LAB ASSIGNMENT No. 7: TCPDUMP Packet Analyzer

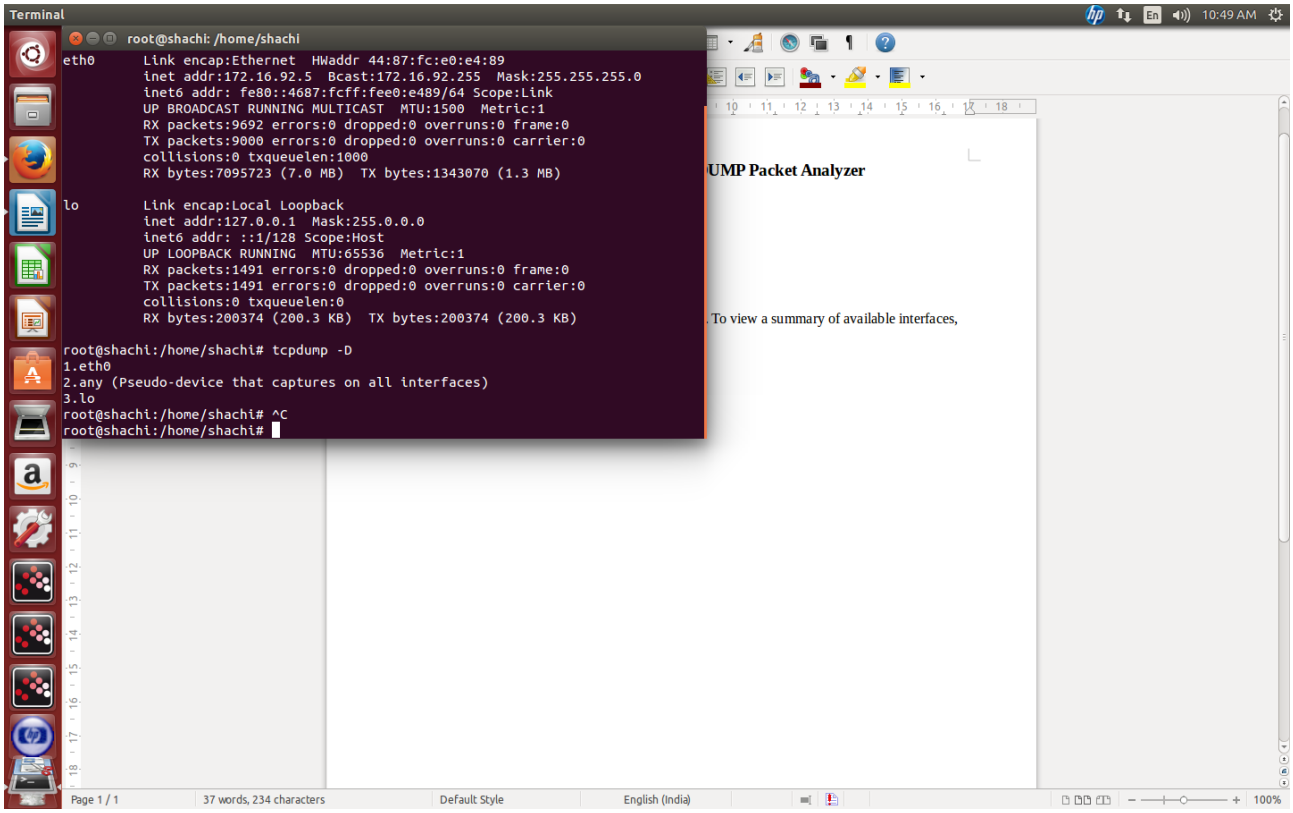
Aim:Study of Packet Sniffer toll TCPDUMP. Use it to capture and analyze the packet.

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

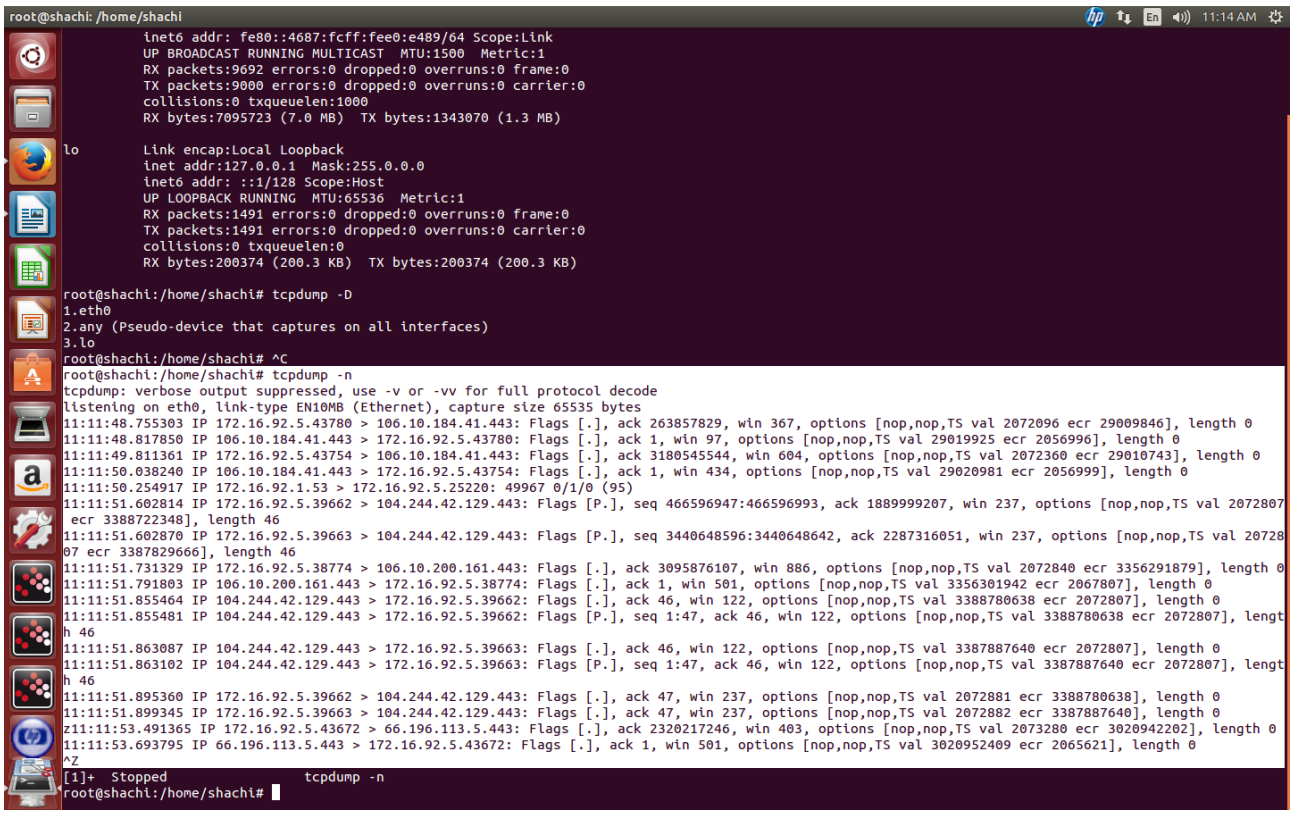
```
# tcpdump -D
```



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.



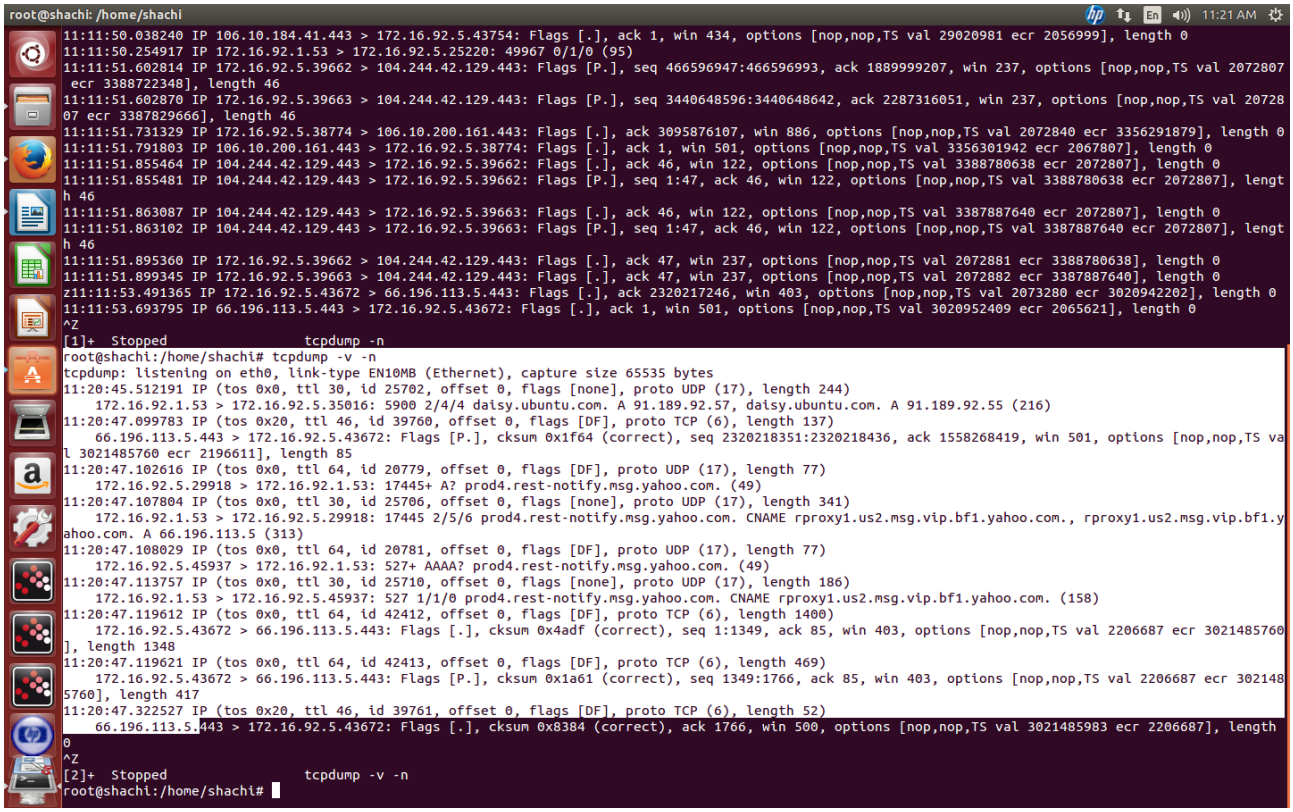
Consider the output line
11:11:48.755303 IP 172.16.92.5.43780 > 106.10.184.41.443: Flags [.], ack 263857829, win 367, options [nop,nop,TS val 2072096 ecr 29009846], length 0

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

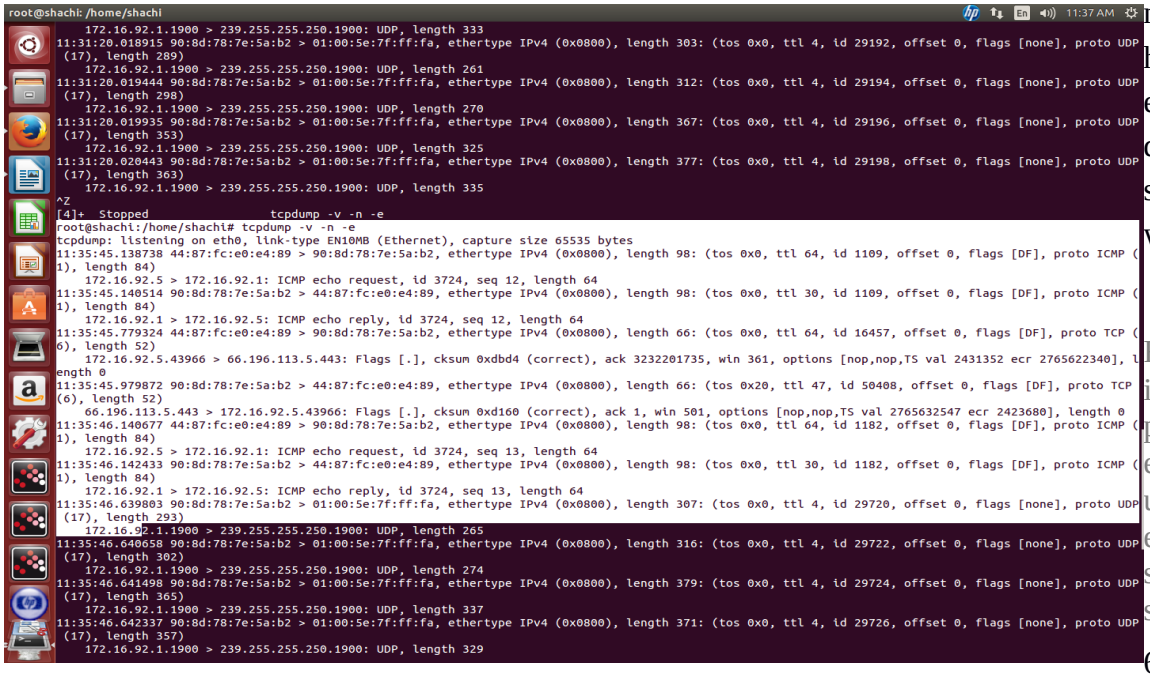
4. tcpdump -v -n

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.

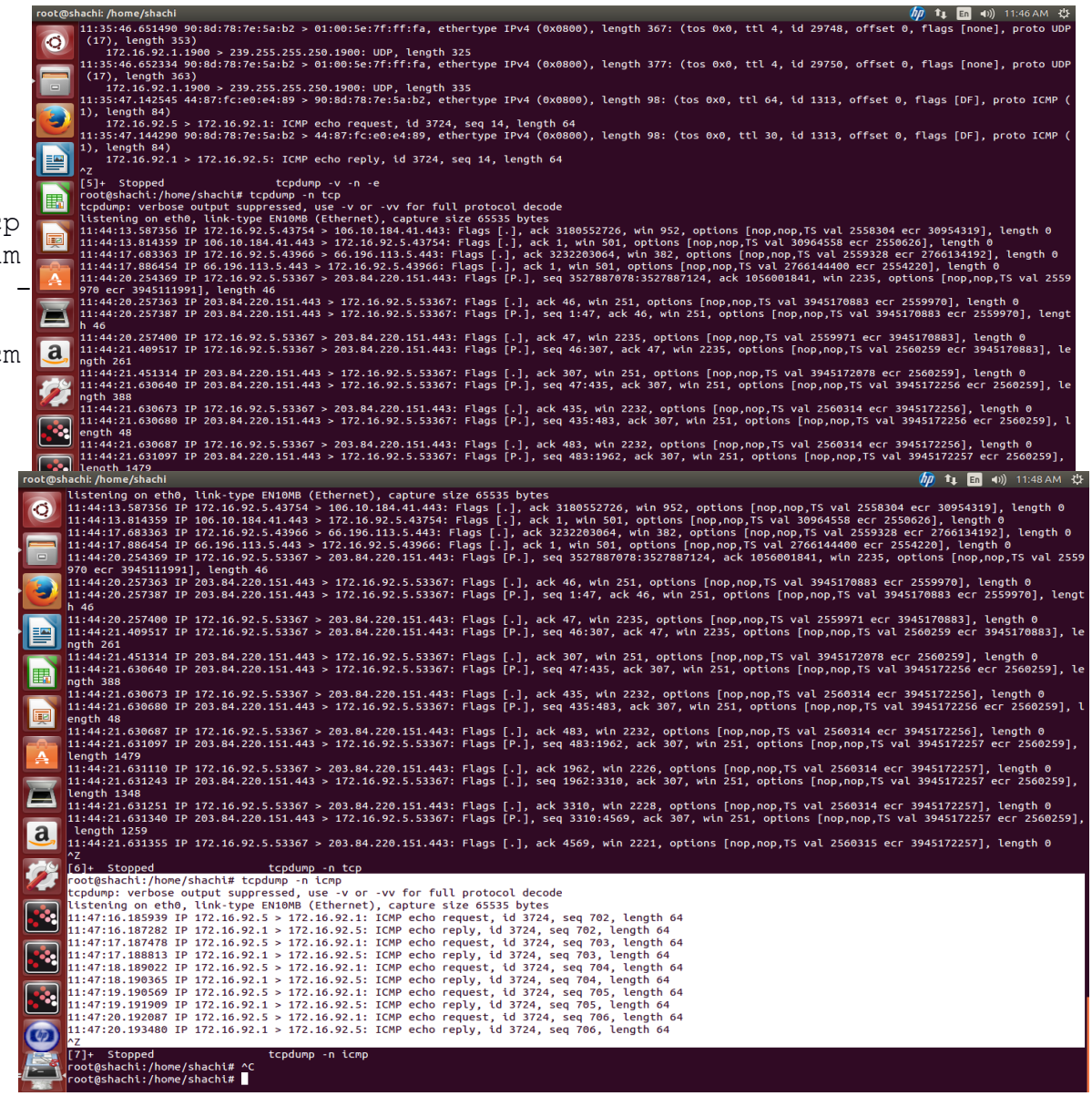


Filtering packets using expressions

6. selecting packets with specific protocol

```
# tcpdump -n tcp
```

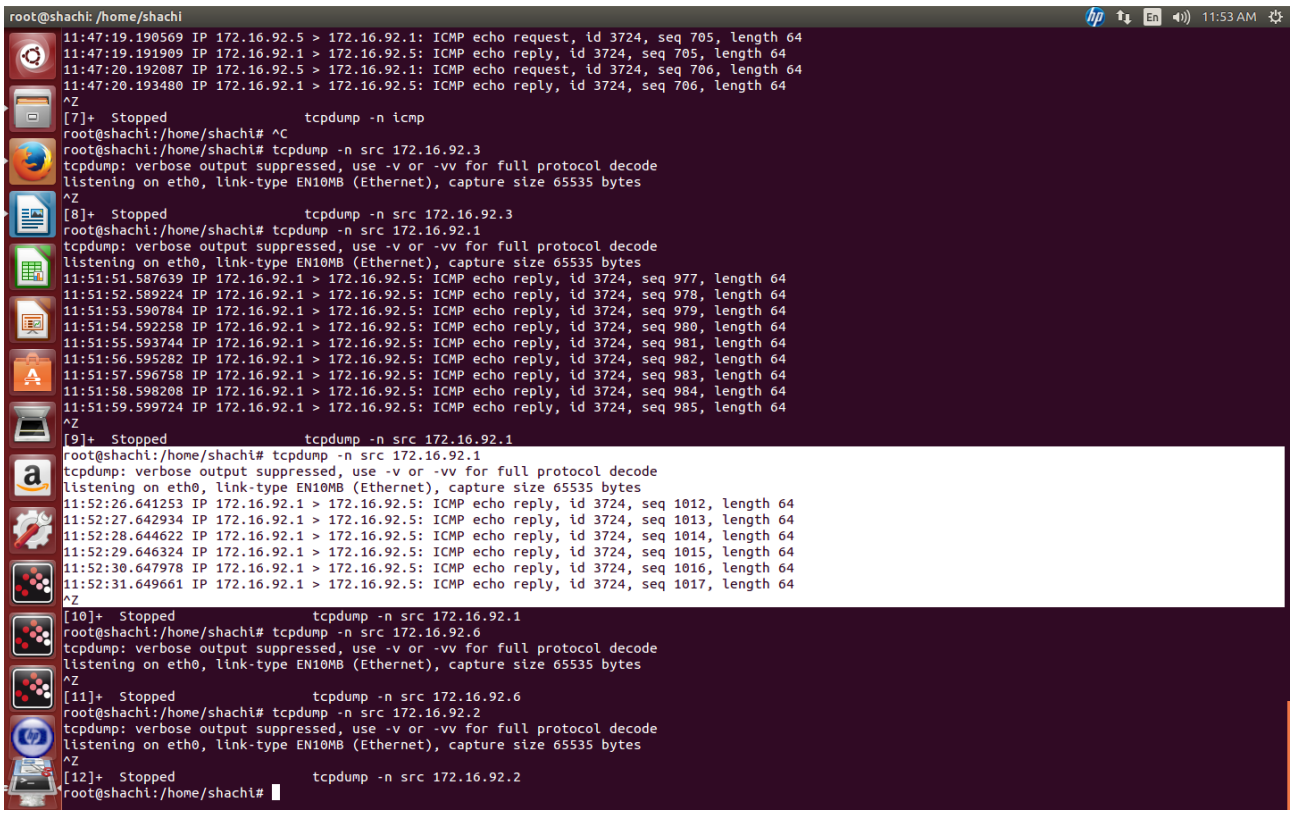
tcpdump -n icmp



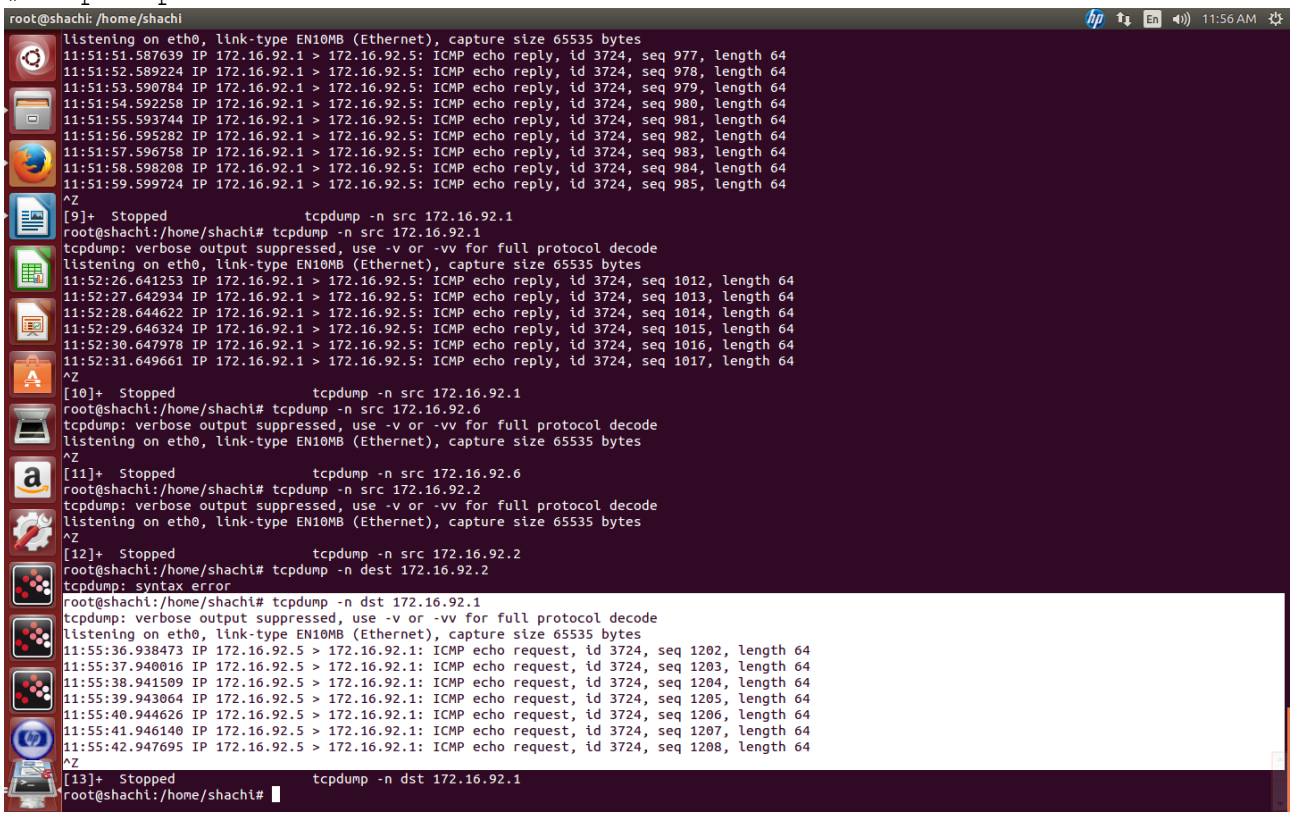
7. Particular host or port

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

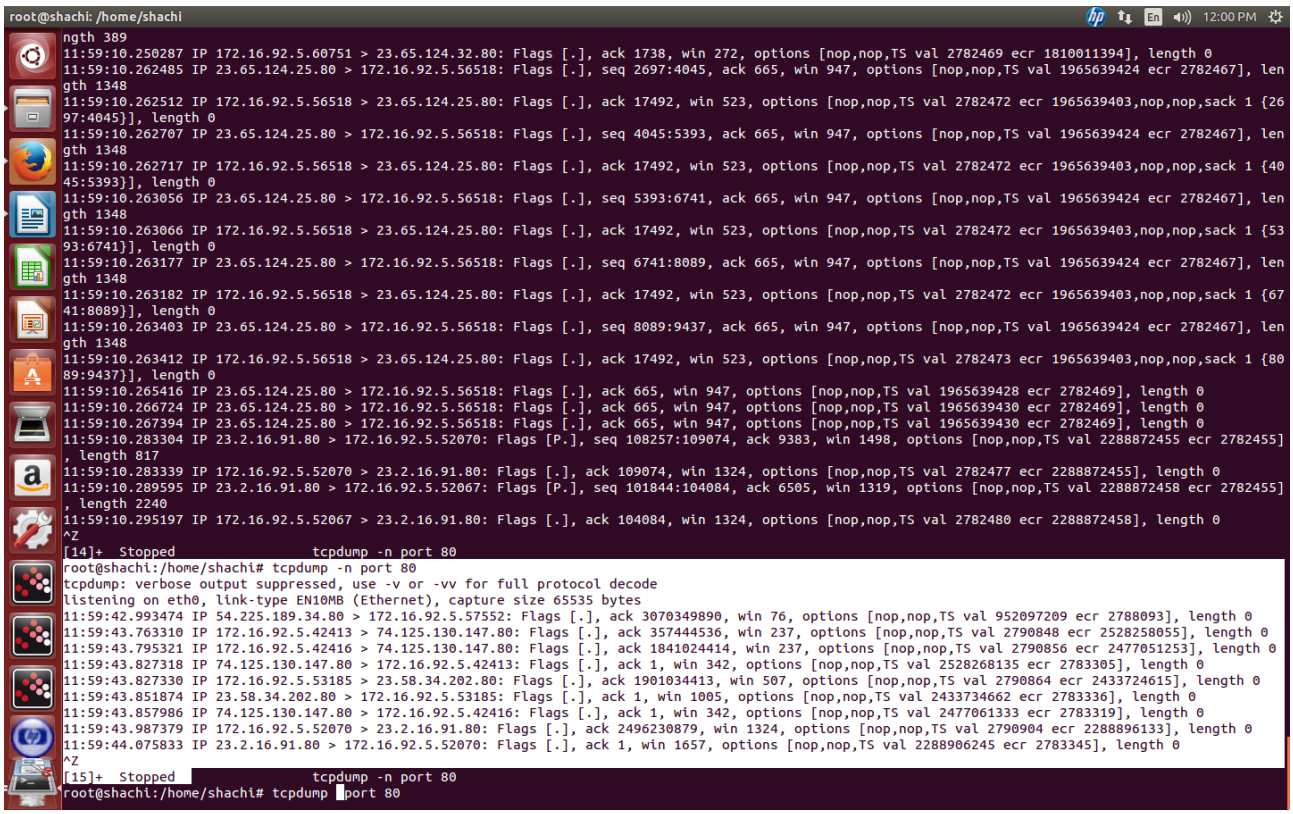
```
# tcpdump -n src 172.16.92.1
```



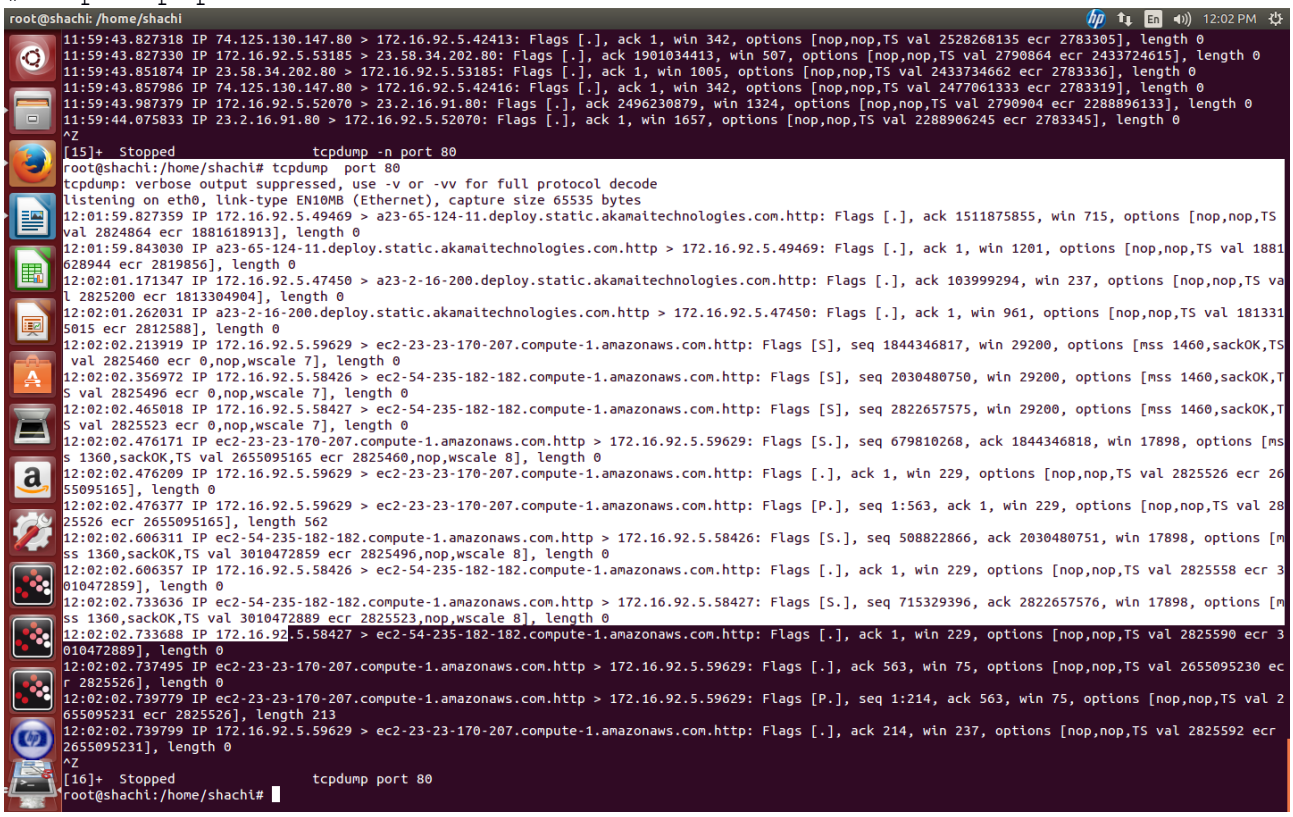
tcpdump -n dst 172.16.92.1



tcpdump -n port 80

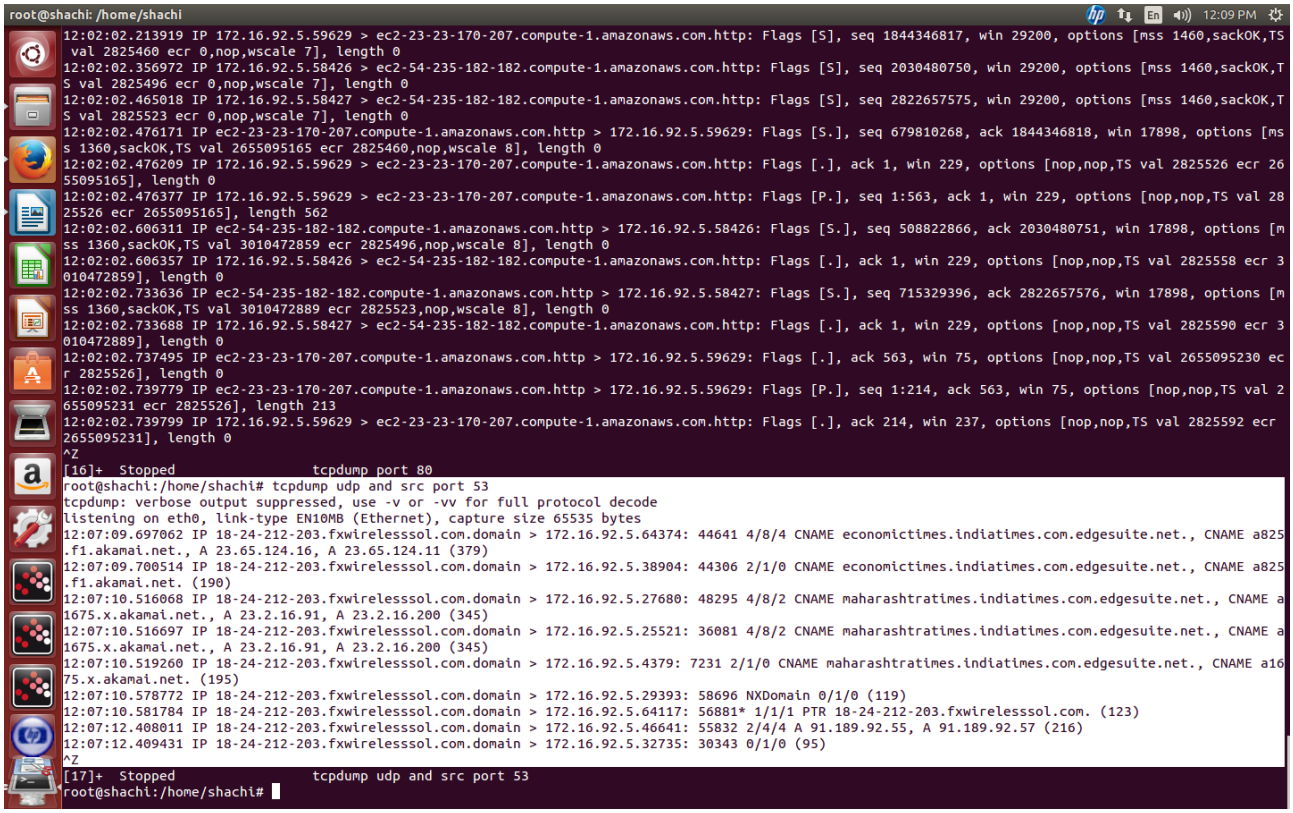


tcpdump port 80



Specific Packets from specific port

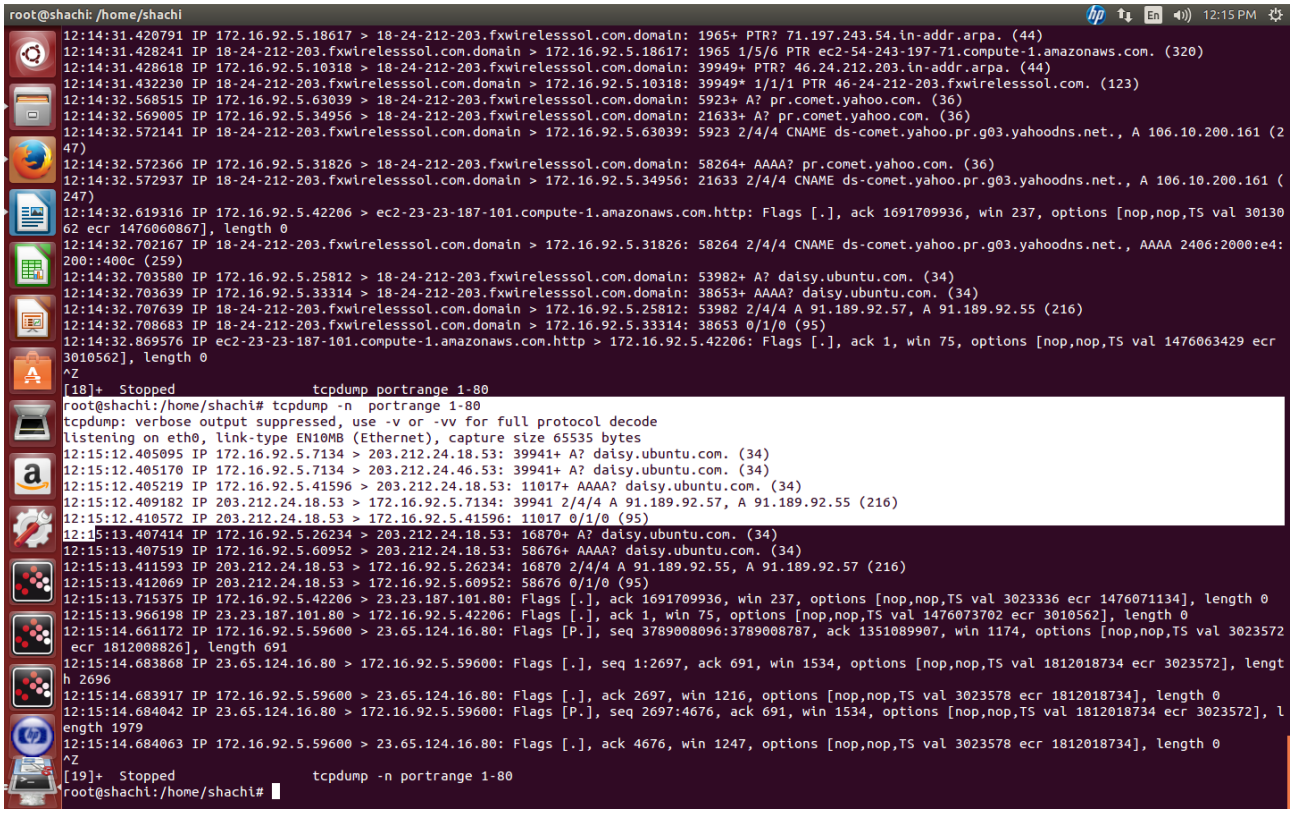
```
# tcpdump udp and src port 53
```



observing packets within a specific port range

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

It shows all packets whose source or destination port is between 1 to 80



#tcpdump -n src port 443