Roll Number:- 2105048
Name:-Manav Jain
Date:- 23/08/2023

Lab Assignment No:-7

Aim:-Study of packet sniffer tools TCPDUMP.

Lab Outcome Attained :- LO3

Theory:-

What is TCPDUMP and how to install it?

Tcpdump is a command-line packet analyzer that allows you to capture and analyze network traffic in real-time. It's commonly used for troubleshooting network issues, analyzing network behavior, and diagnosing problems related to network communication. tcpdump captures packets as they travel through a network interface and provides detailed information about each packet, including source and destination addresses, protocol information, payload data, and more.

Linux (Debian/Ubuntu):

Open a terminal and run the following command to install tcpdump: sudo apt-get update sudo apt-get install tcpdump

Explain various commands in tcpdump to capture different types of packets.

tcpdump provides a wide range of commands and options to capture and analyze different types of packets. Here are some common tcpdump commands and filters to capture specific types of packets:

1. **Capture All Traffic on a Specific Interface:**

sudo tcpdump -i eth0

This captures all traffic on the "eth0" network interface.

2. **Capture Traffic to or from a Specific IP Address:**

sudo tcpdump host 192.168.1.100

This captures all traffic to or from the IP address "192.168.1.100".

3. **Capture Traffic on a Specific Port:**

sudo tcpdump port 80

This captures all traffic on port 80.

4. **Capture Traffic Using a Specific Protocol:**

sudo tcpdump icmp

This captures ICMP (ping) traffic.

5. **Capture Traffic from a Specific Source IP:**

sudo tcpdump src 192.168.1.200

This captures traffic originating from IP address "192.168.1.200".

6. **Capture Traffic to a Specific Destination IP:**

sudo tcpdump dst 192.168.1.100

This captures traffic directed to IP address "192.168.1.100".

7. **Capture Traffic on a Specific Port Using a Protocol:**

sudo tcpdump udp port 53

This captures UDP traffic on port 53 (DNS).

8. **Capture Traffic Using a Combination of Filters:**

sudo tcpdump src 192.168.1.100 and port 22

This captures traffic originating from IP address "192.168.1.100" and using port 22 (SSH).

9. Capture Traffic with Specific Packet Size:

sudo tcpdump greater 1000

This captures packets larger than 1000 bytes.

10. Capture Specific Number of Packets:

sudo tcpdump -c 10

This captures 10 packets and then exits.

11. Capture Packets Using Hexadecimal Filter:

sudo tcpdump -X 'tcp[13] & 2 != 0'

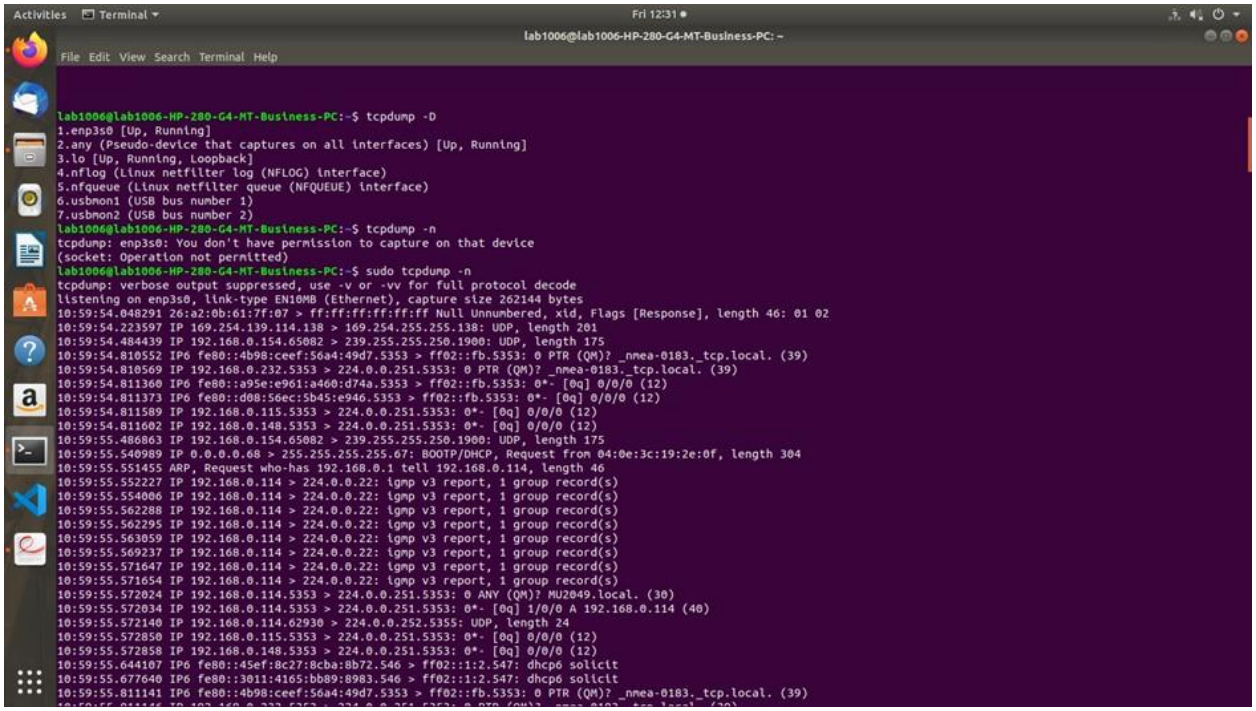
This captures only SYN packets (TCP packets with the SYN flag set).

12. Capture and Save Output to a File:

sudo tcpdump -i eth0 -w output.pcap

This captures traffic on the "eth0" interface and saves it to the "output.pcap" file.

Output Screenshot:-



```
Activities  Terminal  Fri 12:31
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File  Edit  View  Search  Terminal  Help
10:59:55.811146 IP 192.168.0.232.5353 > 224.0.0.251.5353: 0 PTR (QM)? _nmea-0183._tcp.local. (39)
10:59:55.811627 IP6 fe80::a95e:e961:a460:d74a.5353 > ff02::fb.5353: 0*- [0q] 0/0/0 (12)
10:59:55.811783 IP 192.168.0.115.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
10:59:55.811942 IP6 fe80::d08:56ec:5b45:e946.5353 > ff02::fb.5353: 0*- [0q] 0/0/0 (12)
10:59:55.812212 IP 192.168.0.148.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
^C
33 packets captured
33 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudp tcpdump -v -n

Command 'sudp' not found, did you mean:

  command 'ssdp' from snap ssdp (0.0.1)
  command 'sudo' from deb sudo
  command 'sudo' from deb sudo-ldap
  command 'sfdp' from deb graphviz
  command 'sup' from deb sup

See 'snap info <snapname>' for additional versions.

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -v -n
tcpdump: listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:01:45.107922 IP (tos 0x0, ttl 1, id 32932, offset 0, flags [none], proto UDP (17), length 203)
    192.168.0.194.65406 > 239.255.255.250.1900: UDP, length 175
11:01:45.431136 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.240 tell 192.168.0.107, length 46
11:01:45.566252 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.141 tell 192.168.0.190, length 46
11:01:45.590670 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.164 tell 192.168.0.107, length 46
11:01:45.738253 IP (tos 0x0, ttl 1, id 52371, offset 0, flags [none], proto UDP (17), length 204)
    192.168.0.190.54153 > 239.255.255.250.1900: UDP, length 176
11:01:46.086093 IP (tos 0x0, ttl 1, id 29968, offset 0, flags [none], proto UDP (17), length 203)
    192.168.0.166.65144 > 239.255.255.250.1900: UDP, length 175
11:01:46.097290 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.240 tell 192.168.0.107, length 46
11:01:46.108753 IP (tos 0x0, ttl 1, id 32933, offset 0, flags [none], proto UDP (17), length 203)
    192.168.0.194.65406 > 239.255.255.250.1900: UDP, length 175
11:01:46.524893 IP6 (hlim 1, next-header UDP (17) payload length: 103) fe80::98b4:47fb:4996:5056.546 > ff02::1:2.547: [udp sum ok] dhcp6 solicit (xid=c0f377 (elapsed-ti
me 6303) (client-ID hwaddr/time type 1 time 744492727 040e3c19288f) (IA_NA IAID:50597436 T1:0 T2:0) (Client-FQDN) (vendor-class) (option-request DNS-search-list DNS-ser
ver vendor-specific-info Client-FQDN))
11:01:46.566009 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.141 tell 192.168.0.190, length 46
11:01:47.046890 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 0101  ................
11:01:47.094578 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.240 tell 192.168.0.107, length 46
11:01:47.096305 IP (tos 0x0, ttl 1, id 29969, offset 0, flags [none], proto UDP (17), length 203)
```

```
Activities  Terminal  Fri 12:31
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File  Edit  View  Search  Terminal  Help
    192.168.0.115.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
11:06:48.559410 04:0e:3c:19:2d:d2 > 33:33:00:00:00:fb, ethertype IPv6 (0x86dd), length 74: (hlim 1, next-header UDP (17) payload length: 20) fe80::d08:56ec:5b45:e946.53
53 > ff02::fb.5353: [udp sum ok] 0*- [0q] 0/0/0 (12)
11:06:48.559669 04:0e:3c:19:2d:d2 > 01:00:5e:00:00:fb, ethertype IPv4 (0x0800), length 60: (tos 0x0, ttl 1, id 17398, 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)
11:06:48.859888 a4:ae:12:84:80:ea > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.134 tell 192.168.0.1
85, length 46
11:06:49.156505 ac:15:a2:b9:9e:29 > 01:00:5e:7f:ff:fa, ethertype IPv4 (0x0800), length 218: (tos 0x0, ttl 1, id 620, offset 0, flags [none], proto UDP (17), length 204)
    192.44.44.202.60046 > 239.255.255.250.1900: UDP, length 176
11:06:49.943390 04:0e:3c:1a:60:2f > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.141 tell 192.168.0.1
90, length 46
11:06:50.170534 ac:15:a2:b9:9e:29 > 01:00:5e:7f:ff:fa, ethertype IPv4 (0x0800), length 218: (tos 0x0, ttl 1, id 621, offset 0, flags [none], proto UDP (17), length 204)
    192.44.44.202.60046 > 239.255.255.250.1900: UDP, length 176
11:06:50.567535 04:0e:3c:1a:60:2f > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.141 tell 192.168.0.1
90, length 46
11:06:50.584752 04:0e:3c:1b:d1:42 > ac:15:a2:b9:9e:29, ethertype IPv4 (0x0800), length 105: (tos 0x0, ttl 64, id 15809, offset 0, flags [DF], proto TCP (6), length 91)
    192.168.0.213.51252 > 185.199.108.154.443: Flags [P.], cksum 0xe82c (incorrect -> 0xc33f), seq 1873020008:1873020047, ack 1011178678, win 4607, options [nop,nop,TS
val 3555857482 ecr 1680001507], length 39
11:06:50.601299 ac:15:a2:b9:9e:29 > 04:0e:3c:1b:d1:42, ethertype IPv4 (0x0800), length 66: (tos 0x34, ttl 55, id 60381, offset 0, flags [DF], proto TCP (6), length 52)
    185.199.108.154.443 > 192.168.0.213.51252: Flags [.], cksum 0xbab0 (correct), ack 39, win 284, options [nop,nop,TS val 1680060306 ecr 3555857482], length 0
11:06:50.601323 ac:15:a2:b9:9e:29 > 04:0e:3c:1b:d1:42, ethertype IPv4 (0x0800), length 105: (tos 0x34, ttl 55, id 60382, offset 0, flags [DF], proto TCP (6), length 91)
    185.199.108.154.443 > 192.168.0.213.51252: Flags [P.], cksum 0x5056 (correct), seq 1:40, ack 39, win 284, options [nop,nop,TS val 1680060306 ecr 3555857482], length
 39
11:06:50.601400 04:0e:3c:1b:d1:42 > ac:15:a2:b9:9e:29, ethertype IPv4 (0x0800), length 66: (tos 0x0, ttl 64, id 15810, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.213.51252 > 185.199.108.154.443: Flags [.], cksum 0xe805 (incorrect -> 0xa995), ack 40, win 4607, options [nop,nop,TS val 3555857499 ecr 1680060306], leng
th 0
11:06:50.675239 ac:15:a2:b9:9e:29 > 01:00:5e:7f:ff:fa, ethertype IPv4 (0x0800), length 428: (tos 0x0, ttl 2, id 37639, offset 0, flags [DF], proto UDP (17), length 414)
    192.168.0.1.60033 > 239.255.255.250.1900: UDP, length 386
11:06:50.675463 ac:15:a2:b9:9e:29 > 01:00:5e:7f:ff:fa, ethertype IPv4 (0x0800), length 437: (tos 0x0, ttl 2, id 37640, offset 0, flags [DF], proto UDP (17), length 423)
    192.168.0.1.60033 > 239.255.255.250.1900: UDP, length 395
11:06:50.675567 ac:15:a2:b9:9e:29 > 01:00:5e:7f:ff:fa, ethertype IPv4 (0x0800), length 500: (tos 0x0, ttl 2, id 37641, offset 0, flags [DF], proto UDP (17), length 486)
    192.168.0.1.60033 > 239.255.255.250.1900: UDP, length 458
11:06:50.675836 ac:15:a2:b9:9e:29 > 01:00:5e:7f:ff:fa, ethertype IPv4 (0x0800), length 496: (tos 0x0, ttl 2, id 37642, offset 0, flags [DF], proto UDP (17), length 482)
    192.168.0.1.60033 > 239.255.255.250.1900: UDP, length 454
11:06:50.675997 ac:15:a2:b9:9e:29 > 01:00:5e:7f:ff:fa, ethertype IPv4 (0x0800), length 476: (tos 0x0, ttl 2, id 37643, offset 0, flags [DF], proto UDP (17), length 462)
    192.168.0.1.60033 > 239.255.255.250.1900: UDP, length 434
11:06:50.676187 ac:15:a2:b9:9e:29 > 01:00:5e:7f:ff:fa, ethertype IPv4 (0x0800), length 508: (tos 0x0, ttl 2, id 37644, offset 0, flags [DF], proto UDP (17), length 494)
    192.168.0.1.60033 > 239.255.255.250.1900: UDP, length 466
11:06:50.676299 ac:15:a2:b9:9e:29 > 01:00:5e:7f:ff:fa, ethertype IPv4 (0x0800), length 490: (tos 0x0, ttl 2, id 37645, offset 0, flags [DF], proto UDP (17), length 476)
    192.168.0.1.60033 > 239.255.255.250.1900: UDP, length 448
11:06:50.676493 ac:15:a2:b9:9e:29 > 01:00:5e:7f:ff:fa, ethertype IPv4 (0x0800), length 492: (tos 0x0, ttl 2, id 37646, offset 0, flags [DF], proto UDP (17), length 478)
    192.168.0.1.60033 > 239.255.255.250.1900: UDP, length 450
11:06:50.676669 ac:15:a2:b9:9e:29 > 01:00:5e:7f:ff:fa, ethertype IPv4 (0x0800), length 492: (tos 0x0, ttl 2, id 37647, offset 0, flags [DF], proto UDP (17), length 478)
    192.168.0.1.60033 > 239.255.255.250.1900: UDP, length 450
11:06:50.696063 04:0e:3c:1a:5c:1f > 33:33:00:00:00:fb, ethertype IPv6 (0x86dd), length 102: (flowlabel 0x061d2, hlim 255, next-header UDP (17) payload length: 48) fe80:
```

```
Activities  Terminal  Fri 12:31
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File  Edit  View  Search  Terminal  Help
    192.168.0.213.38292 > 152.195.38.76.80: Flags [.], cksum 0x80b3 (incorrect -> 0xbd9d), ack 1018572014, win 501, options [nop,nop,TS val 1531651325 ecr 4184076819],
length 0
11:06:51.426290 ac:15:a2:b9:9e:29 > 04:0e:3c:1b:d1:42, ethertype IPv4 (0x0800), length 66: (tos 0x0, ttl 58, id 61638, offset 0, flags [none], proto TCP (6), length 52)
    152.195.38.76.80 > 192.168.0.213.38292: Flags [.], cksum 0xeb9a (correct), ack 1, win 135, options [nop,nop,TS val 4184087059 ecr 1531629677], length 0
11:06:51.567263 04:0e:3c:1a:60:2f > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.141 tell 192.168.0.1
90, length 46
11:06:51.691627 a4:ae:12:84:80:ea > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.134 tell 192.168.0.1
85, length 46
11:06:51.831366 ac:15:a2:b9:9e:29 > 04:0e:3c:1b:d1:42, ethertype IPv4 (0x0800), length 91: (tos 0x34, ttl 46, id 7178, offset 0, flags [DF], proto TCP (6), length 77)
    140.82.112.25.443 > 192.168.0.213.37992: Flags [P.], cksum 0xdcb4 (correct), seq 3601914876:3601914901, ack 4276782204, win 77, options [nop,nop,TS val 3554971416 e
cr 3093326561], length 25
11:06:51.831411 04:0e:3c:1b:d1:42 > ac:15:a2:b9:9e:29, ethertype IPv4 (0x0800), length 66: (tos 0x0, ttl 64, id 46494, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.213.37992 > 140.82.112.25.443: Flags [.], cksum 0xbe0f (incorrect -> 0xc80d), ack 25, win 501, options [nop,nop,TS val 3093366561 ecr 3554971416], length
0
11:06:51.831638 04:0e:3c:1b:d1:42 > ac:15:a2:b9:9e:29, ethertype IPv4 (0x0800), length 95: (tos 0x0, ttl 64, id 46495, offset 0, flags [DF], proto TCP (6), length 81)
    192.168.0.213.37992 > 140.82.112.25.443: Flags [P.], cksum 0xbe2c (incorrect -> 0x50e9), seq 1:30, ack 25, win 501, options [nop,nop,TS val 3093366561 ecr 355497141
6], length 29
^C
43 packets captured
43 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo 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
11:08:51.831101 IP 140.82.112.25.443 > 192.168.0.213.37992: Flags [P.], seq 3601914926:3601914951, ack 4276782262, win 77, options [nop,nop,TS val 3555091411 ecr 309342
6561], length 25
11:08:51.831308 IP 192.168.0.213.37992 > 140.82.112.25.443: Flags [P.], seq 1:30, ack 25, win 501, options [nop,nop,TS val 3093486561 ecr 3555091411], length 29
11:08:52.119414 IP 140.82.112.25.443 > 192.168.0.213.37992: Flags [.], ack 30, win 77, options [nop,nop,TS val 3555091700 ecr 3093486561], length 0
11:08:57.438567 IP 192.168.0.213.39510 > 140.82.114.22.443: Flags [.], seq 2871837009:2871837045, ack 1471998315, win 501, options [nop,nop,TS val 3554701205 ecr 242720
383], length 36
11:08:57.438586 IP 192.168.0.213.39510 > 140.82.114.22.443: Flags [P.], seq 36:39, ack 1, win 501, options [nop,nop,TS val 3554701205 ecr 242720383], length 3
11:08:57.438660 IP 192.168.0.213.51198 > 185.199.108.154.443: Flags [.], seq 4064335366:4064335402, ack 768197512, win 11904, options [nop,nop,TS val 3555984336 ecr 130
5689667], length 36
11:08:57.438664 IP 192.168.0.213.51198 > 185.199.108.154.443: Flags [P.], seq 36:39, ack 1, win 11904, options [nop,nop,TS val 3555984336 ecr 1305689667], length 3
11:08:57.439030 IP 192.168.0.213.51198 > 185.199.108.154.443: Flags [P.], seq 39:63, ack 1, win 11904, options [nop,nop,TS val 3555984337 ecr 1305689667], length 24
11:08:57.439057 IP 192.168.0.213.51198 > 185.199.108.154.443: Flags [F.], seq 63, ack 1, win 11904, options [nop,nop,TS val 3555984337 ecr 1305689667], length 0
11:08:57.439775 IP 192.168.0.213.39510 > 140.82.114.22.443: Flags [P.], seq 39:63, ack 1, win 501, options [nop,nop,TS val 3554701206 ecr 242720383], length 24
11:08:57.439800 IP 192.168.0.213.39510 > 140.82.114.22.443: Flags [F.], seq 63, ack 1, win 501, options [nop,nop,TS val 3554701206 ecr 242720383], length 0
11:08:57.455029 IP 185.199.108.154.443 > 192.168.0.213.51198: Flags [.], ack 0, win 377, options [nop,nop,TS val 1305742675 ecr 3555931344,nop,nop,sack 1 {36:39}], leng
th 0
11:08:57.455044 IP 185.199.108.154.443 > 192.168.0.213.51198: Flags [.], ack 39, win 377, options [nop,nop,TS val 1305742675 ecr 3555984336], length 0
11:08:57.457877 IP 185.199.108.154.443 > 192.168.0.213.51198: Flags [.], ack 63, win 377, options [nop,nop,TS val 1305742675 ecr 3555984337], length 0
11:08:57.457892 IP 185.199.108.154.443 > 192.168.0.213.51198: Flags [P.], seq 1:25, ack 63, win 377, options [nop,nop,TS val 1305742675 ecr 3555984337], length 24
11:08:57.457894 IP 185.199.108.154.443 > 192.168.0.213.51198: Flags [F.], seq 25, ack 63, win 377, options [nop,nop,TS val 1305742675 ecr 3555984337], length 0
11:08:57.457958 IP 192.168.0.213.51198 > 185.199.108.154.443: Flags [R], seq 4064335429, win 0, length 0
```

```
Activities  Terminal  Fri 12:31
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File  Edit  View  Search  Terminal  Help
25 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo 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
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -n tcp src 192.168.0.181
tcpdump: 'tcp' modifier applied to host
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -n src 192.168.0.181 icmp
tcpdump: syntax error in filter expression: syntax error
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -n icmp src 192.168.0.181 icmp
tcpdump: 'icmp' modifier applied to host
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo 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
11:23:14.623598 IP 192.168.0.213 > 103.246.224.160: ICMP echo request, id 13898, seq 10, length 64
11:23:14.624221 IP 103.246.224.160 > 192.168.0.213: ICMP echo reply, id 13898, seq 10, length 64
11:23:15.647605 IP 192.168.0.213 > 103.246.224.160: ICMP echo request, id 13898, seq 11, length 64
11:23:15.648227 IP 103.246.224.160 > 192.168.0.213: ICMP echo reply, id 13898, seq 11, length 64
11:23:16.671565 IP 192.168.0.213 > 103.246.224.160: ICMP echo request, id 13898, seq 12, length 64
11:23:16.672192 IP 103.246.224.160 > 192.168.0.213: ICMP echo reply, id 13898, seq 12, length 64
11:23:17.695594 IP 192.168.0.213 > 103.246.224.160: ICMP echo request, id 13898, seq 13, length 64
11:23:17.696161 IP 103.246.224.160 > 192.168.0.213: ICMP echo reply, id 13898, seq 13, length 64
11:23:18.719632 IP 192.168.0.213 > 103.246.224.160: ICMP echo request, id 13898, seq 14, length 64
11:23:18.720145 IP 103.246.224.160 > 192.168.0.213: ICMP echo reply, id 13898, seq 14, length 64
^C
10 packets captured
10 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcp port 80
sudo: tcp: command not found
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:28:38.285039 IP lab1006-HP-280-G4-MT-Business-PC.49306 > 32.121.122.34.bc.googleusercontent.com.http: Flags [S], seq 3903811227, win 64240, options [mss 1460,sackOK,
TS val 3444133253 ecr 0,nop,wscale 7], length 0
11:28:39.295561 IP lab1006-HP-280-G4-MT-Business-PC.49306 > 32.121.122.34.bc.googleusercontent.com.http: Flags [S], seq 3903811227, win 64240, options [mss 1460,sackOK,
TS val 3444134263 ecr 0,nop,wscale 7], length 0
11:28:39.538360 IP 32.121.122.34.bc.googleusercontent.com.http > lab1006-HP-280-G4-MT-Business-PC.49306: Flags [S.], seq 1089476767, ack 3903811228, win 64768, options
[mss 1420,sackOK,TS val 1089564564 ecr 3444134263,nop,wscale 7], length 0
11:28:39.538421 IP lab1006-HP-280-G4-MT-Business-PC.49306 > 32.121.122.34.bc.googleusercontent.com.http: Flags [.], ack 1, win 502, options [nop,nop,TS val 3444134506 e
cr 1089564564], length 0
```

```
Activities  Terminal  Fri 12:31
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File  Edit  View  Search  Terminal  Help
11:28:39.941579 IP 32.121.122.34.bc.googleusercontent.com.http > lab1006-HP-280-G4-MT-Business-PC.49306: Flags [F.], seq 149, ack 88, win 506, options [nop,nop,TS val 1
089565016 ecr 3444134506], length 0
11:28:39.941608 IP lab1006-HP-280-G4-MT-Business-PC.49306 > 32.121.122.34.bc.googleusercontent.com.http: Flags [.], ack 150, win 501, options [nop,nop,TS val 3444134909
 ecr 1089565016], length 0
11:28:40.183386 IP 32.121.122.34.bc.googleusercontent.com.http > lab1006-HP-280-G4-MT-Business-PC.49306: Flags [.], ack 89, win 506, options [nop,nop,TS val 1089565258
ecr 3444134908], length 0
^C
12 packets captured
12 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump udp and src port 53
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:33:37.241511 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.57215: 10986 9/3/1 A 34.122.121.32, A 35.224.170.84, A 185.125.190.18, A 35.232.111.17, A 91.189.9
1.48, A 185.125.190.49, A 185.125.190.17, A 91.189.91.49, A 185.125.190.48 (266)
11:33:37.241594 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.32907: 3486 6/3/1 AAAA 2001:67c:1562::23, AAAA 2620:2d:4000:1::23, AAAA 2620:2d:4000:1::2b, AAAA 2
620:2d:4000:1::22, AAAA 2001:67c:1562::24, AAAA 2620:2d:4000:1::2a (290)
11:34:04.686194 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.53528: 54238 4/4/1 A 108.158.61.90, A 108.158.61.4, A 108.158.61.10, A 108.158.61.13 (258)
11:34:04.709453 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.59252: 37086 8/4/1 AAAA 2600:9000:237b:c200:1a:5235:f980:93a1, AAAA 2600:9000:237b:c000:1a:5235:f9
80:93a1, AAAA 2600:9000:237b:400:1a:5235:f980:93a1, AAAA 2600:9000:237b:d400:1a:5235:f980:93a1, AAAA 2600:9000:237b:7800:1a:5235:f980:93a1, AAAA 2600:9000:237b:7e00:1a:
5235:f980:93a1, AAAA 2600:9000:237b:dc00:1a:5235:f980:93a1, AAAA 2600:9000:237b:2800:1a:5235:f980:93a1 (418)
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump portrange 1-80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:35:13.653873 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 04:0e:3c:1a:5c:74 (oui Unknown), length 300
11:35:17.801654 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 04:0e:3c:1a:5c:74 (oui Unknown), length 300
11:35:22.173999 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 04:0e:3c:1a:5c:74 (oui Unknown), length 300
11:35:30.078393 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 04:0e:3c:1a:5c:74 (oui Unknown), length 300
11:35:38.922635 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 1c:6f:65:ae:98:2a (oui Unknown), length 300
11:35:41.918550 IP lab1006-HP-280-G4-MT-Business-PC.36586 > _gateway.domain: 53847+ [1au] A? encrypted-tbn0.gstatic.com. (55)
11:35:41.918818 IP lab1006-HP-280-G4-MT-Business-PC.35381 > _gateway.domain: 12276+ [1au] AAAA? encrypted-tbn0.gstatic.com. (55)
11:35:41.919849 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.36586: 53847 1/0/1 A 142.250.183.78 (71)
11:35:41.938280 IP lab1006-HP-280-G4-MT-Business-PC.56668 > _gateway.domain: 933+ [1au] A? www.google.com. (43)
11:35:41.938421 IP lab1006-HP-280-G4-MT-Business-PC.59077 > _gateway.domain: 26727+ [1au] AAAA? www.google.com. (43)
11:35:41.939510 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.56668: 933 1/0/1 A 172.217.27.196 (59)
11:35:41.939601 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.59077: 26727 1/0/1 AAAA 2404:6800:4009:800::2004 (71)
11:35:41.980589 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.35381: 12276 1/0/1 AAAA 2404:6800:4009:822::200e (83)
11:35:42.677951 IP lab1006-HP-280-G4-MT-Business-PC.37545 > _gateway.domain: 56141+ [1au] A? www.gstatic.com. (44)
11:35:42.678020 IP lab1006-HP-280-G4-MT-Business-PC.41726 > _gateway.domain: 30891+ [1au] AAAA? www.gstatic.com. (44)
11:35:42.679208 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.41726: 30891 1/0/1 AAAA 2404:6800:4009:82b::2003 (72)
11:35:42.679329 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.37545: 56141 1/0/1 A 142.250.192.131 (60)
```

```
Activities  Terminal  Fri 12:31
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File  Edit  View  Search  Terminal  Help
11:35:42.744434 IP lab1006-HP-280-G4-MT-Business-PC.55375 > _gateway.domain: 35292+ [1au] A? apis.google.com. (44)
11:35:42.744508 IP lab1006-HP-280-G4-MT-Business-PC.47736 > _gateway.domain: 45730+ [1au] AAAA? apis.google.com. (44)
11:35:42.745662 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.55375: 35292 2/0/1 CNAME plus.l.google.com., A 142.251.42.78 (81)
11:35:42.745668 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.47736: 45730 2/0/1 CNAME plus.l.google.com., AAAA 2404:6800:4009:831::200e (93)
11:35:42.845172 IP lab1006-HP-280-G4-MT-Business-PC.55210 > _gateway.domain: 48143+ [1au] A? adservice.google.com. (49)
11:35:42.845258 IP lab1006-HP-280-G4-MT-Business-PC.51043 > _gateway.domain: 27592+ [1au] AAAA? adservice.google.com. (49)
11:35:42.846395 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.55210: 48143 1/0/1 A 142.250.192.98 (65)
11:35:42.846733 IP lab1006-HP-280-G4-MT-Business-PC.39669 > _gateway.domain: 31162+ [1au] A? safebrowsing.googleapis.com. (56)
11:35:42.846788 IP lab1006-HP-280-G4-MT-Business-PC.48992 > _gateway.domain: 63325+ [1au] AAAA? safebrowsing.googleapis.com. (56)
11:35:42.847885 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.48992: 63325 1/0/1 AAAA 2404:6800:4009:823::200a (84)
11:35:42.847898 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.39669: 31162 1/0/1 A 142.250.183.106 (72)
11:35:42.850258 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.51043: 27592 1/0/1 AAAA 2404:6800:4009:820::2002 (77)
11:35:43.014836 IP lab1006-HP-280-G4-MT-Business-PC.43491 > _gateway.domain: 41945+ [1au] A? adservice.google.co.in. (51)
11:35:43.014910 IP lab1006-HP-280-G4-MT-Business-PC.35711 > _gateway.domain: 33071+ [1au] AAAA? adservice.google.co.in. (51)
11:35:43.015190 IP lab1006-HP-280-G4-MT-Business-PC.54633 > _gateway.domain: 59138+ [1au] A? googleads.g.doubleclick.net. (56)
11:35:43.015251 IP lab1006-HP-280-G4-MT-Business-PC.34413 > _gateway.domain: 1087+ [1au] AAAA? googleads.g.doubleclick.net. (56)
11:35:43.016017 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.43491: 41945 2/0/1 CNAME pagead46.l.doubleclick.net., A 142.250.192.34 (107)
11:35:43.016055 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.35711: 33071 2/0/1 CNAME pagead46.l.doubleclick.net., AAAA 2404:6800:4009:823::2002 (119)
11:35:43.016261 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.54633: 59138 1/0/1 A 142.250.199.130 (72)
11:35:43.039586 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.34413: 1087 1/0/1 AAAA 2404:6800:4009:82c::2002 (84)
11:35:45.136757 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 04:0e:3c:1a:5c:74 (oui Unknown), length 300
^C
38 packets captured
38 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump port 80 -w capture_1
tcpdump: listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C86 packets captured
86 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -nnvvS src 10.5.2.3 and dst port 3389
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
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -nnvvS src 103.246.224.160 and dst port 3389
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
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ tcpdump 'tcp[13] & 32!=0'
tcpdump: enp3s0: You don't have permission to capture on that device
(socket: Operation not permitted)
```

```
Activities  Terminal  Fri 12:31
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File  Edit  View  Search  Terminal  Help
12:04:44.335645 IP ip98.ip-51-75-86.eu.https > lab1006-HP-280-G4-MT-Business-PC.42950: Flags [R], seq 3863433480, win 0, length 0
12:04:44.335649 IP ip98.ip-51-75-86.eu.https > lab1006-HP-280-G4-MT-Business-PC.42950: Flags [R], seq 3863433480, win 0, length 0
12:04:44.335649 IP ip98.ip-51-75-86.eu.https > lab1006-HP-280-G4-MT-Business-PC.42950: Flags [R], seq 3863433480, win 0, length 0
12:04:55.146342 IP 39.12.213.35.bc.googleusercontent.com.https > lab1006-HP-280-G4-MT-Business-PC.48000: Flags [R], seq 585098989, win 0, length 0
12:04:55.146361 IP 39.12.213.35.bc.googleusercontent.com.https > lab1006-HP-280-G4-MT-Business-PC.48000: Flags [R], seq 585098989, win 0, length 0
^C
5 packets captured
5 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump 'tcp[13] & 1!=0'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:05:20.015253 IP 39.12.213.35.bc.googleusercontent.com.https > lab1006-HP-280-G4-MT-Business-PC.48012: Flags [F.], seq 2629149024, ack 1929302308, win 501, options [n
op,nop,TS val 2466317305 ecr 2922664599], length 0
12:05:20.015507 IP lab1006-HP-280-G4-MT-Business-PC.48012 > 39.12.213.35.bc.googleusercontent.com.https: Flags [F.], seq 32, ack 1, win 501, options [nop,nop,TS val 292
2729599 ecr 2466317305], length 0
12:05:21.308781 IP lab1006-HP-280-G4-MT-Business-PC.43518 > bom12s13-in-f10.1e100.net.https: Flags [F.], seq 2428652434, ack 1126368455, win 501, options [nop,nop,TS va
l 2874683512 ecr 3493271097], length 0
12:05:21.310519 IP bom12s13-in-f10.1e100.net.https > lab1006-HP-280-G4-MT-Business-PC.43518: Flags [F.], seq 1, ack 0, win 267, options [nop,nop,TS val 3493271099 ecr 2
874683512], length 0
12:05:31.935100 IP lab1006-HP-280-G4-MT-Business-PC.34760 > bom07s36-in-f2.1e100.net.https: Flags [F.], seq 1180428611, ack 3813265531, win 501, options [nop,nop,TS val
 41552518 ecr 1543554862], length 0
12:05:31.937062 IP bom07s36-in-f2.1e100.net.https > lab1006-HP-280-G4-MT-Business-PC.34760: Flags [F.], seq 1, ack 0, win 265, options [nop,nop,TS val 1543554864 ecr 41
552518], length 0
12:05:36.868948 IP lab1006-HP-280-G4-MT-Business-PC.50560 > 103.226.190.44.https: Flags [F.], seq 1711529759, ack 2298162122, win 501, options [nop,nop,TS val 319482289
2 ecr 583854437], length 0
12:05:36.871338 IP 103.226.190.44.https > lab1006-HP-280-G4-MT-Business-PC.50560: Flags [F.], seq 1, ack 0, win 261, options [nop,nop,TS val 583859434 ecr 3194822892],
length 0
12:05:43.871629 IP lab1006-HP-280-G4-MT-Business-PC.44260 > ec2-44-215-138-223.compute-1.amazonaws.com.https: Flags [F.], seq 3141369856, ack 2220810018, win 501, optio
ns [nop,nop,TS val 1678878368 ecr 2067633469], length 0
12:05:44.060653 IP ec2-44-215-138-223.compute-1.amazonaws.com.https > lab1006-HP-280-G4-MT-Business-PC.44260: Flags [F.], seq 1, ack 0, win 479, options [nop,nop,TS val
 2067636189 ecr 1678878368], length 0
12:05:45.873434 IP lab1006-HP-280-G4-MT-Business-PC.43688 > 52.46.151.131.https: Flags [F.], seq 400986082, ack 208373217, win 501, length 0
12:05:46.068962 IP 52.46.151.131.https > lab1006-HP-280-G4-MT-Business-PC.43688: Flags [F.], seq 1, ack 0, win 942, length 0
^C
12 packets captured
12 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump 'tcp[tcpflags] == tcp-rst'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:09:45.018984 IP lab1006-HP-280-G4-MT-Business-PC.48656 > 102.115.120.34.bc.googleusercontent.com.https: Flags [R], seq 2984745258, win 0, length 0
12:09:45.019042 IP lab1006-HP-280-G4-MT-Business-PC.48656 > 102.115.120.34.bc.googleusercontent.com.https: Flags [R], seq 2984745258, win 0, length 0
12:09:51.570479 IP lab1006-HP-280-G4-MT-Business-PC.36552 > 104.17.25.14.https: Flags [R], seq 1050894372, win 0, length 0
12:09:51.578512 IP lab1006-HP-280-G4-MT-Business-PC.36532 > 104.17.25.14.https: Flags [R], seq 1460208463, win 0, length 0
```

```
Activities  Terminal  Fri 12:31
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File  Edit  View  Search  Terminal  Help
12 packets captured
12 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump 'tcp[tcpflags] == tcp-rst'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:09:45.018984 IP lab1006-HP-280-G4-MT-Business-PC.48656 > 102.115.120.34.bc.googleusercontent.com.https: Flags [R], seq 2984745258, win 0, length 0
12:09:45.019042 IP lab1006-HP-280-G4-MT-Business-PC.48656 > 102.115.120.34.bc.googleusercontent.com.https: Flags [R], seq 2984745258, win 0, length 0
12:09:51.570479 IP lab1006-HP-280-G4-MT-Business-PC.36552 > 104.17.25.14.https: Flags [R], seq 1050894372, win 0, length 0
12:09:51.578512 IP lab1006-HP-280-G4-MT-Business-PC.36532 > 104.17.25.14.https: Flags [R], seq 1460208463, win 0, length 0
12:09:51.581245 IP lab1006-HP-280-G4-MT-Business-PC.36532 > 104.17.25.14.https: Flags [R], seq 1460208487, win 0, length 0
12:09:51.581249 IP lab1006-HP-280-G4-MT-Business-PC.36532 > 104.17.25.14.https: Flags [R], seq 1460208488, win 0, length 0
12:09:52.167861 IP lab1006-HP-280-G4-MT-Business-PC.56434 > bom07s32-in-f3.1e100.net.https: Flags [R], seq 3656444749, win 0, length 0
12:09:52.167868 IP lab1006-HP-280-G4-MT-Business-PC.56444 > bom07s32-in-f3.1e100.net.https: Flags [R], seq 2520567994, win 0, length 0
12:09:52.997559 IP lab1006-HP-280-G4-MT-Business-PC.50482 > bom07s36-in-f6.1e100.net.https: Flags [R], seq 207038670, win 0, length 0
12:09:52.997636 IP lab1006-HP-280-G4-MT-Business-PC.50482 > bom07s36-in-f6.1e100.net.https: Flags [R], seq 207038670, win 0, length 0
12:09:52.997648 IP lab1006-HP-280-G4-MT-Business-PC.50482 > bom07s36-in-f6.1e100.net.https: Flags [R], seq 207038670, win 0, length 0
12:09:52.997649 IP lab1006-HP-280-G4-MT-Business-PC.50482 > bom07s36-in-f6.1e100.net.https: Flags [R], seq 207038670, win 0, length 0
12:09:58.330850 IP lab1006-HP-280-G4-MT-Business-PC.41382 > venuepool.venuepool.com.https: Flags [R], seq 2568885250, win 0, length 0
12:09:58.330930 IP lab1006-HP-280-G4-MT-Business-PC.41382 > venuepool.venuepool.com.https: Flags [R], seq 2568885250, win 0, length 0
12:09:58.331079 IP lab1006-HP-280-G4-MT-Business-PC.41382 > venuepool.venuepool.com.https: Flags [R], seq 2568885250, win 0, length 0
12:09:58.331146 IP lab1006-HP-280-G4-MT-Business-PC.41382 > venuepool.venuepool.com.https: Flags [R], seq 2568885250, win 0, length 0
12:09:58.331651 IP lab1006-HP-280-G4-MT-Business-PC.41382 > venuepool.venuepool.com.https: Flags [R], seq 2568885250, win 0, length 0
12:09:58.331663 IP lab1006-HP-280-G4-MT-Business-PC.41382 > venuepool.venuepool.com.https: Flags [R], seq 2568885250, win 0, length 0
12:09:58.331763 IP lab1006-HP-280-G4-MT-Business-PC.41382 > venuepool.venuepool.com.https: Flags [R], seq 2568885250, win 0, length 0
12:09:58.518067 IP lab1006-HP-280-G4-MT-Business-PC.41370 > venuepool.venuepool.com.https: Flags [R], seq 2400063489, win 0, length 0
12:09:58.518141 IP lab1006-HP-280-G4-MT-Business-PC.41370 > venuepool.venuepool.com.https: Flags [R], seq 2400063489, win 0, length 0
12:09:58.518147 IP lab1006-HP-280-G4-MT-Business-PC.41370 > venuepool.venuepool.com.https: Flags [R], seq 2400063489, win 0, length 0
12:09:58.518164 IP lab1006-HP-280-G4-MT-Business-PC.41370 > venuepool.venuepool.com.https: Flags [R], seq 2400063489, win 0, length 0
12:10:11.001618 IP lab1006-HP-280-G4-MT-Business-PC.60294 > 151.101.153.229.https: Flags [R], seq 3683966171, win 0, length 0
12:10:11.001840 IP lab1006-HP-280-G4-MT-Business-PC.60294 > 151.101.153.229.https: Flags [R], seq 3683966195, win 0, length 0
12:10:11.001890 IP lab1006-HP-280-G4-MT-Business-PC.60294 > 151.101.153.229.https: Flags [R], seq 3683966195, win 0, length 0
12:10:11.001903 IP lab1006-HP-280-G4-MT-Business-PC.60294 > 151.101.153.229.https: Flags [R], seq 3683966195, win 0, length 0
12:10:11.002174 IP lab1006-HP-280-G4-MT-Business-PC.60294 > 151.101.153.229.https: Flags [R], seq 3683966196, win 0, length 0
12:10:11.390956 IP lab1006-HP-280-G4-MT-Business-PC.55150 > bom07s32-in-f3.1e100.net.https: Flags [R], seq 1738671314, win 0, length 0
12:10:11.391016 IP lab1006-HP-280-G4-MT-Business-PC.55150 > bom07s32-in-f3.1e100.net.https: Flags [R], seq 1738671314, win 0, length 0
12:10:33.454979 IP lab1006-HP-280-G4-MT-Business-PC.55754 > bom12s13-in-f22.1e100.net.https: Flags [R], seq 3496861439, win 0, length 0
12:10:33.455808 IP lab1006-HP-280-G4-MT-Business-PC.55754 > bom12s13-in-f22.1e100.net.https: Flags [R], seq 3496861463, win 0, length 0
12:10:33.455809 IP lab1006-HP-280-G4-MT-Business-PC.55754 > bom12s13-in-f22.1e100.net.https: Flags [R], seq 3496861464, win 0, length 0
12:10:38.236441 IP lab1006-HP-280-G4-MT-Business-PC.40492 > 151.101.153.229.https: Flags [R], seq 2267406728, win 0, length 0
12:10:38.236517 IP lab1006-HP-280-G4-MT-Business-PC.40492 > 151.101.153.229.https: Flags [R], seq 2267406728, win 0, length 0
12:10:38.236519 IP lab1006-HP-280-G4-MT-Business-PC.40492 > 151.101.153.229.https: Flags [R], seq 2267406729, win 0, length 0
12:10:40.533314 IP lab1006-HP-280-G4-MT-Business-PC.60308 > 151.101.153.229.https: Flags [R], seq 2608403810, win 0, length 0
12:10:40.533465 IP lab1006-HP-280-G4-MT-Business-PC.60308 > 151.101.153.229.https: Flags [R], seq 2608403810, win 0, length 0
12:10:40.534225 IP lab1006-HP-280-G4-MT-Business-PC.60308 > 151.101.153.229.https: Flags [R], seq 2608403811, win 0, length 0
```

Conclusion:-

Learnt about how TCPDump can be used in practical life and how can it be used to capture , dissect , interpret network packets , offering various insights about network behavior , troubleshooting and security assessment . Also explored various commands related to TCPDump