

Name : Yash kanojia

Roll no : 2018372

## ASSIGNMENT-2

Ans 1) a)

```
TERMINAL  PROBLEMS  4  OUTPUT  DEBUG CONSOLE
yash@LAPTOP-JSHLQ76B:/mnt/c/Users/YASH_KANOJIA$ ifconfig -a
eth0: flags=64<RUNNING>  mtu 1500
    inet 169.254.65.1  netmask 255.255.0.0
    inet6 fe80::2454:ed65:bbd7:4101  prefixlen 64  scopeid 0xfd<compat,link,site,host>
    ether 24:ee:9a:8c:ad:ba  (Ethernet)
    RX packets 0  bytes 0 (0.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 0  bytes 0 (0.0 B)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=64<RUNNING>  mtu 1500
    inet 169.254.77.237  netmask 255.255.0.0
    inet6 fe80::cd51:6547:91c6:4ded  prefixlen 64  scopeid 0xfd<compat,link,site,host>
    ether 00:09:0f:fe:00:01  (Ethernet)
    RX packets 0  bytes 0 (0.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 0  bytes 0 (0.0 B)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth2: flags=64<RUNNING>  mtu 1392
    inet 169.254.10.169  netmask 255.255.0.0
    inet6 fe80::9c1c:3486:2df8:aa9  prefixlen 64  scopeid 0xfd<compat,link,site,host>
    ether 00:09:0f:aa:00:01  (Ethernet)
    RX packets 0  bytes 0 (0.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 0  bytes 0 (0.0 B)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 1500
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0xfe<compat,link,site,host>
    loop (Local Loopback)
    RX packets 0  bytes 0 (0.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 0  bytes 0 (0.0 B)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Ifconfig -a shows the ip in the above ss of network interface.

b)

---

**My Public IPv4 is: 43.225.0.41**

My Public IPv6 is: Not Detected

Location: Delhi, DL IN ?

ISP: True Broadband Service

[My IP Information](#)

[IP Address Lookup](#)

Yes, both IP addresses are different. IP address shown by whatmyip is the public IP address or external IP address and the internal IP address which starts with (192.168..) are not the public IP addresses these are reserved IP address or internal IP addresses.

Ans 2 a) Network latency when sending ping to [www.google.com](http://www.google.com) is 15.689 ms (milliseconds) it is the delay when the packet is sent (PING) and response is received (PONG).

```
yashkanojia@yashkanojia-VirtualBox:~$ ping -c 5 google.com
PING google.com (172.217.166.206) 56(84) bytes of data:
64 bytes from del03s13-in-f14.1e100.net (172.217.166.206): icmp_seq=1 ttl=118 t
ime=25.2 ms
64 bytes from del03s13-in-f14.1e100.net (172.217.166.206): icmp_seq=2 ttl=118 t
ime=22.2 ms
64 bytes from del03s13-in-f14.1e100.net (172.217.166.206): icmp_seq=3 ttl=118 t
ime=11.3 ms
64 bytes from del03s13-in-f14.1e100.net (172.217.166.206): icmp_seq=4 ttl=118 t
ime=9.51 ms
64 bytes from del03s13-in-f14.1e100.net (172.217.166.206): icmp_seq=5 ttl=118 t
ime=10.1 ms

--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 9.512/15.689/25.215/6.658 ms
yashkanojia@yashkanojia-VirtualBox:~$
```

b)

```
yash@LAPTOP-JSHLQ76B:/mnt/c/Users/YASH KANOJIA/Desktop/cn/hw_2$ python3 file.py
90 percentile 24.080000000000002
99 percentile 60.441999999999995
median 7.95
yash@LAPTOP-JSHLQ76B:/mnt/c/Users/YASH KANOJIA/Desktop/cn/hw_2$
```

To do this question I had written a small python file ,In which using the “subprocess” run() function I run the command to send the 100 ping to the my other device and save the output of the above command in the “ouput.txt” file then I read the data of the file line by line and extract the time column in the list.To find the 90 percentile, 99 percentile and median I had used the percentile and median function of numpy and displays the output.

c)

```
yash@LAPTOP-JSHLQ76B:/mnt/c/Users/YASH KANOJIA/Desktop/cn/hw_2$ python3 file.py
90 percentile 490.39999999999999
99 percentile 688.74000000000004
median 346.5
yash@LAPTOP-JSHLQ76B:/mnt/c/Users/YASH KANOJIA/Desktop/cn/hw_2$
```

To do this question I had written a small python file ,In which using the “subprocess” run() function I run the command to send the 100 ping to the my other device and save the output of the above command in the “amazon.txt” file then I read the data of the file line by line and extract the time column in the list.To find the 90 percentile, 99 percentile and median I had used the percentile and median function of numpy and displays the output.

d) when sending ping to Amazon.com 2% packet got loss (2 packets) and when sending the ping to the device connected on the same network as I 1% packet got loss(1 packet).when sending the ping to the amazon.com more number of packets got drop and at the same time amazon.com has high latency.It means it was taking a longer time to response(PONG) to the packet that I send as compare to the other device that is connected to my network.It was taking a longer time because the Amazon server to whom I am sending the ping is far away from me as compare to other device on my network.so,distance is the factor causing the high ping.

Ans 3)a)

```

C:\Users\YASH KANOJIA>ping -f -l 2000 google.com

Pinging google.com [172.217.160.238] with 2000 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 172.217.160.238:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\YASH KANOJIA>ping -f -l 1200 google.com

Pinging google.com [172.217.160.238] with 1200 bytes of data:
Reply from 172.217.160.238: bytes=68 (sent 1200) time=8ms TTL=119
Reply from 172.217.160.238: bytes=68 (sent 1200) time=7ms TTL=119
Reply from 172.217.160.238: bytes=68 (sent 1200) time=5ms TTL=119
Reply from 172.217.160.238: bytes=68 (sent 1200) time=5ms TTL=119

Ping statistics for 172.217.160.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 8ms, Average = 6ms

```

When we send the packet of mtu 2000 then it shows the message that “Message too long” this is because the default MTU setting has 1500 MTU in this 1500 mtu we need to leave the space for the header and IP addresses. but here we are not leaving any space. so, it will not send the packet because its maximum transmission unit (MTU) is greater than 1500. One thing to note that here we are sending without fragmentation that’s why it is not sending but if we do the fragmentation then it will send the packet.



```

yash@LAPTOP-JSHLQ76B:/mnt/c/Users/YASH KANOJIA$ ifconfig -a
eth0: flags=64<RUNNING> mtu 1500
    inet 169.254.65.1 netmask 255.255.0.0
    inet6 fe80::2454:ed65:bbd7:4101 prefixlen 64 scopeid 0xfd<compat,link,site,host>
    ether 24:ee:9a:8c:ad:ba (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=64<RUNNING> mtu 1500
    inet 169.254.77.237 netmask 255.255.0.0
    inet6 fe80::cd51:6547:91c6:4ded prefixlen 64 scopeid 0xfd<compat,link,site,host>
    ether 00:09:0f:fe:00:01 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth2: flags=64<RUNNING> mtu 1392
    inet 169.254.10.169 netmask 255.255.0.0
    inet6 fe80::9c1c:3486:2df8:aa9 prefixlen 64 scopeid 0xfd<compat,link,site,host>
    ether 00:09:0f:aa:00:01 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 1500
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0xfe<compat,link,site,host>
    loop (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
  
```

b)

```
C:\Users\YASH KANOJIA>netstat -n -o -p tcp
```

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	127.0.0.1:49671	127.0.0.1:49672	ESTABLISHED	6472
TCP	127.0.0.1:49672	127.0.0.1:49671	ESTABLISHED	6472
TCP	192.168.0.107:58567	52.177.166.224:443	ESTABLISHED	15156
TCP	192.168.0.107:58575	52.177.166.224:443	ESTABLISHED	5512
TCP	192.168.0.107:58708	34.251.141.125:8282	ESTABLISHED	17796
TCP	192.168.0.107:58716	74.125.24.188:5228	ESTABLISHED	17796
TCP	192.168.0.107:61698	35.244.159.8:443	ESTABLISHED	17796
TCP	192.168.0.107:61740	216.58.221.51:443	ESTABLISHED	17796
TCP	192.168.0.107:61798	151.101.2.133:443	ESTABLISHED	17796
TCP	192.168.0.107:61805	23.200.234.147:443	ESTABLISHED	17796
TCP	192.168.0.107:61808	185.184.8.30:443	ESTABLISHED	17796
TCP	192.168.0.107:61809	161.69.226.72:443	CLOSE_WAIT	17796
TCP	192.168.0.107:61836	199.232.192.134:443	ESTABLISHED	17796
TCP	192.168.0.107:61847	23.58.72.45:443	ESTABLISHED	17796
TCP	192.168.0.107:61848	23.58.72.45:443	ESTABLISHED	17796
TCP	192.168.0.107:61864	151.101.2.165:443	ESTABLISHED	17796
TCP	192.168.0.107:61865	104.121.242.77:443	TIME_WAIT	0
TCP	192.168.0.107:61866	13.35.131.92:443	ESTABLISHED	17796
TCP	192.168.0.107:61868	99.86.49.170:443	ESTABLISHED	17796
TCP	192.168.0.107:61869	99.86.42.34:443	ESTABLISHED	17796
TCP	192.168.0.107:61870	23.111.9.35:443	ESTABLISHED	17796
TCP	192.168.0.107:61871	2.18.13.39:443	CLOSE_WAIT	17796
TCP	192.168.0.107:61872	99.84.144.120:443	ESTABLISHED	17796
TCP	192.168.0.107:61874	99.86.42.48:443	ESTABLISHED	17796
TCP	192.168.0.107:61875	99.84.144.73:443	ESTABLISHED	17796
TCP	192.168.0.107:61876	23.54.89.35:443	ESTABLISHED	17796
TCP	192.168.0.107:61877	23.54.89.117:443	ESTABLISHED	17796
TCP	192.168.0.107:61879	13.35.191.91:443	ESTABLISHED	17796
TCP	192.168.0.107:61881	104.19.150.54:443	ESTABLISHED	17796
TCP	192.168.0.107:61883	13.35.191.91:443	ESTABLISHED	17796
TCP	192.168.0.107:61884	13.35.191.40:443	ESTABLISHED	17796
TCP	192.168.0.107:61886	52.52.244.32:443	CLOSE_WAIT	17796
TCP	192.168.0.107:61887	23.54.89.141:443	TIME_WAIT	0
TCP	192.168.0.107:61888	104.19.150.54:443	ESTABLISHED	17796
TCP	192.168.0.107:61890	54.227.255.202:443	CLOSE_WAIT	17796



TCP	192.168.0.107:61890	54.227.255.202:443	CLOSE_WAIT	17796
TCP	192.168.0.107:61893	99.86.42.129:443	ESTABLISHED	17796
TCP	192.168.0.107:61894	52.201.97.1:443	CLOSE_WAIT	17796
TCP	192.168.0.107:61895	172.67.190.104:443	ESTABLISHED	17796
TCP	192.168.0.107:61896	151.101.2.110:443	ESTABLISHED	17796
TCP	192.168.0.107:61898	52.201.97.1:443	CLOSE_WAIT	17796
TCP	192.168.0.107:61901	13.35.191.49:443	ESTABLISHED	17796
TCP	192.168.0.107:61903	64.38.119.27:443	ESTABLISHED	17796
TCP	192.168.0.107:61904	103.229.206.182:443	ESTABLISHED	17796
TCP	192.168.0.107:61906	52.36.181.52:443	CLOSE_WAIT	17796
TCP	192.168.0.107:61907	172.67.36.86:443	ESTABLISHED	17796
TCP	192.168.0.107:61908	23.54.89.35:443	ESTABLISHED	17796
TCP	192.168.0.107:61910	23.54.89.215:443	ESTABLISHED	17796
TCP	192.168.0.107:61911	34.107.254.252:443	ESTABLISHED	17796
TCP	192.168.0.107:61912	52.36.181.52:443	CLOSE_WAIT	17796
TCP	192.168.0.107:61914	64.38.119.27:443	ESTABLISHED	17796
TCP	192.168.0.107:61915	99.86.42.34:443	ESTABLISHED	17796
TCP	192.168.0.107:61916	3.221.33.53:443	CLOSE_WAIT	17796
TCP	192.168.0.107:61918	151.101.2.114:443	ESTABLISHED	17796
TCP	192.168.0.107:61919	99.84.144.17:443	ESTABLISHED	17796
TCP	192.168.0.107:61920	151.101.1.140:443	ESTABLISHED	17796
TCP	192.168.0.107:61921	151.101.8.157:443	ESTABLISHED	17796
TCP	192.168.0.107:61922	152.195.62.252:443	ESTABLISHED	17796
TCP	192.168.0.107:61924	3.221.33.53:443	CLOSE_WAIT	17796
TCP	192.168.0.107:61927	151.101.1.140:443	ESTABLISHED	17796
TCP	192.168.0.107:61930	103.231.98.194:443	ESTABLISHED	17796
TCP	192.168.0.107:61931	104.244.42.3:443	ESTABLISHED	17796
TCP	192.168.0.107:61937	104.244.42.5:443	ESTABLISHED	17796
TCP	192.168.0.107:61938	69.173.159.48:443	ESTABLISHED	17796
TCP	192.168.0.107:61940	69.173.159.48:443	ESTABLISHED	17796
TCP	192.168.0.107:61941	69.173.159.48:443	ESTABLISHED	17796
TCP	192.168.0.107:61942	23.215.194.118:443	ESTABLISHED	17796
TCP	192.168.0.107:61950	52.201.97.1:443	CLOSE_WAIT	17796
TCP	192.168.0.107:61951	151.101.2.2:443	ESTABLISHED	17796
TCP	192.168.0.107:61952	54.227.255.202:443	CLOSE_WAIT	17796
TCP	192.168.0.107:61954	23.54.89.35:443	ESTABLISHED	17796
TCP	192.168.0.107:61955	182.161.72.130:443	TIME_WAIT	0
TCP	192.168.0.107:61956	34.200.115.102:443	CLOSE_WAIT	17796
TCP	192.168.0.107:61957	34.107.254.252:443	ESTABLISHED	17796
TCP	192.168.0.107:61961	23.54.89.35:443	ESTABLISHED	17796
TCP	192.168.0.107:61962	172.217.166.1:443	ESTABLISHED	17796

```

TCP    192.168.0.107:61957    34.107.254.252:443    ESTABLISHED    17796
TCP    192.168.0.107:61961    23.54.89.35:443       ESTABLISHED    17796
TCP    192.168.0.107:61962    172.217.166.1:443     ESTABLISHED    17796
TCP    192.168.0.107:61964    151.101.2.114:443     ESTABLISHED    17796
TCP    192.168.0.107:61968    23.54.89.253:443      TIME_WAIT      0
TCP    192.168.0.107:61975    54.243.123.94:443     CLOSE_WAIT     17796
TCP    192.168.0.107:61976    54.243.123.94:443     CLOSE_WAIT     17796
TCP    192.168.0.107:61977    54.243.123.94:443     CLOSE_WAIT     17796
TCP    192.168.0.107:61982    35.186.224.25:443     TIME_WAIT      0
TCP    192.168.0.107:61988    104.20.19.53:443      ESTABLISHED    17796
TCP    192.168.0.107:61989    52.203.65.22:443      CLOSE_WAIT     17796
TCP    192.168.0.107:61990    172.217.167.10:443    ESTABLISHED    17796
TCP    192.168.0.107:61993    161.69.226.73:443     CLOSE_WAIT     17796
TCP    192.168.0.107:61994    161.69.226.73:443     CLOSE_WAIT     17796
TCP    192.168.0.107:61995    35.227.202.26:443     ESTABLISHED    17796
TCP    192.168.0.107:61996    103.231.98.196:443    ESTABLISHED    17796
TCP    192.168.0.107:61998    103.229.10.173:443    ESTABLISHED    17796
TCP    192.168.0.107:62001    103.231.98.196:443    ESTABLISHED    17796
TCP    192.168.0.107:62003    35.227.252.103:443    ESTABLISHED    17796
TCP    192.168.0.107:62006    13.35.191.64:443      ESTABLISHED    17796
TCP    192.168.0.107:62007    103.231.98.196:443    ESTABLISHED    17796
TCP    192.168.0.107:62009    23.54.89.35:443       ESTABLISHED    17796
TCP    192.168.0.107:62011    54.190.202.24:443     CLOSE_WAIT     17796
TCP    192.168.0.107:62013    13.114.132.45:443     CLOSE_WAIT     17796
TCP    192.168.0.107:62020    192.168.0.102:8009    ESTABLISHED    17796
TCP    192.168.0.107:62023    192.168.0.102:8008    ESTABLISHED    17796

```

```
:\Users\YASH KANOJIA>
```

command used is : “netstat -p tcp -n -o”

where “net” in netstat stands for network

“stat” in netstat stands for statistics

-p : tells netstat to display all the active connections of tcp.

-n : tells to display only the port number and the IP address in the numbers or numerical value.

-O: tells to display the PID.



Ans 4) a)

```
yashkanojia@yashkanojia-VirtualBox:~$ nslookup -type=SOA google.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
google.com
  origin = ns1.google.com
  mail addr = dns-admin.google.com
  serial = 333039439
  refresh = 900
  retry = 900
  expire = 1800
  minimum = 60

Authoritative answers can be found from:

yashkanojia@yashkanojia-VirtualBox:~$ nslookup google.com ns1.google.com
Server:      ns1.google.com
Address:     216.239.32.10#53

Name:   google.com
Address: 172.217.167.46
Name:   google.com
Address: 2404:6800:4002:80b::200e
```

It may be possible that when we are looking for the authoritative server name the nslookup query will provide the result which is not obtained by the authoritative server the result return is obtained by the server Which stores the cached copy of the of the DNS record.so,to find the authoritative result we need to run nslookup again on origin.Here, SOA stands for (Starts of authority) it helps fetch the authoritative information about the domain.

b)

```

yashkanojia@yashkanojia-VirtualBox:~$ nslookup -type=SOA google.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
google.com
  origin = ns1.google.com
  mail addr = dns-admin.google.com
  serial = 333039439
  refresh = 900
  retry = 900
  expire = 1800
  minimum = 60

Authoritative answers can be found from:

yashkanojia@yashkanojia-VirtualBox:~$ nslookup google.com ns1.google.com
Server:      ns1.google.com
Address:     216.239.32.10#53

Name:   google.com
Address: 172.217.167.46
Name:   google.com
Address: 2404:6800:4002:80b::200e

```

In the output of this command we can see the answer where it has mentioned the refresh time as 900 seconds for google.com in the local DNS cache it means that after 900 seconds it will be removed from the local DNS cache. It is the time at which the secondary servers refresh the files which came from the primary servers.

Ans 3) a)

```

yashkanojia@yashkanojia-VirtualBox:~$ traceroute -I -z 12345 google.com
traceroute to google.com (172.217.160.238), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.845 ms  1.016 ms  0.495 ms
 2  192.168.0.1 (192.168.0.1)  5.988 ms  5.285 ms  8.484 ms
 3  172.28.135.1 (172.28.135.1)  6.732 ms  11.304 ms  6.043 ms
 4  103.139.60.1 (103.139.60.1)  7.537 ms  7.645 ms  6.217 ms
 5  10.100.8.37 (10.100.8.37)  13.936 ms  26.411 ms  7.237 ms
 6  72.14.205.145 (72.14.205.145)  5.283 ms  11.595 ms  7.719 ms
 7  108.170.251.97 (108.170.251.97)  10.384 ms  6.448 ms  6.046 ms
 8  64.233.174.17 (64.233.174.17)  10.554 ms  8.534 ms  10.084 ms
 9  del03s09-in-f14.1e100.net (172.217.160.238)  9.075 ms  9.511 ms  5.803 ms
yashkanojia@yashkanojia-VirtualBox:~$

```

Traceroute “-z” is used to specify the time interval between each probe in milliseconds. Here we have set the time interval to 12345 milliseconds.

b)

```
yashkanojia@yashkanojia-VirtualBox:~$ traceroute -I -q 5 google.com
traceroute to google.com (172.217.166.238), 30 hops max, 60 byte packets
 1 _gateway (10.0.2.2) 1.396 ms 1.323 ms 1.292 ms 1.276 ms 1.262 ms
 2 192.168.0.1 (192.168.0.1) 8.100 ms * * * *
 3 * * * * *
 4 * 103.139.60.1 (103.139.60.1) 5.245 ms 5.692 ms 6.749 ms 7.458 ms
 5 10.100.8.37 (10.100.8.37) 7.949 ms 5.010 ms 5.469 ms 5.446 ms *
 6 72.14.205.145 (72.14.205.145) 5.574 ms 7.800 ms 9.193 ms 9.356 ms 9.35
0 ms
 7 108.170.251.97 (108.170.251.97) 9.488 ms 5.253 ms 4.819 ms 5.746 ms 5.
722 ms
 8 72.14.232.57 (72.14.232.57) 5.251 ms 6.148 ms 7.110 ms 7.129 ms 7.123
ms
 9 del03s14-in-f14.1e100.net (172.217.166.238) 7.263 ms 7.397 ms 7.523 ms
7.665 ms 4.656 ms
yashkanojia@yashkanojia-VirtualBox:~$
```

Traceroute “-q” option is used to specify the number of probes that you want to send. here as per question we have set it to the 5 probes.

c)

```
yashkanojia@yashkanojia-VirtualBox:~$ traceroute -I -m 7 -f 4 google.com
traceroute to google.com (172.217.166.238), 7 hops max, 60 byte packets
 4 103.139.60.1 (103.139.60.1) 7.411 ms 7.376 ms 13.537 ms
 5 10.100.8.37 (10.100.8.37) 6.567 ms 6.856 ms 13.807 ms
 6 72.14.205.145 (72.14.205.145) 14.119 ms 14.941 ms 15.081 ms
 7 108.170.251.97 (108.170.251.97) 15.245 ms 15.242 ms 15.485 ms
yashkanojia@yashkanojia-VirtualBox:~$
```

I started a traceroute of the hops from the 4<sup>th</sup> one and I limited the hops to 7 hops. so, it will only go from 4<sup>th</sup> router to 7<sup>th</sup> router.

Traceroute “-m” use specify the max hop.

Traceroute “-f” use to specify the first hop from where we have start.



Ans 5)

```
yashkanojia@yashkanojia-VirtualBox:~$ sudo ifconfig lo down
yashkanojia@yashkanojia-VirtualBox:~$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::7f41:cbb:c4d4:253c prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:7d:ee:fa txqueuelen 1000 (Ethernet)
    RX packets 1914 bytes 2178850 (2.1 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 643 bytes 62376 (62.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=8<LOOPBACK> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 246 bytes 21387 (21.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 246 bytes 21387 (21.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

yashkanojia@yashkanojia-VirtualBox:~$ ping -c 10 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.

--- 127.0.0.1 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9219ms
```

All the ping send to 127.0.0.1 is received by lo(loop back) but when we down this interface using “sudo ifconfig lo down” this lo will no longer respond to anything send to him.that’s why when we down the lo and then send the ping all the ping will get drop.

Ans 6)

```

yashkanojia@yashkanojia-VirtualBox:~$ dig +short google.com
216.58.196.206
yashkanojia@yashkanojia-VirtualBox:~$ dig -x 216.58.196.206

; <<>> DiG 9.16.1-Ubuntu <<>> -x 216.58.196.206
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62993
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;206.196.58.216.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
206.196.58.216.in-addr.arpa. 3249 IN     PTR     del03s06-in-f14.1e100.net.
206.196.58.216.in-addr.arpa. 3249 IN     PTR     kul06s14-in-f206.1e100.net.

;; Query time: 23 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Wed Sep 23 22:22:07 IST 2020
;; MSG SIZE rcvd: 126

yashkanojia@yashkanojia-VirtualBox:~$ █

```

Reverse DNS is the opposite of the DNS. Here we have performed reverse dns. Reverse DNS is used to find the hostname from the IP address which is just opposite of the DNS. "dig -x domain ip" here -x is just a shortcut for reverse lookup. dig is the domain information groper used to display information. It works by sending the query to the name server.