LAB ASSIGNMENT No. 7: TCPDUMP Packet Analyzer

Aim:Study of Packet Sniffer toll TCPDUMP. Use it to capture and analyze the packet.

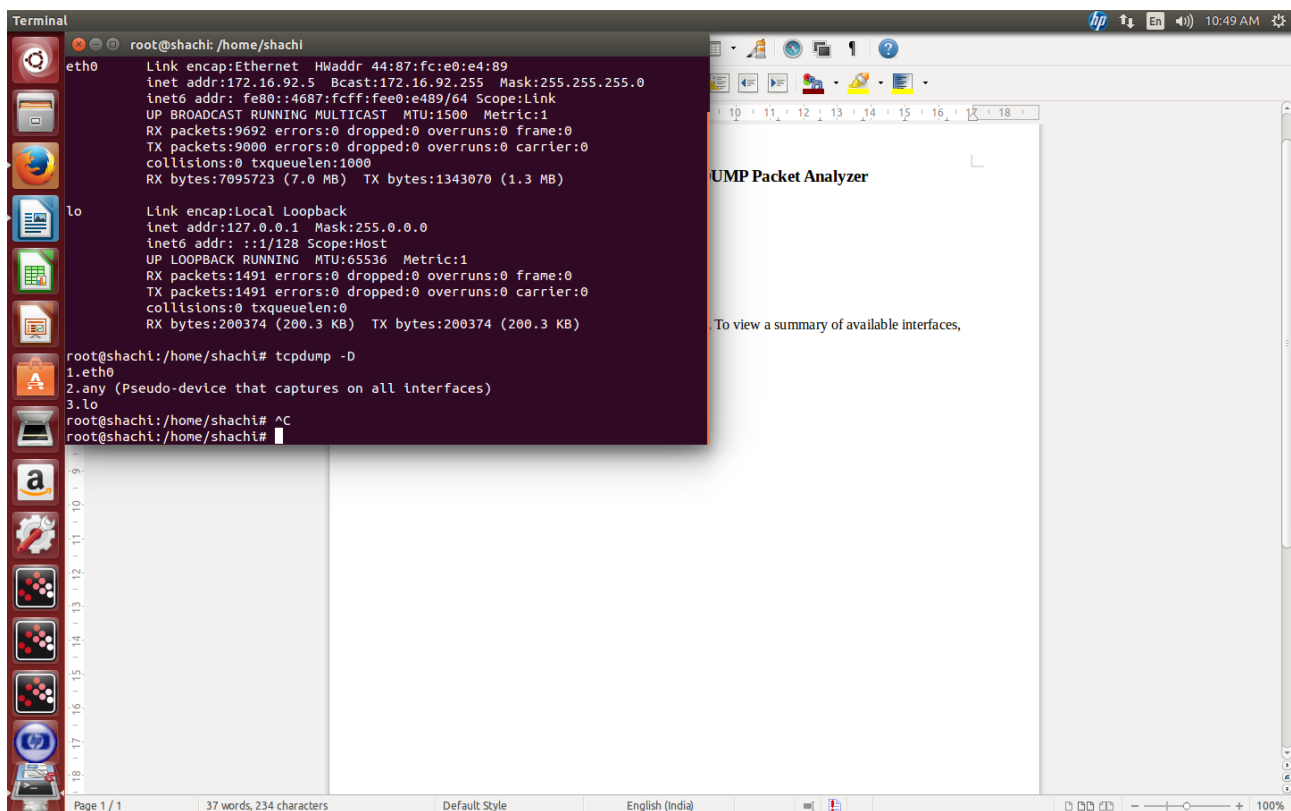1. To install tcpdump

```
$ sudo apt-get install tcpdump
```

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

```
# tcpdump -D
```


3. Basic command for sniffing

```
# tcpdump -n
```

The -n parameter is given to stop tcpdump from resolving ip addresses to hostnames, which take look and not required right now.

```
root@shachi: /home/shachi                                    hp  ⇵  En  ◀))  11:14 AM  ⚙
         inet6 addr: fe80::4687:fcff:fee0:e489/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:9692 errors:0 dropped:0 overruns:0 frame:0
         TX packets:9000 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:7095723 (7.0 MB)  TX bytes:1343070 (1.3 MB)

lo       Link encap:Local Loopback
         inet addr:127.0.0.1  Mask:255.0.0.0
         inet6 addr: ::1/128 Scope:Host
         UP LOOPBACK RUNNING  MTU:65536  Metric:1
         RX packets:1491 errors:0 dropped:0 overruns:0 frame:0
         TX packets:1491 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:200374 (200.3 KB)  TX bytes:200374 (200.3 KB)

root@shachi:/home/shachi# tcpdump -D
1.eth0
2.any (Pseudo-device that captures on all interfaces)
3.lo
root@shachi:/home/shachi# ^C
root@shachi:/home/shachi# tcpdump -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
11:11:48.755303 IP 172.16.92.5.43780 > 106.10.184.41.443: Flags [.], ack 263857829, win 367, options [nop,nop,TS val 2072096 ecr 29009846], length 0
11:11:48.817850 IP 106.10.184.41.443 > 172.16.92.5.43780: Flags [.], ack 1, win 97, options [nop,nop,TS val 29019925 ecr 2056996], length 0
11:11:49.811361 IP 172.16.92.5.43754 > 106.10.184.41.443: Flags [.], ack 3180545544, win 604, options [nop,nop,TS val 2072360 ecr 29010743], length 0
11:11:50.038240 IP 106.10.184.41.443 > 172.16.92.5.43754: Flags [.], ack 1, win 434, options [nop,nop,TS val 29020981 ecr 2056999], length 0
11:11:50.254917 IP 172.16.92.1.53 > 172.16.92.5.25220: 49967 0/1/0 (95)
11:11:51.602814 IP 172.16.92.5.39662 > 104.244.42.129.443: Flags [P.], seq 466596947:466596993, ack 1889999207, win 237, options [nop,nop,TS val 2072807
 ecr 3388722348], length 46
11:11:51.602870 IP 172.16.92.5.39663 > 104.244.42.129.443: Flags [P.], seq 3440648596:3440648642, ack 2287316051, win 237, options [nop,nop,TS val 20728
07 ecr 3387829666], length 46
11:11:51.731329 IP 172.16.92.5.38774 > 106.10.200.161.443: Flags [.], ack 3095876107, win 886, options [nop,nop,TS val 2072840 ecr 3356291879], length 0
11:11:51.791803 IP 106.10.200.161.443 > 172.16.92.5.38774: Flags [.], ack 1, win 501, options [nop,nop,TS val 3356301942 ecr 2067807], length 0
11:11:51.855464 IP 104.244.42.129.443 > 172.16.92.5.39662: Flags [.], ack 46, win 122, options [nop,nop,TS val 3388780638 ecr 2072807], length 0
11:11:51.855481 IP 104.244.42.129.443 > 172.16.92.5.39662: Flags [P.], seq 1:47, ack 46, win 122, options [nop,nop,TS val 3388780638 ecr 2072807], lengt
h 46
11:11:51.863087 IP 104.244.42.129.443 > 172.16.92.5.39663: Flags [.], ack 46, win 122, options [nop,nop,TS val 3387887640 ecr 2072807], length 0
11:11:51.863102 IP 104.244.42.129.443 > 172.16.92.5.39663: Flags [P.], seq 1:47, ack 46, win 122, options [nop,nop,TS val 3387887640 ecr 2072807], lengt
h 46
11:11:51.895360 IP 172.16.92.5.39662 > 104.244.42.129.443: Flags [.], ack 47, win 237, options [nop,nop,TS val 2072881 ecr 3388780638], length 0
11:11:51.899345 IP 172.16.92.5.39663 > 104.244.42.129.443: Flags [.], ack 47, win 237, options [nop,nop,TS val 2072882 ecr 3387887640], length 0
z11:11:53.491365 IP 172.16.92.5.43672 > 66.196.113.5.443: Flags [.], ack 2320217246, win 403, options [nop,nop,TS val 2073280 ecr 3020942202], length 0
11:11:53.693795 IP 66.196.113.5.443 > 172.16.92.5.43672: Flags [.], ack 1, win 501, options [nop,nop,TS val 3020952409 ecr 2065621], length 0
^Z
[1]+  Stopped                 tcpdump -n
root@shachi:/home/shachi#
```

Consider the output line
11:11:48.755303 IP 172.16.92.5.43780 > 106.10.184.41.443: Flags [.], ack 263857829, win 367, options [nop,nop,TS val 2072096 ecr 29009846], length 0

11:11:48.755303 is the time stamp with microsecond precision. Next is the protocol of the packet called IP (stands for Internet protocol and it is under this protocol that most of the internet communication goes on). Next is the source ip address joined with the source port. Following next is the destination port and then some information about the packet.

Now lets increase the display resolution of this packet, or get more details about it. The verbose switch comes in handy. Here is a quick example

4. tcpdump -v -n

Now with the verbose switch lots of additional details about the packet are also being displayed. And these include the ttl, id, tcp flags, packet length etc.

5. Getting the ethernet header (link layer headers)

In the above examples details of the ethernet header are not printed. Use the -e option to print the ethernet header details as well.

Filtering packets using expressions

6. selecting packets with specific protocol

```
# tcpdump -n tcp
```

#

tcpdump -n icmp

7. 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
```

```
root@shachi:/home/shachi
11:47:19.190569 IP 172.16.92.5 > 172.16.92.1: ICMP echo request, id 3724, seq 705, length 64
11:47:19.191909 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 705, length 64
11:47:20.192087 IP 172.16.92.5 > 172.16.92.1: ICMP echo request, id 3724, seq 706, length 64
11:47:20.193480 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 706, length 64
^Z
[7]+  Stopped                 tcpdump -n icmp
root@shachi:/home/shachi# ^C
root@shachi:/home/shachi# tcpdump -n src 172.16.92.3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
^Z
[8]+  Stopped                 tcpdump -n src 172.16.92.3
root@shachi:/home/shachi# tcpdump -n src 172.16.92.1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
11:51:51.587639 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 977, length 64
11:51:52.589224 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 978, length 64
11:51:53.590784 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 979, length 64
11:51:54.592258 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 980, length 64
11:51:55.593744 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 981, length 64
11:51:56.595282 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 982, length 64
11:51:57.596758 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 983, length 64
11:51:58.598208 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 984, length 64
11:51:59.599724 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 985, length 64
^Z
[9]+  Stopped                 tcpdump -n src 172.16.92.1
root@shachi:/home/shachi# tcpdump -n src 172.16.92.1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
11:52:26.641253 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 1012, length 64
11:52:27.642934 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 1013, length 64
11:52:28.644622 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 1014, length 64
11:52:29.646324 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 1015, length 64
11:52:30.647978 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 1016, length 64
11:52:31.649661 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 1017, length 64
^Z
[10]+  Stopped                tcpdump -n src 172.16.92.1
root@shachi:/home/shachi# tcpdump -n src 172.16.92.6
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
^Z
[11]+  Stopped                tcpdump -n src 172.16.92.6
root@shachi:/home/shachi# tcpdump -n src 172.16.92.2
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
^Z
[12]+  Stopped                tcpdump -n src 172.16.92.2
root@shachi:/home/shachi#
```

tcpdump -n dst 172.16.92.1


```
root@shachi:/home/shachi
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
11:51:51.587639 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 977, length 64
11:51:52.589224 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 978, length 64
11:51:53.590784 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 979, length 64
11:51:54.592258 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 980, length 64
11:51:55.593744 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 981, length 64
11:51:56.595282 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 982, length 64
11:51:57.596758 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 983, length 64
11:51:58.598208 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 984, length 64
11:51:59.599724 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 985, length 64
^Z
[9]+  Stopped                 tcpdump -n src 172.16.92.1
root@shachi:/home/shachi# tcpdump -n src 172.16.92.1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
11:52:26.641253 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 1012, length 64
11:52:27.642934 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 1013, length 64
11:52:28.644622 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 1014, length 64
11:52:29.646324 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 1015, length 64
11:52:30.647978 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 1016, length 64
11:52:31.649661 IP 172.16.92.1 > 172.16.92.5: ICMP echo reply, id 3724, seq 1017, length 64
^Z
[10]+  Stopped                tcpdump -n src 172.16.92.6
root@shachi:/home/shachi# tcpdump -n src 172.16.92.6
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
^Z
[11]+  Stopped                tcpdump -n src 172.16.92.2
root@shachi:/home/shachi# tcpdump -n src 172.16.92.2
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
^Z
[12]+  Stopped                tcpdump -n src 172.16.92.2
root@shachi:/home/shachi# tcpdump -n dest 172.16.92.2
tcpdump: syntax error
root@shachi:/home/shachi# tcpdump -n dst 172.16.92.1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
11:55:36.938473 IP 172.16.92.5 > 172.16.92.1: ICMP echo request, id 3724, seq 1202, length 64
11:55:37.940016 IP 172.16.92.5 > 172.16.92.1: ICMP echo request, id 3724, seq 1203, length 64
11:55:38.941509 IP 172.16.92.5 > 172.16.92.1: ICMP echo request, id 3724, seq 1204, length 64
11:55:39.943064 IP 172.16.92.5 > 172.16.92.1: ICMP echo request, id 3724, seq 1205, length 64
11:55:40.944626 IP 172.16.92.5 > 172.16.92.1: ICMP echo request, id 3724, seq 1206, length 64
11:55:41.946140 IP 172.16.92.5 > 172.16.92.1: ICMP echo request, id 3724, seq 1207, length 64
11:55:42.947695 IP 172.16.92.5 > 172.16.92.1: ICMP echo request, id 3724, seq 1208, length 64
^Z
[13]+  Stopped                tcpdump -n dst 172.16.92.1
root@shachi:/home/shachi#
```

tcpdump -n port 80

```
ngth 389
11:59:10.250287 IP 172.16.92.5.60751 > 23.65.124.32.80: Flags [.], ack 1738, win 272, options [nop,nop,TS val 2782469 ecr 1810011394], length 0
11:59:10.262485 IP 23.65.124.25.80 > 172.16.92.5.56518: Flags [.], seq 2697:4045, ack 665, win 947, options [nop,nop,TS val 1965639424 ecr 2782467], len
gth 1348
11:59:10.262512 IP 172.16.92.5.56518 > 23.65.124.25.80: Flags [.], ack 17492, win 523, options [nop,nop,TS val 2782472 ecr 1965639403,nop,nop,sack 1 {26
97:4045}], length 0
11:59:10.262707 IP 23.65.124.25.80 > 172.16.92.5.56518: Flags [.], seq 4045:5393, ack 665, win 947, options [nop,nop,TS val 1965639424 ecr 2782467], len
gth 1348
11:59:10.262717 IP 172.16.92.5.56518 > 23.65.124.25.80: Flags [.], ack 17492, win 523, options [nop,nop,TS val 2782472 ecr 1965639403,nop,nop,sack 1 {40
45:5393}], length 0
11:59:10.263056 IP 23.65.124.25.80 > 172.16.92.5.56518: Flags [.], seq 5393:6741, ack 665, win 947, options [nop,nop,TS val 1965639424 ecr 2782467], len
gth 1348
11:59:10.263066 IP 172.16.92.5.56518 > 23.65.124.25.80: Flags [.], ack 17492, win 523, options [nop,nop,TS val 2782472 ecr 1965639403,nop,nop,sack 1 {53
93:6741}], length 0
11:59:10.263177 IP 23.65.124.25.80 > 172.16.92.5.56518: Flags [.], seq 6741:8089, ack 665, win 947, options [nop,nop,TS val 1965639424 ecr 2782467], len
gth 1348
11:59:10.263182 IP 172.16.92.5.56518 > 23.65.124.25.80: Flags [.], ack 17492, win 523, options [nop,nop,TS val 2782472 ecr 1965639403,nop,nop,sack 1 {67
41:8089}], length 0
11:59:10.263403 IP 23.65.124.25.80 > 172.16.92.5.56518: Flags [.], seq 8089:9437, ack 665, win 947, options [nop,nop,TS val 1965639424 ecr 2782467], len
gth 1348
11:59:10.263412 IP 172.16.92.5.56518 > 23.65.124.25.80: Flags [.], ack 17492, win 523, options [nop,nop,TS val 2782473 ecr 1965639403,nop,nop,sack 1 {80
89:9437}], length 0
11:59:10.265416 IP 23.65.124.25.80 > 172.16.92.5.56518: Flags [.], ack 665, win 947, options [nop,nop,TS val 1965639428 ecr 2782469], length 0
11:59:10.266724 IP 23.65.124.25.80 > 172.16.92.5.56518: Flags [.], ack 665, win 947, options [nop,nop,TS val 1965639430 ecr 2782469], length 0
11:59:10.267394 IP 23.65.124.25.80 > 172.16.92.5.56518: Flags [.], ack 665, win 947, options [nop,nop,TS val 1965639430 ecr 2782469], length 0
11:59:10.283304 IP 23.2.16.91.80 > 172.16.92.5.52070: Flags [P.], seq 108257:109074, ack 9383, win 1498, options [nop,nop,TS val 2288872455 ecr 2782455]
, length 817
11:59:10.283339 IP 172.16.92.5.52070 > 23.2.16.91.80: Flags [.], ack 109074, win 1324, options [nop,nop,TS val 2782477 ecr 2288872455], length 0
11:59:10.289595 IP 23.2.16.91.80 > 172.16.92.5.52067: Flags [P.], seq 101844:104084, ack 6505, win 1319, options [nop,nop,TS val 2288872458 ecr 2782455]
, length 2240
11:59:10.295197 IP 172.16.92.5.52067 > 23.2.16.91.80: Flags [.], ack 104084, win 1324, options [nop,nop,TS val 2782480 ecr 2288872458], length 0
^Z
[14]+  Stopped                 tcpdump -n port 80
root@shachi:/home/shachi# tcpdump -n port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
11:59:42.993474 IP 54.225.189.34.80 > 172.16.92.5.57552: Flags [.], ack 3070349890, win 76, options [nop,nop,TS val 952097209 ecr 2788093], length 0
11:59:43.763310 IP 172.16.92.5.42413 > 74.125.130.147.80: Flags [.], ack 357444536, win 237, options [nop,nop,TS val 2790848 ecr 2528258055], length 0
11:59:43.795321 IP 172.16.92.5.42416 > 74.125.130.147.80: Flags [.], ack 1841024414, win 237, options [nop,nop,TS val 2790856 ecr 2477051253], length 0
11:59:43.827318 IP 74.125.130.147.80 > 172.16.92.5.42413: Flags [.], ack 1, win 342, options [nop,nop,TS val 2528268135 ecr 2783305], length 0
11:59:43.827330 IP 172.16.92.5.53185 > 23.58.34.202.80: Flags [.], ack 1901034413, win 507, options [nop,nop,TS val 2790864 ecr 2433724615], length 0
11:59:43.851874 IP 23.58.34.202.80 > 172.16.92.5.53185: Flags [.], ack 1, win 1005, options [nop,nop,TS val 2433734662 ecr 2783336], length 0
11:59:43.857986 IP 74.125.130.147.80 > 172.16.92.5.42416: Flags [.], ack 1, win 342, options [nop,nop,TS val 2477061333 ecr 2783319], length 0
11:59:43.987379 IP 172.16.92.5.52070 > 23.2.16.91.80: Flags [.], ack 2496230879, win 1324, options [nop,nop,TS val 2790904 ecr 2288896133], length 0
11:59:44.075833 IP 23.2.16.91.80 > 172.16.92.5.52070: Flags [.], ack 1, win 1657, options [nop,nop,TS val 2288906245 ecr 2783345], length 0
^Z
[15]+  Stopped                 tcpdump -n port 80
root@shachi:/home/shachi# tcpdump  port 80
```

tcpdump port 80


```
11:59:43.827318 IP 74.125.130.147.80 > 172.16.92.5.42413: Flags [.], ack 1, win 342, options [nop,nop,TS val 2528268135 ecr 2783305], length 0
11:59:43.827330 IP 172.16.92.5.53185 > 23.58.34.202.80: Flags [.], ack 1901034413, win 507, options [nop,nop,TS val 2790864 ecr 2433724615], length 0
11:59:43.851874 IP 23.58.34.202.80 > 172.16.92.5.53185: Flags [.], ack 1, win 1005, options [nop,nop,TS val 2433734662 ecr 2783336], length 0
11:59:43.857986 IP 74.125.130.147.80 > 172.16.92.5.42416: Flags [.], ack 1, win 342, options [nop,nop,TS val 2477061333 ecr 2783319], length 0
11:59:43.987379 IP 172.16.92.5.52070 > 23.2.16.91.80: Flags [.], ack 2496230879, win 1324, options [nop,nop,TS val 2790904 ecr 2288896133], length 0
11:59:44.075833 IP 23.2.16.91.80 > 172.16.92.5.52070: Flags [.], ack 1, win 1657, options [nop,nop,TS val 2288906245 ecr 2783345], length 0
^Z
[15]+  Stopped                 tcpdump -n port 80
root@shachi:/home/shachi# tcpdump  port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
12:01:59.827359 IP 172.16.92.5.49469 > a23-65-124-11.deploy.static.akamaitechnologies.com.http: Flags [.], ack 1511875855, win 715, options [nop,nop,TS
val 2824864 ecr 1881618913], length 0
12:01:59.843030 IP a23-65-124-11.deploy.static.akamaitechnologies.com.http > 172.16.92.5.49469: Flags [.], ack 1, win 1201, options [nop,nop,TS val 1881
628944 ecr 2819856], length 0
12:02:01.171347 IP 172.16.92.5.47450 > a23-2-16-200.deploy.static.akamaitechnologies.com.http: Flags [.], ack 103999294, win 237, options [nop,nop,TS va
l 2825200 ecr 1813304904], length 0
12:02:01.262031 IP a23-2-16-200.deploy.static.akamaitechnologies.com.http > 172.16.92.5.47450: Flags [.], ack 1, win 961, options [nop,nop,TS val 181331
5015 ecr 2812588], length 0
12:02:02.213919 IP 172.16.92.5.59629 > ec2-23-23-170-207.compute-1.amazonaws.com.http: Flags [S], seq 1844346817, win 29200, options [mss 1460,sackOK,TS
 val 2825460 ecr 0,nop,wscale 7], length 0
12:02:02.356972 IP 172.16.92.5.58426 > ec2-54-235-182-182.compute-1.amazonaws.com.http: Flags [S], seq 2030480750, win 29200, options [mss 1460,sackOK,T
S val 2825496 ecr 0,nop,wscale 7], length 0
12:02:02.465018 IP 172.16.92.5.58427 > ec2-54-235-182-182.compute-1.amazonaws.com.http: Flags [S], seq 2822657575, win 29200, options [mss 1460,sackOK,T
S val 2825523 ecr 0,nop,wscale 7], length 0
12:02:02.476171 IP ec2-23-23-170-207.compute-1.amazonaws.com.http > 172.16.92.5.59629: Flags [S.], seq 679810268, ack 1844346818, win 17898, options [ms
s 1360,sackOK,TS val 2655095165 ecr 2825460,nop,wscale 8], length 0
12:02:02.476209 IP 172.16.92.5.59629 > ec2-23-23-170-207.compute-1.amazonaws.com.http: Flags [.], ack 1, win 229, options [nop,nop,TS val 2825526 ecr 26
55095165], length 0
12:02:02.476377 IP 172.16.92.5.59629 > ec2-23-23-170-207.compute-1.amazonaws.com.http: Flags [P.], seq 1:563, ack 1, win 229, options [nop,nop,TS val 28
25526 ecr 2655095165], length 562
12:02:02.606311 IP ec2-54-235-182-182.compute-1.amazonaws.com.http > 172.16.92.5.58426: Flags [S.], seq 508822866, ack 2030480751, win 17898, options [m
ss 1360,sackOK,TS val 3010472859 ecr 2825496,nop,wscale 8], length 0
12:02:02.606357 IP 172.16.92.5.58426 > ec2-54-235-182-182.compute-1.amazonaws.com.http: Flags [.], ack 1, win 229, options [nop,nop,TS val 2825558 ecr 3
010472859], length 0
12:02:02.733636 IP ec2-54-235-182-182.compute-1.amazonaws.com.http > 172.16.92.5.58427: Flags [S.], seq 715329396, ack 2822657576, win 17898, options [m
ss 1360,sackOK,TS val 3010472889 ecr 2825523,nop,wscale 8], length 0
12:02:02.733688 IP 172.16.92.5.58427 > ec2-54-235-182-182.compute-1.amazonaws.com.http: Flags [.], ack 1, win 229, options [nop,nop,TS val 2825590 ecr 3
010472889], length 0
12:02:02.737495 IP ec2-23-23-170-207.compute-1.amazonaws.com.http > 172.16.92.5.59629: Flags [.], ack 563, win 75, options [nop,nop,TS val 2655095230 ec
r 2825526], length 0
12:02:02.739779 IP ec2-23-23-170-207.compute-1.amazonaws.com.http > 172.16.92.5.59629: Flags [P.], seq 1:214, ack 563, win 75, options [nop,nop,TS val 2
655095231 ecr 2825526], length 213
12:02:02.739799 IP 172.16.92.5.59629 > ec2-23-23-170-207.compute-1.amazonaws.com.http: Flags [.], ack 214, win 237, options [nop,nop,TS val 2825592 ecr
2655095231], length 0
^Z
[16]+  Stopped                 tcpdump port 80
root@shachi:/home/shachi#
```

Specific Packets from specific port

```
# 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

root@shachi: /home/shachi

12:15:14.683917 IP 172.16.92.5.59600 > 23.65.124.16.80: Flags [.], ack 2697, win 1216, options [nop,nop,TS val 3023578 ecr 1812018734], length 0
12:15:14.684042 IP 23.65.124.16.80 > 172.16.92.5.59600: Flags [P.], seq 2697:4676, ack 691, win 1534, options [nop,nop,TS val 1812018734 ecr 3023572], l
ength 1979
12:15:14.684063 IP 172.16.92.5.59600 > 23.65.124.16.80: Flags [.], ack 4676, win 1247, options [nop,nop,TS val 3023578 ecr 1812018734], length 0
^Z
[19]+ Stopped   tcpdump -n portrange 1-80
root@shachi:/home/shachi# tcpdump less 32
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
^Z
[20]+ Stopped   tcpdump less 32
root@shachi:/home/shachi# tcpdump -n >32
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
^Z
[21]+ Stopped   tcpdump -n > 32
root@shachi:/home/shachi# tcpdump -n src port 1025 # tcpdump dst port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
^Z
[22]+ Stopped   tcpdump -n src port 1025
root@shachi:/home/shachi# tcpdump -n src port 443
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
12:23:30.744322 IP 203.84.220.151.443 > 172.16.92.5.54288: Flags [.], ack 399553216, win 103, options [nop,nop,TS val 3956133356 ecr 3147592], length 0
12:23:30.744352 IP 203.84.220.151.443 > 172.16.92.5.54288: Flags [P.], seq 0:46, ack 1, win 103, options [nop,nop,TS val 3956133356 ecr 3147592], length
 46
12:23:30.833318 IP 106.10.200.161.443 > 172.16.92.5.39631: Flags [P.], seq 3713984124:3713984422, ack 3661746272, win 151, options [nop,nop,TS val 33606
00379 ecr 3103255], length 298
12:23:30.833357 IP 106.10.200.161.443 > 172.16.92.5.39631: Flags [P.], seq 298:616, ack 1, win 151, options [nop,nop,TS val 3360600379 ecr 3103255], len
gth 318
12:23:30.850860 IP 106.10.200.161.443 > 172.16.92.5.39631: Flags [P.], seq 616:650, ack 1, win 151, options [nop,nop,TS val 3360600398 ecr 3103255], len
gth 34
12:23:32.519042 IP 203.84.220.151.443 > 172.16.92.5.54288: Flags [.], ack 262, win 112, options [nop,nop,TS val 3956135131 ecr 3148026], length 0
12:23:32.694379 IP 203.84.220.151.443 > 172.16.92.5.54288: Flags [P.], seq 46:434, ack 262, win 112, options [nop,nop,TS val 3956135306 ecr 3148026], le
ngth 388
12:23:32.694431 IP 203.84.220.151.443 > 172.16.92.5.54288: Flags [P.], seq 434:482, ack 262, win 112, options [nop,nop,TS val 3956135306 ecr 3148026], l
ength 48
12:23:32.695135 IP 203.84.220.151.443 > 172.16.92.5.54288: Flags [.], seq 482:1830, ack 262, win 112, options [nop,nop,TS val 3956135306 ecr 3148026], l
ength 1348
12:23:32.695415 IP 203.84.220.151.443 > 172.16.92.5.54288: Flags [P.], seq 1830:4525, ack 262, win 112, options [nop,nop,TS val 3956135306 ecr 3148026],
 length 2695
12:23:33.080739 IP 106.10.200.161.443 > 172.16.92.5.39631: Flags [.], ack 1, win 151, options [nop,nop,TS val 3360602627 ecr 3147619,nop,nop,sack 1 {134
9:1778}], length 0
12:23:33.080788 IP 106.10.200.161.443 > 172.16.92.5.39631: Flags [.], ack 1778, win 172, options [nop,nop,TS val 3360602627 ecr 3148121], length 0
^Z
[23]+ Stopped   tcpdump -n src port 443
root@shachi:/home/shachi#