417060 ARP, Request who-has 192.168.0.203 tell 0.0.0.0, length 46
```

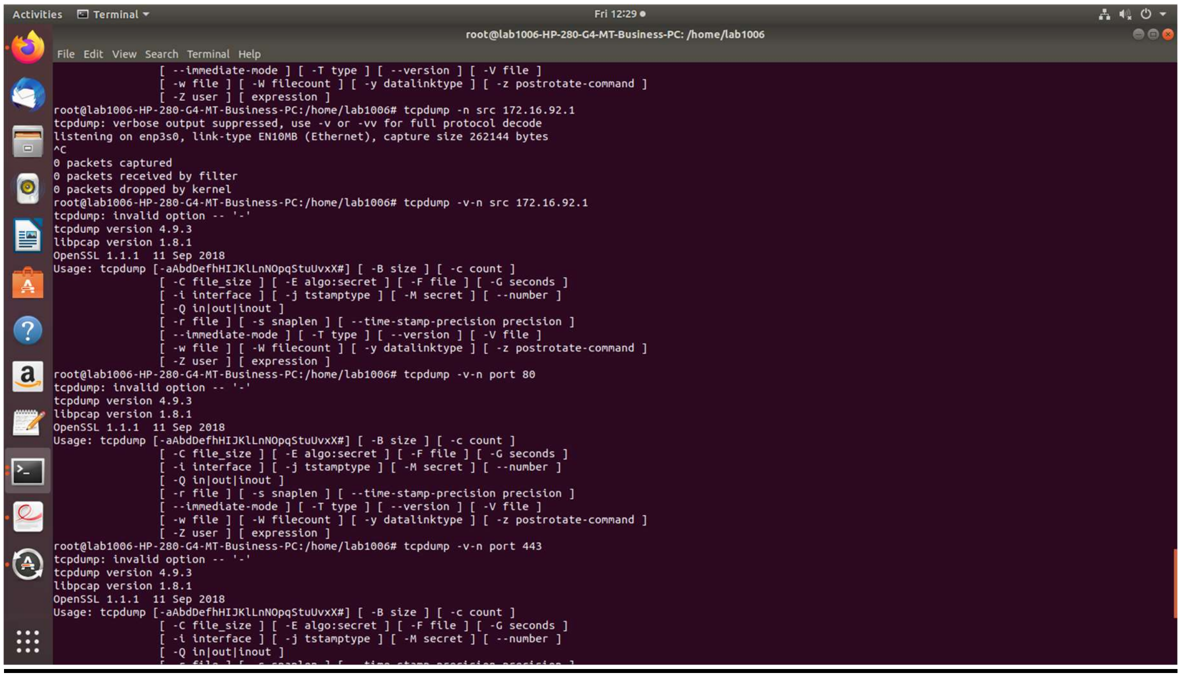

Activities
Terminal
Fri 12:29
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

```
0 packets dropped by kernel
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -n tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^[[A^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -ntcp
tcpdump: invalid packet count p
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
^[[A^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -v-n icmp
tcpdump: invalid option -- '-'
tcpdump version 4.9.3
libpcap version 1.8.1
OpenSSL 1.1.1  11 Sep 2018
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
                [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
                [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate-command ]
                [ -Z user ] [ expression ]
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -v-n tcp
tcpdump: invalid option -- '-'
tcpdump version 4.9.3
libpcap version 1.8.1
OpenSSL 1.1.1  11 Sep 2018
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
                [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
                [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate-command ]
                [ -Z user ] [ expression ]
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -n src 172.16.92.1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

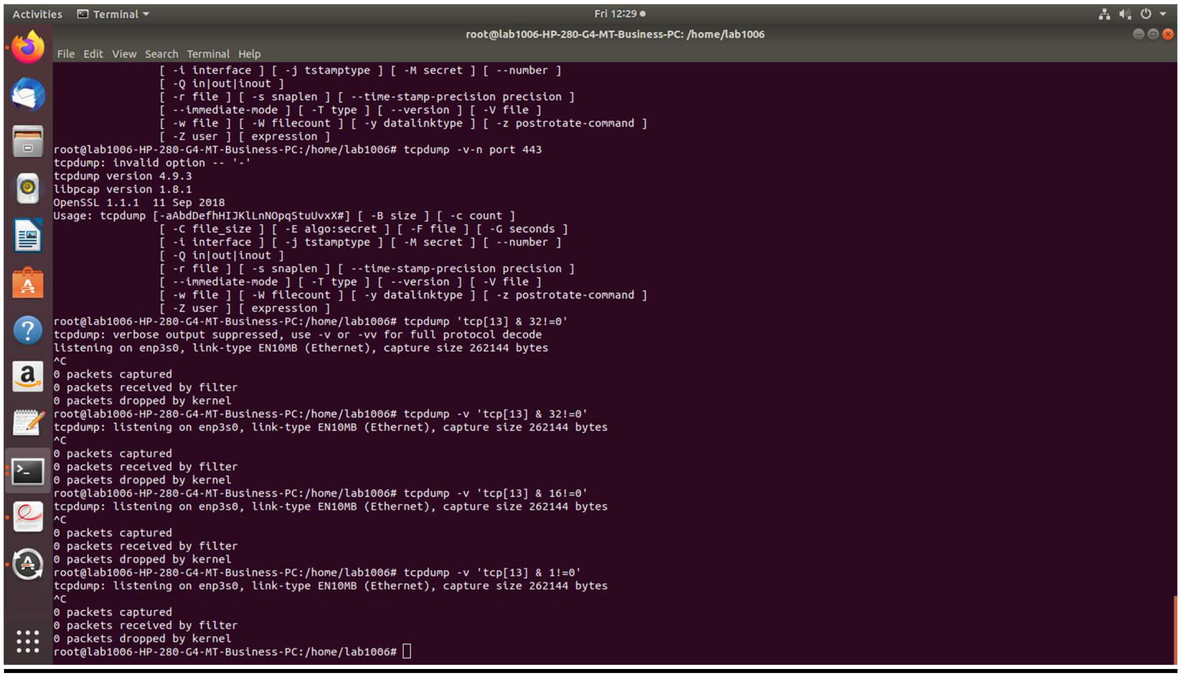
Roll No: 09
Name: Shreya Bagade
Date: 18/08/2023


Activities
Terminal
Fri 12:29
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

```
        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       ..............
11:55:35.237299 IP (tos 0x0, ttl 1, id 18656, offset 0, flags [none], proto UDP (17), length 204)
    192.168.0.185.51359 > 239.255.255.250.1900: UDP, length 176
11:55:35.413226 IP (tos 0x0, ttl 1, id 11107, offset 0, flags [none], proto UDP (17), length 203)
    192.168.0.159.53675 > 239.255.255.250.1900: UDP, length 175
11:55:35.456039 IP (tos 0x0, ttl 1, id 62147, offset 0, flags [none], proto UDP (17), length 203)
    192.168.0.100.63073 > 239.255.255.250.1900: UDP, length 175
11:55:36.250183 IP (tos 0x0, ttl 1, id 18657, offset 0, flags [none], proto UDP (17), length 204)
    192.168.0.185.51359 > 239.255.255.250.1900: UDP, length 176
11:55:36.422124 IP (tos 0x0, ttl 1, id 11108, offset 0, flags [none], proto UDP (17), length 203)
    192.168.0.159.53675 > 239.255.255.250.1900: UDP, length 175
11:55:37.651742 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.141 tell 192.168.0.230, length 46
11:55:37.863300 IP (tos 0x0, ttl 1, id 47989, offset 0, flags [none], proto UDP (17), length 65)
    192.168.0.173.5353 > 224.0.0.251.5353: 31748 PTR (QM)? _arduino._tcp.local. (37)
11:55:37.863319 IP6 (flowlabel 0x5fb11, hlim 1, next-header UDP (17) payload length: 45) fe80::91fa:1498:7025:96fc.5353 > ff02::fb.5353: [udp sum ok] 31748 PTR (QM)? _a
rduino._tcp.local. (37)
11:55:37.863346 IP (tos 0x0, ttl 1, id 23584, 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)
11:55:37.863360 IP (tos 0x0, ttl 1, id 18833, 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)
11:55:37.863362 IP6 (hlim 1, next-header UDP (17) payload length: 20) fe80::98b4:47fb:4996:5056.5353 > ff02::fb.5353: [udp sum ok] 0*- [0q] 0/0/0 (12)
11:55:37.863369 IP6 (hlim 1, next-header UDP (17) payload length: 20) fe80::d08:56ec:5b45:e946.5353 > ff02::fb.5353: [udp sum ok] 0*- [0q] 0/0/0 (12)
11:55:38.184224 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.141 tell 192.168.0.230, length 46
11:55:38.455300 LLDP, length 46
        Chassis ID TLV (1), length 7
          Subtype MAC address (4): a4:ae:12:84:80:d8
        Port ID TLV (2), length 7
          Subtype MAC address (3): a4:ae:12:84:80:d8
        Time to Live TLV (3), length 2: TTL 0s
        End TLV (0), length 0
^C
60 packets captured
60 packets received by filter
0 packets dropped by kernel
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -n tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^[[A^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -ntcp
tcpdump: invalid packet count p
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -n icmp
```


Activities
Terminal
Fri 12:29
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

```
                [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate-command ]
                [ -Z user ] [ expression ]
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -n src 172.16.92.1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -v-n src 172.16.92.1
tcpdump: invalid option -- '-'
tcpdump version 4.9.3
libpcap version 1.8.1
OpenSSL 1.1.1  11 Sep 2018
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
                [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
                [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate-command ]
                [ -Z user ] [ expression ]
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -v-n port 80
tcpdump: invalid option -- '-'
tcpdump version 4.9.3
libpcap version 1.8.1
OpenSSL 1.1.1  11 Sep 2018
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
                [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
                [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate-command ]
                [ -Z user ] [ expression ]
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -v-n port 443
tcpdump: invalid option -- '-'
tcpdump version 4.9.3
libpcap version 1.8.1
OpenSSL 1.1.1  11 Sep 2018
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
                [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
```


Activities
Terminal
Fri 12:29
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File Edit View Search Terminal Help

```
                [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
                [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
                [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate-command ]
                [ -Z user ] [ expression ]
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -v-n port 443
tcpdump: invalid option -- '-'
tcpdump version 4.9.3
libpcap version 1.8.1
OpenSSL 1.1.1  11 Sep 2018
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
                [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
                [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate-command ]
                [ -Z user ] [ expression ]
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump 'tcp[13] & 32!=0'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -v 'tcp[13] & 32!=0'
tcpdump: listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -v 'tcp[13] & 16!=0'
tcpdump: listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# tcpdump -v 'tcp[13] & 1!=0'
tcpdump: listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# 
```

Conclusion: This experiment involving the study of the packet sniffer tool tcpdump has provided valuable insights into the world of network analysis and packet capture. Through this experiment, we have gained a deeper understanding of how tcpdump can be effectively utilized to monitor and analyze network traffic. The tool's ability to capture packets on specific network interfaces and its versatility in applying filters to capture various types of packets have been demonstrated. By using tcpdump in verbose mode, we were able to extract detailed information about packet headers, payloads, and protocol specifics, enabling us to examine network communication patterns in depth.