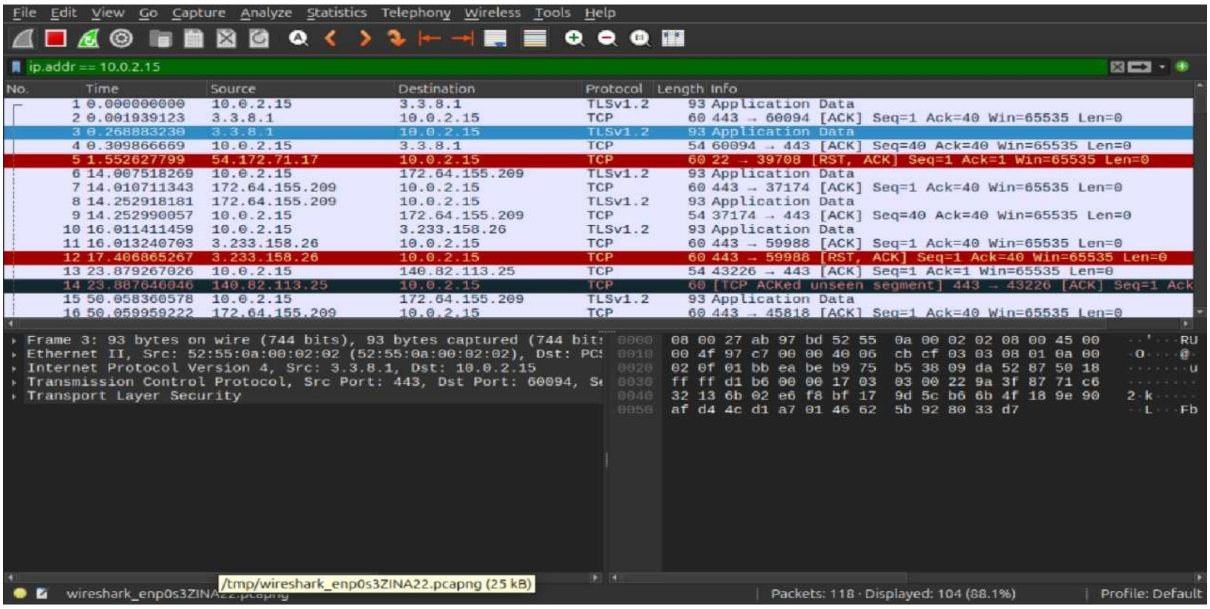
LINUX NETWORKING MODULE 1 AND 2 ASSESSMENT SOLUTIONS

-BY SAKTHI KUMAR S

3. Explore with Wireshark/TCP-dump/cisco packet tracer tools and learn about packets filters.

WIRESHARK:

1) Packet tracing with IP address


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.0.2.15

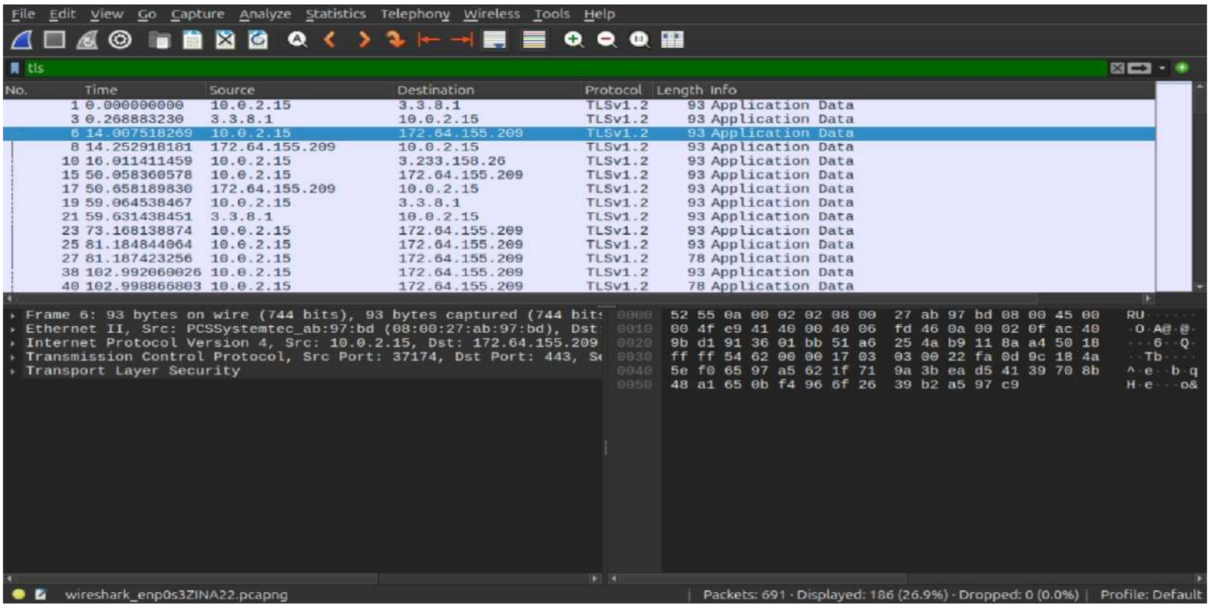
```
No.    Time          Source           Destination      Protocol  Length Info
     1 0.000000000   10.0.2.15        3.3.8.1          TLSv1.2      93 Application Data
     2 0.001939123   3.3.8.1          10.0.2.15        TCP          60 443 → 60094 [ACK] Seq=1 Ack=40 Win=65535 Len=0
     3 0.268883230   3.3.8.1          10.0.2.15        TLSv1.2      93 Application Data
     4 0.309866669   10.0.2.15        3.3.8.1          TCP          54 60094 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0
     5 1.552627799   54.172.71.17     10.0.2.15        TCP          60 22 → 39708 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
     6 14.007518269  10.0.2.15        172.64.155.209   TLSv1.2      93 Application Data
     7 14.010711343  172.64.155.209   10.0.2.15        TCP          60 443 → 37174 [ACK] Seq=1 Ack=40 Win=65535 Len=0
     8 14.252918181  172.64.155.209   10.0.2.15        TLSv1.2      93 Application Data
     9 14.252990057  10.0.2.15        172.64.155.209   TCP          54 37174 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0
    10 16.011411459  10.0.2.15        3.233.158.26     TLSv1.2      93 Application Data
    11 16.013240703  3.233.158.26     10.0.2.15        TCP          60 443 → 59988 [ACK] Seq=1 Ack=40 Win=65535 Len=0
    12 17.406865267  3.233.158.26     10.0.2.15        TCP          60 443 → 59988 [RST, ACK] Seq=1 Ack=40 Win=65535 Len=0
    13 23.879267026  10.0.2.15        140.82.113.25    TCP          54 43226 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
    14 23.887646046  140.82.113.25    10.0.2.15        TCP          60 [TCP ACKed unseen segment] 443 → 43226 [ACK] Seq=1 Ack
    15 50.058360578  10.0.2.15        172.64.155.209   TLSv1.2      93 Application Data
    16 50.059959222  172.64.155.209   10.0.2.15        TCP          60 443 → 45818 [ACK] Seq=1 Ack=40 Win=65535 Len=0
```

```
▸ Frame 3: 93 bytes on wire (744 bits), 93 bytes captured (744 bit:
▸ Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PC:
▸ Internet Protocol Version 4, Src: 3.3.8.1, Dst: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 60094, S
▸ Transport Layer Security
```

```
0000  08 00 27 ab 97 bd 52 55  0a 00 02 02 08 00 45 00   ··'···RU
0010  00 4f 97 c7 00 00 40 06  cb cf 03 03 08 01 0a 00   ·O····@·
0020  02 0f 01 bb ea be b9 75  b5 38 09 da 52 87 50 18   ·······u
0030  ff ff d1 b6 00 00 17 03  03 00 22 9a 3f 87 71 c6   ········
0040  32 13 6b 02 e6 f8 bf 17  9d 5c b6 6b 4f 18 9e 90   2·k·····
0050  af d4 4c d1 a7 01 46 62  5b 92 80 33 d7            ··L···Fb
```

wireshark_enp0s3ZINA22.pcapng | /tmp/wireshark_enp0s3ZINA22.pcapng (25 kB) | Packets: 118 · Displayed: 104 (88.1%) | Profile: Default

2) Packet Tracing with protocol names


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tls

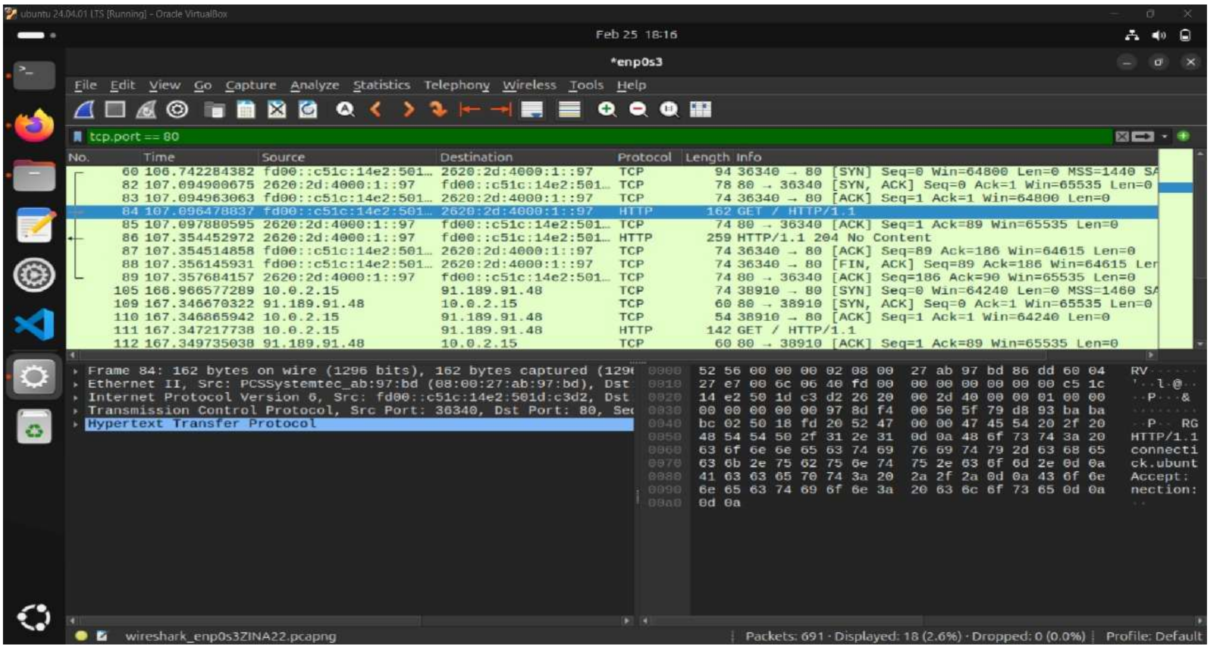
```
No.    Time          Source           Destination      Protocol  Length Info
     1 0.000000000   10.0.2.15        3.3.8.1          TLSv1.2      93 Application Data
     3 0.268883230   3.3.8.1          10.0.2.15        TLSv1.2      93 Application Data
     6 14.007518269  10.0.2.15        172.64.155.209   TLSv1.2      93 Application Data
     8 14.252918181  172.64.155.209   10.0.2.15        TLSv1.2      93 Application Data
    10 16.011411459  10.0.2.15        3.233.158.26     TLSv1.2      93 Application Data
    15 50.058360578  10.0.2.15        172.64.155.209   TLSv1.2      93 Application Data
    17 50.658189830  172.64.155.209   10.0.2.15        TLSv1.2      93 Application Data
    19 59.064538467  10.0.2.15        3.3.8.1          TLSv1.2      93 Application Data
    21 59.631438451  3.3.8.1          10.0.2.15        TLSv1.2      93 Application Data
    23 73.168138874  10.0.2.15        172.64.155.209   TLSv1.2      93 Application Data
    25 81.184844064  10.0.2.15        172.64.155.209   TLSv1.2      93 Application Data
    27 81.187423256  10.0.2.15        172.64.155.209   TLSv1.2      78 Application Data
    38 102.992060026 10.0.2.15        172.64.155.209   TLSv1.2      93 Application Data
    40 102.998866803 10.0.2.15        172.64.155.209   TLSv1.2      78 Application Data
```

```
▸ Frame 6: 93 bytes on wire (744 bits), 93 bytes captured (744 bit:
▸ Ethernet II, Src: PCSSystemtec_ab:97:bd (08:00:27:ab:97:bd), Dst
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.64.155.209
▸ Transmission Control Protocol, Src Port: 37174, Dst Port: 443, S
▸ Transport Layer Security
```

```
0000  52 55 0a 00 02 02 08 00  27 ab 97 bd 08 00 45 00   RU······
0010  00 4f e9 41 40 00 40 06  fd 46 0a 00 02 0f ac 40   ·O·A@·@·
0020  9b d1 91 36 01 bb 51 a6  25 4a b9 11 8a a4 50 18   ···6··Q·
0030  ff ff 54 62 00 00 17 03  03 00 22 fa 0d 9c 18 4a   ··Tb····
0040  5e f0 65 97 a5 62 1f 71  9a 3b ea d5 41 39 70 8b   ^·e··b·q
0050  48 a1 65 0b f4 96 6f 26  39 b2 a5 97 c9            H·e···o&
```

wireshark_enp0s3ZINA22.pcapng | Packets: 691 · Displayed: 186 (26.9%) · Dropped: 0 (0.0%) | Profile: Default

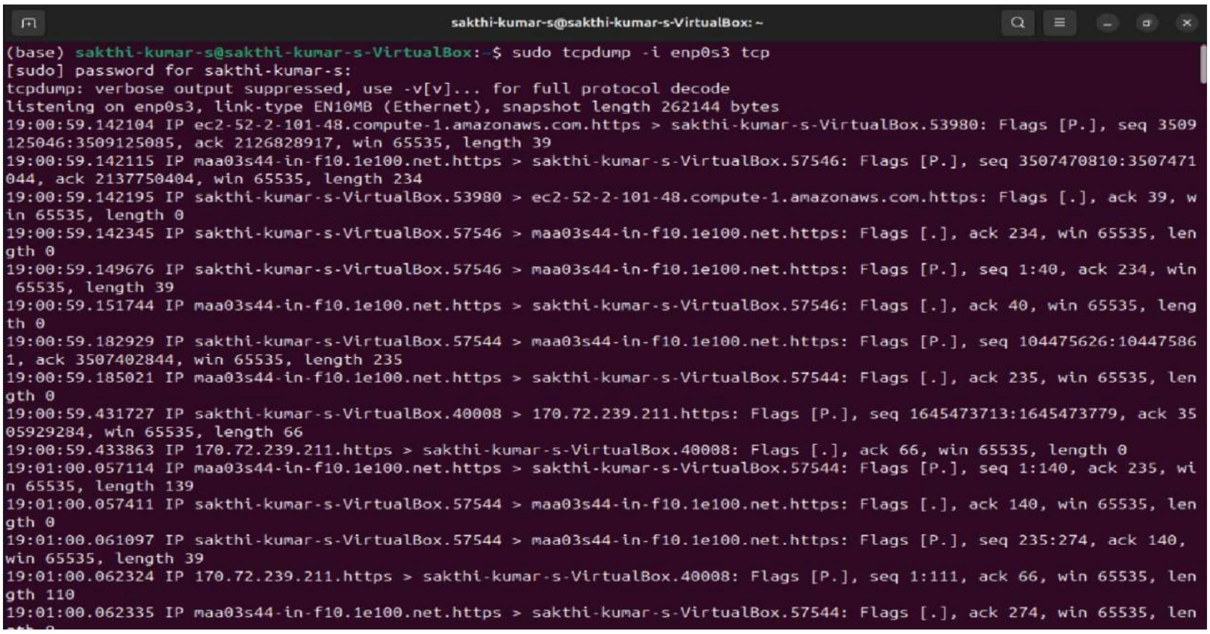
3) Packet Tracing with Port Numbers


ubuntu 24.04.01 LTS [Running] - Oracle VirtualBox
Feb 25 18:16
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.port == 80

No.  Time             Source                   Destination             Protocol Length Info
  60 106.742284382 fd00::c51c:14e2:501… 2620:2d:4000:1::97    TCP        94 36340 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SA
  82 107.094900675 2620:2d:4000:1::97   fd00::c51c:14e2:501…  TCP        78 80 → 36340 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
  83 107.094963063 fd00::c51c:14e2:501… 2620:2d:4000:1::97    TCP        74 36340 → 80 [ACK] Seq=1 Ack=1 Win=64800 Len=0
  84 107.096478837 fd00::c51c:14e2:501… 2620:2d:4000:1::97    HTTP      162 GET / HTTP/1.1
  85 107.097880595 2620:2d:4000:1::97   fd00::c51c:14e2:501…  TCP        74 80 → 36340 [ACK] Seq=1 Ack=89 Win=65535 Len=0
  86 107.354452972 2620:2d:4000:1::97   fd00::c51c:14e2:501…  HTTP      259 HTTP/1.1 204 No Content
  87 107.354514858 fd00::c51c:14e2:501… 2620:2d:4000:1::97    TCP        74 36340 → 80 [ACK] Seq=89 Ack=186 Win=64615 Len=0
  88 107.356145931 fd00::c51c:14e2:501… 2620:2d:4000:1::97    TCP        74 36340 → 80 [FIN, ACK] Seq=89 Ack=186 Win=64615 Ler
  89 107.357684157 2620:2d:4000:1::97   fd00::c51c:14e2:501…  TCP        74 80 → 36340 [ACK] Seq=186 Ack=90 Win=65535 Len=0
 105 166.966577289 10.0.2.15            91.189.91.48          TCP        74 38910 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
 109 167.346670322 91.189.91.48         10.0.2.15             TCP        60 80 → 38910 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
 110 167.346865942 10.0.2.15            91.189.91.48          TCP        54 38910 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
 111 167.347217738 10.0.2.15            91.189.91.48          HTTP      142 GET / HTTP/1.1
 112 167.349735038 91.189.91.48         10.0.2.15             TCP        60 80 → 38910 [ACK] Seq=1 Ack=89 Win=65535 Len=0

› Frame 84: 162 bytes on wire (1296 bits), 162 bytes captured (129(
› Ethernet II, Src: PCSSystemtec_ab:97:bd (08:00:27:ab:97:bd), Dst
› Internet Protocol Version 6, Src: fd00::c51c:14e2:501d:c3d2, Dst
› Transmission Control Protocol, Src Port: 36340, Dst Port: 80, Sec
› Hypertext Transfer Protocol

0000  52 56 00 00 00 02 08 00  27 ab 97 bd 86 dd 60 04   RV······
0010  27 e7 00 6c 06 40 fd 00  00 00 00 00 00 00 c5 1c   '··l·@··
0020  14 e2 50 1d c3 d2 26 20  00 2d 40 00 00 01 00 00   ··P···&
0030  00 00 00 00 00 97 8d f4  00 50 5f 79 d8 93 ba ba   ········
0040  bc 02 50 18 fd 20 52 47  00 00 47 45 54 20 2f 20   ··P·· RG
0050  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1
0060  63 6f 6e 6e 65 63 74 69  76 69 74 79 2d 63 68 65   connecti
0070  63 6b 2e 75 62 75 6e 74  75 2e 63 6f 6d 2e 0d 0a   ck.ubunt
0080  41 63 63 65 70 74 3a 20  2a 2f 2a 0d 0a 43 6f 6e   Accept:
0090  6e 65 63 74 69 6f 6e 3a  20 63 6c 6f 73 65 0d 0a   nection:
00a0  0d 0a                                              ··

wireshark_enp0s3ZINA22.pcapng    Packets: 691 · Displayed: 18 (2.6%) · Dropped: 0 (0.0%)    Profile: Default
```

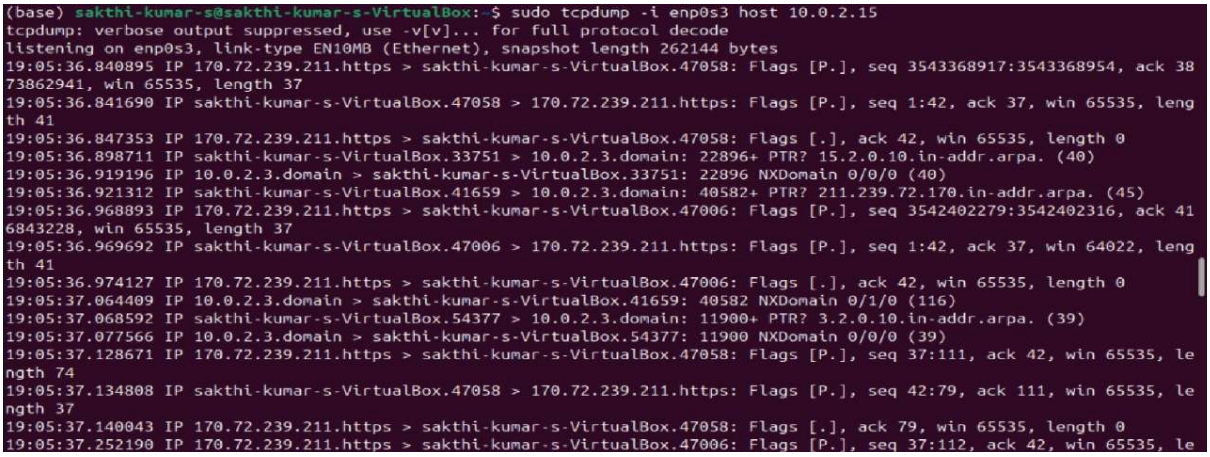
TCPDUMP:

1) Capture Packets on a Specific Interface



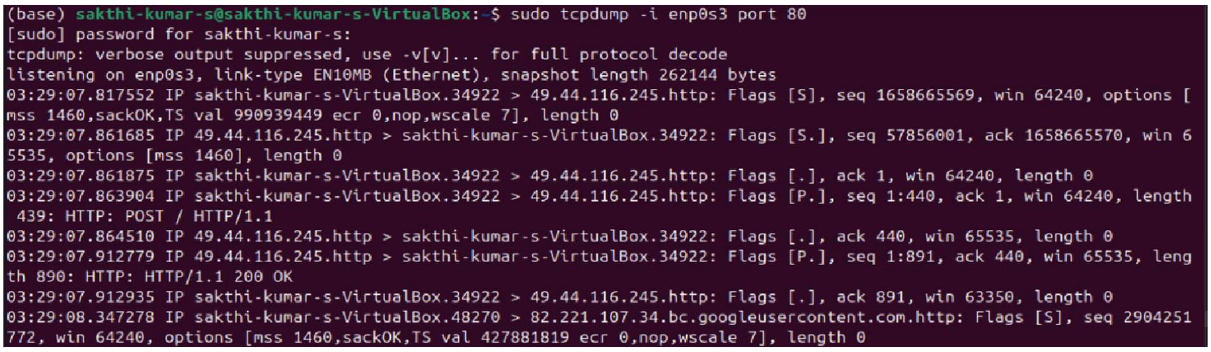
```
(base) sakthi-kumar-s@sakthi-kumar-s-VirtualBox:~$ sudo tcpdump -i enp0s3 tcp
[sudo] password for sakthi-kumar-s:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:00:59.142104 IP ec2-52-2-101-48.compute-1.amazonaws.com.https > sakthi-kumar-s-VirtualBox.53980: Flags [P.], seq 3509
125046:3509125085, ack 2126828917, win 65535, length 39
19:00:59.142115 IP maa03s44-in-f10.1e100.net.https > sakthi-kumar-s-VirtualBox.57546: Flags [P.], seq 3507470810:3507471
044, ack 2137750404, win 65535, length 234
19:00:59.142195 IP sakthi-kumar-s-VirtualBox.53980 > ec2-52-2-101-48.compute-1.amazonaws.com.https: Flags [.], ack 39, w
in 65535, length 0
19:00:59.142345 IP sakthi-kumar-s-VirtualBox.57546 > maa03s44-in-f10.1e100.net.https: Flags [.], ack 234, win 65535, len
gth 0
19:00:59.149676 IP sakthi-kumar-s-VirtualBox.57546 > maa03s44-in-f10.1e100.net.https: Flags [P.], seq 1:40, ack 234, win
 65535, length 39
19:00:59.151744 IP maa03s44-in-f10.1e100.net.https > sakthi-kumar-s-VirtualBox.57546: Flags [.], ack 40, win 65535, leng
th 0
19:00:59.182929 IP sakthi-kumar-s-VirtualBox.57544 > maa03s44-in-f10.1e100.net.https: Flags [P.], seq 104475626:10447586
1, ack 3507402844, win 65535, length 235
19:00:59.185021 IP maa03s44-in-f10.1e100.net.https > sakthi-kumar-s-VirtualBox.57544: Flags [.], ack 235, win 65535, len
gth 0
19:00:59.431727 IP sakthi-kumar-s-VirtualBox.40008 > 170.72.239.211.https: Flags [P.], seq 1645473713:1645473779, ack 35
05929284, win 65535, length 66
19:00:59.433863 IP 170.72.239.211.https > sakthi-kumar-s-VirtualBox.40008: Flags [.], ack 66, win 65535, length 0
19:01:00.057114 IP maa03s44-in-f10.1e100.net.https > sakthi-kumar-s-VirtualBox.57544: Flags [P.], seq 1:140, ack 235, wi
n 65535, length 139
19:01:00.057411 IP sakthi-kumar-s-VirtualBox.57544 > maa03s44-in-f10.1e100.net.https: Flags [.], ack 140, win 65535, len
gth 0
19:01:00.061097 IP sakthi-kumar-s-VirtualBox.57544 > maa03s44-in-f10.1e100.net.https: Flags [P.], seq 235:274, ack 140,
win 65535, length 39
19:01:00.062324 IP 170.72.239.211.https > sakthi-kumar-s-VirtualBox.40008: Flags [P.], seq 1:111, ack 66, win 65535, len
gth 110
19:01:00.062335 IP maa03s44-in-f10.1e100.net.https > sakthi-kumar-s-VirtualBox.57544: Flags [.], ack 274, win 65535, len
```

2) Capture Packets with IP address

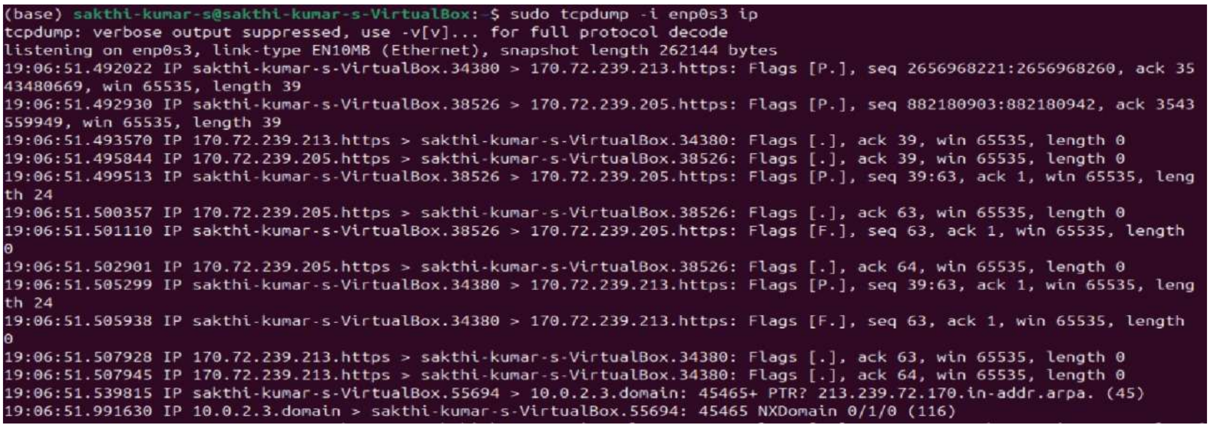


```
(base) sakthi-kumar-s@sakthi-kumar-s-VirtualBox:~$ sudo tcpdump -i enp0s3 host 10.0.2.15
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:05:36.840895 IP 170.72.239.211.https > sakthi-kumar-s-VirtualBox.47058: Flags [P.], seq 3543368917:3543368954, ack 38
73862941, win 65535, length 37
19:05:36.841690 IP sakthi-kumar-s-VirtualBox.47058 > 170.72.239.211.https: Flags [P.], seq 1:42, ack 37, win 65535, leng
th 41
19:05:36.847353 IP 170.72.239.211.https > sakthi-kumar-s-VirtualBox.47058: Flags [.], ack 42, win 65535, length 0
19:05:36.898711 IP sakthi-kumar-s-VirtualBox.33751 > 10.0.2.3.domain: 22896+ PTR? 15.2.0.10.in-addr.arpa. (40)
19:05:36.919196 IP 10.0.2.3.domain > sakthi-kumar-s-VirtualBox.33751: 22896 NXDomain 0/0/0 (40)
19:05:36.921312 IP sakthi-kumar-s-VirtualBox.41659 > 10.0.2.3.domain: 40582+ PTR? 211.239.72.170.in-addr.arpa. (45)
19:05:36.968893 IP 170.72.239.211.https > sakthi-kumar-s-VirtualBox.47006: Flags [P.], seq 3542402279:3542402316, ack 41
6843228, win 65535, length 37
19:05:36.969692 IP sakthi-kumar-s-VirtualBox.47006 > 170.72.239.211.https: Flags [P.], seq 1:42, ack 37, win 64022, leng
th 41
19:05:36.974127 IP 170.72.239.211.https > sakthi-kumar-s-VirtualBox.47006: Flags [.], ack 42, win 65535, length 0
19:05:37.064409 IP 10.0.2.3.domain > sakthi-kumar-s-VirtualBox.41659: 40582 NXDomain 0/1/0 (116)
19:05:37.068592 IP sakthi-kumar-s-VirtualBox.54377 > 10.0.2.3.domain: 11900+ PTR? 3.2.0.10.in-addr.arpa. (39)
19:05:37.077566 IP 10.0.2.3.domain > sakthi-kumar-s-VirtualBox.54377: 11900 NXDomain 0/0/0 (39)
19:05:37.128671 IP 170.72.239.211.https > sakthi-kumar-s-VirtualBox.47058: Flags [P.], seq 37:111, ack 42, win 65535, le
ngth 74
19:05:37.134808 IP sakthi-kumar-s-VirtualBox.47058 > 170.72.239.211.https: Flags [P.], seq 42:79, ack 111, win 65535, le
ngth 37
19:05:37.140043 IP 170.72.239.211.https > sakthi-kumar-s-VirtualBox.47058: Flags [.], ack 79, win 65535, length 0
19:05:37.252190 IP 170.72.239.211.https > sakthi-kumar-s-VirtualBox.47006: Flags [P.], seq 37:112, ack 42, win 65535, le
```

3) using port number



```
(base) sakthi-kumar-s@sakthi-kumar-s-VirtualBox:~$ sudo tcpdump -i enp0s3 port 80
[sudo] password for sakthi-kumar-s:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
03:29:07.817552 IP sakthi-kumar-s-VirtualBox.34922 > 49.44.116.245.http: Flags [S], seq 1658665569, win 64240, options [
mss 1460,sackOK,TS val 990939449 ecr 0,nop,wscale 7], length 0
03:29:07.861685 IP 49.44.116.245.http > sakthi-kumar-s-VirtualBox.34922: Flags [S.], seq 57856001, ack 1658665570, win 6
5535, options [mss 1460], length 0
03:29:07.861875 IP sakthi-kumar-s-VirtualBox.34922 > 49.44.116.245.http: Flags [.], ack 1, win 64240, length 0
03:29:07.863904 IP sakthi-kumar-s-VirtualBox.34922 > 49.44.116.245.http: Flags [P.], seq 1:440, ack 1, win 64240, length
 439: HTTP: POST / HTTP/1.1
03:29:07.864510 IP 49.44.116.245.http > sakthi-kumar-s-VirtualBox.34922: Flags [.], ack 440, win 65535, length 0
03:29:07.912779 IP 49.44.116.245.http > sakthi-kumar-s-VirtualBox.34922: Flags [P.], seq 1:891, ack 440, win 65535, leng
th 890: HTTP: HTTP/1.1 200 OK
03:29:07.912935 IP sakthi-kumar-s-VirtualBox.34922 > 49.44.116.245.http: Flags [.], ack 891, win 63350, length 0
03:29:08.347278 IP sakthi-kumar-s-VirtualBox.48270 > 82.221.107.34.bc.googleusercontent.com.http: Flags [S], seq 2904251
772, win 64240, options [mss 1460,sackOK,TS val 427881819 ecr 0,nop,wscale 7], length 0
```



```
(base) sakthi-kumar-s@sakthi-kumar-s-VirtualBox:~$ sudo tcpdump -i enp0s3 ip
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:06:51.492022 IP sakthi-kumar-s-VirtualBox.34380 > 170.72.239.213.https: Flags [P.], seq 2656968221:2656968260, ack 35
43480669, win 65535, length 39
19:06:51.492930 IP sakthi-kumar-s-VirtualBox.38526 > 170.72.239.205.https: Flags [P.], seq 882180903:882180942, ack 3543
559949, win 65535, length 39
19:06:51.493570 IP 170.72.239.213.https > sakthi-kumar-s-VirtualBox.34380: Flags [.], ack 39, win 65535, length 0
19:06:51.495844 IP 170.72.239.205.https > sakthi-kumar-s-VirtualBox.38526: Flags [.], ack 39, win 65535, length 0
19:06:51.499513 IP sakthi-kumar-s-VirtualBox.38526 > 170.72.239.205.https: Flags [P.], seq 39:63, ack 1, win 65535, leng
th 24
19:06:51.500357 IP 170.72.239.205.https > sakthi-kumar-s-VirtualBox.38526: Flags [.], ack 63, win 65535, length 0
19:06:51.501110 IP sakthi-kumar-s-VirtualBox.38526 > 170.72.239.205.https: Flags [F.], seq 63, ack 1, win 65535, length
0
19:06:51.502901 IP 170.72.239.205.https > sakthi-kumar-s-VirtualBox.38526: Flags [.], ack 64, win 65535, length 0
19:06:51.505299 IP sakthi-kumar-s-VirtualBox.34380 > 170.72.239.213.https: Flags [P.], seq 39:63, ack 1, win 65535, leng
th 24
19:06:51.505938 IP sakthi-kumar-s-VirtualBox.34380 > 170.72.239.213.https: Flags [F.], seq 63, ack 1, win 65535, length
0
19:06:51.507928 IP 170.72.239.213.https > sakthi-kumar-s-VirtualBox.34380: Flags [.], ack 63, win 65535, length 0
19:06:51.507945 IP 170.72.239.213.https > sakthi-kumar-s-VirtualBox.34380: Flags [.], ack 64, win 65535, length 0
19:06:51.539815 IP sakthi-kumar-s-VirtualBox.55694 > 10.0.2.3.domain: 45465+ PTR? 213.239.72.170.in-addr.arpa. (45)
19:06:51.991630 IP 10.0.2.3.domain > sakthi-kumar-s-VirtualBox.55694: 45465 NXDomain 0/1/0 (116)
```