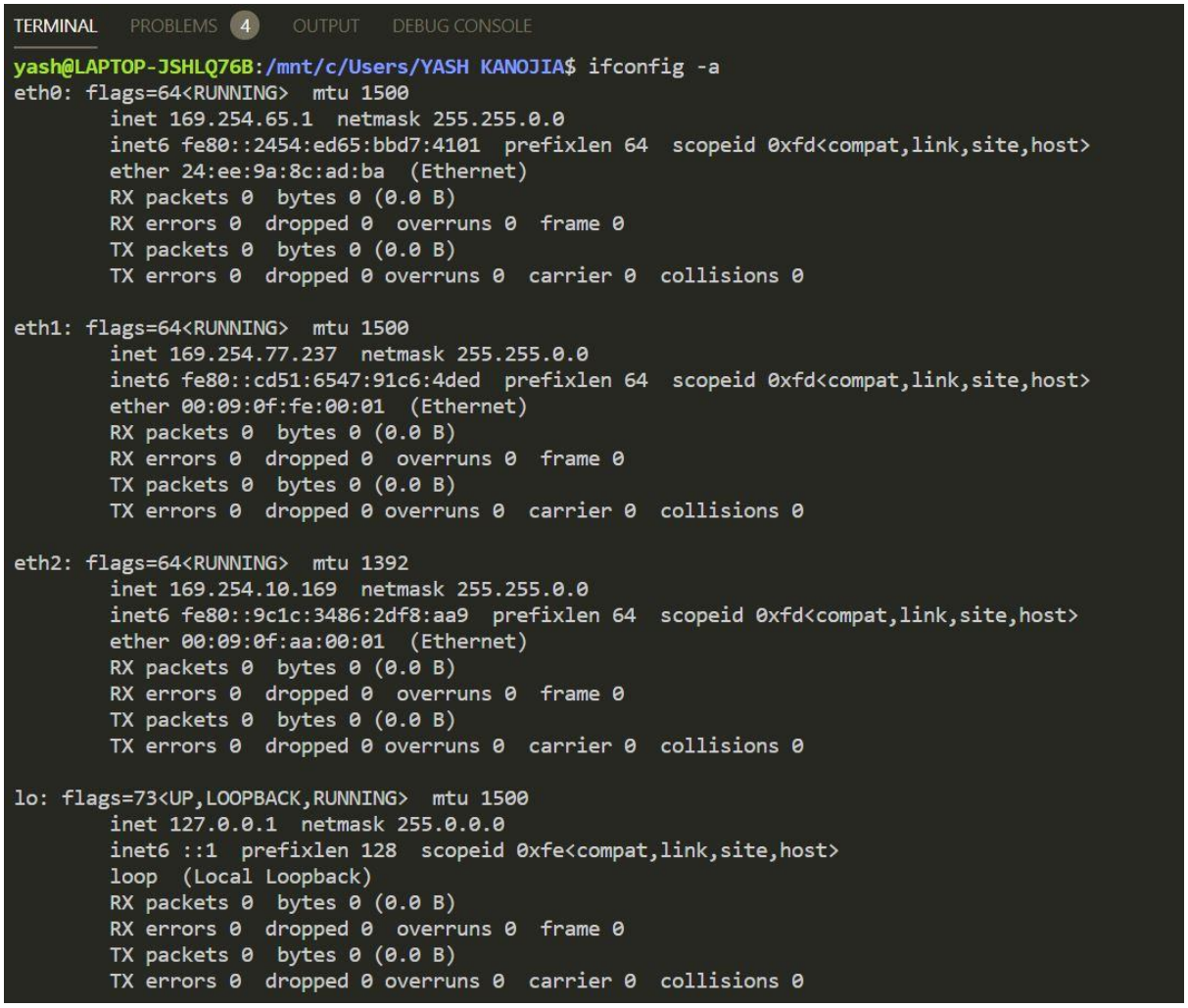
Name : Yash kanojia

Roll no : 2018372

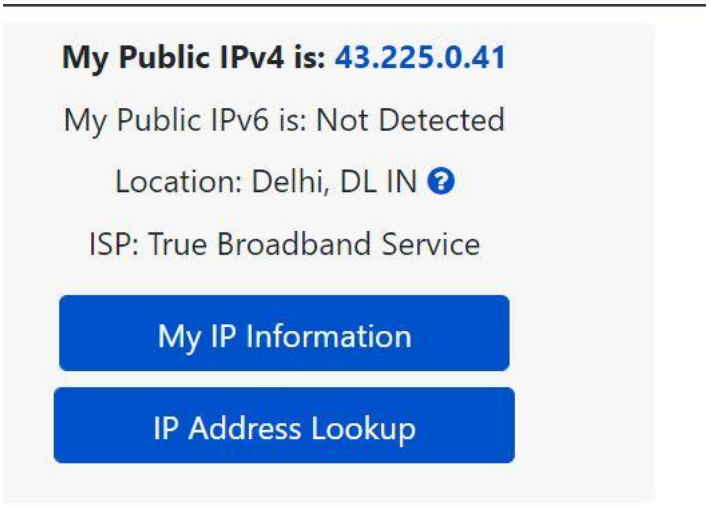
ASSIGNMENT-2

Ans 1) a)



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

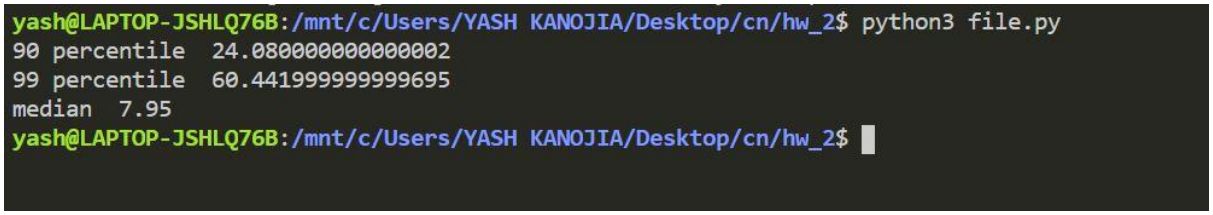
b)



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 strarts with(192.168..) are not the public Id addresses these are reserved Ip address or internal IP adresses.

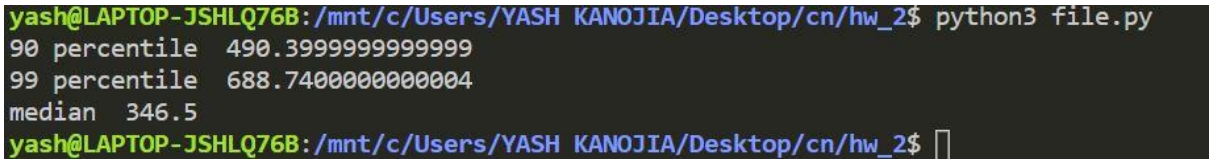
Ans 2 a) Network latency when sending ping to www.google.com is 15.689 ms(milliseconds) it is the delay when the packet is sended (PING) and reponse is received(PONG).

b)



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.

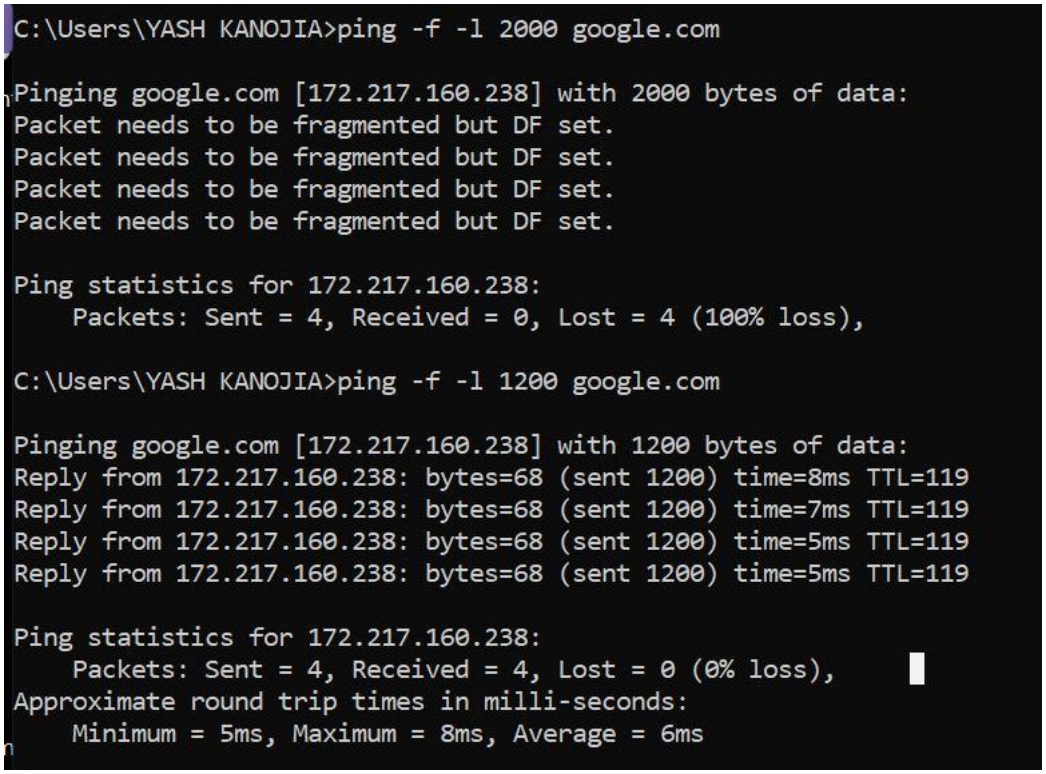
c)



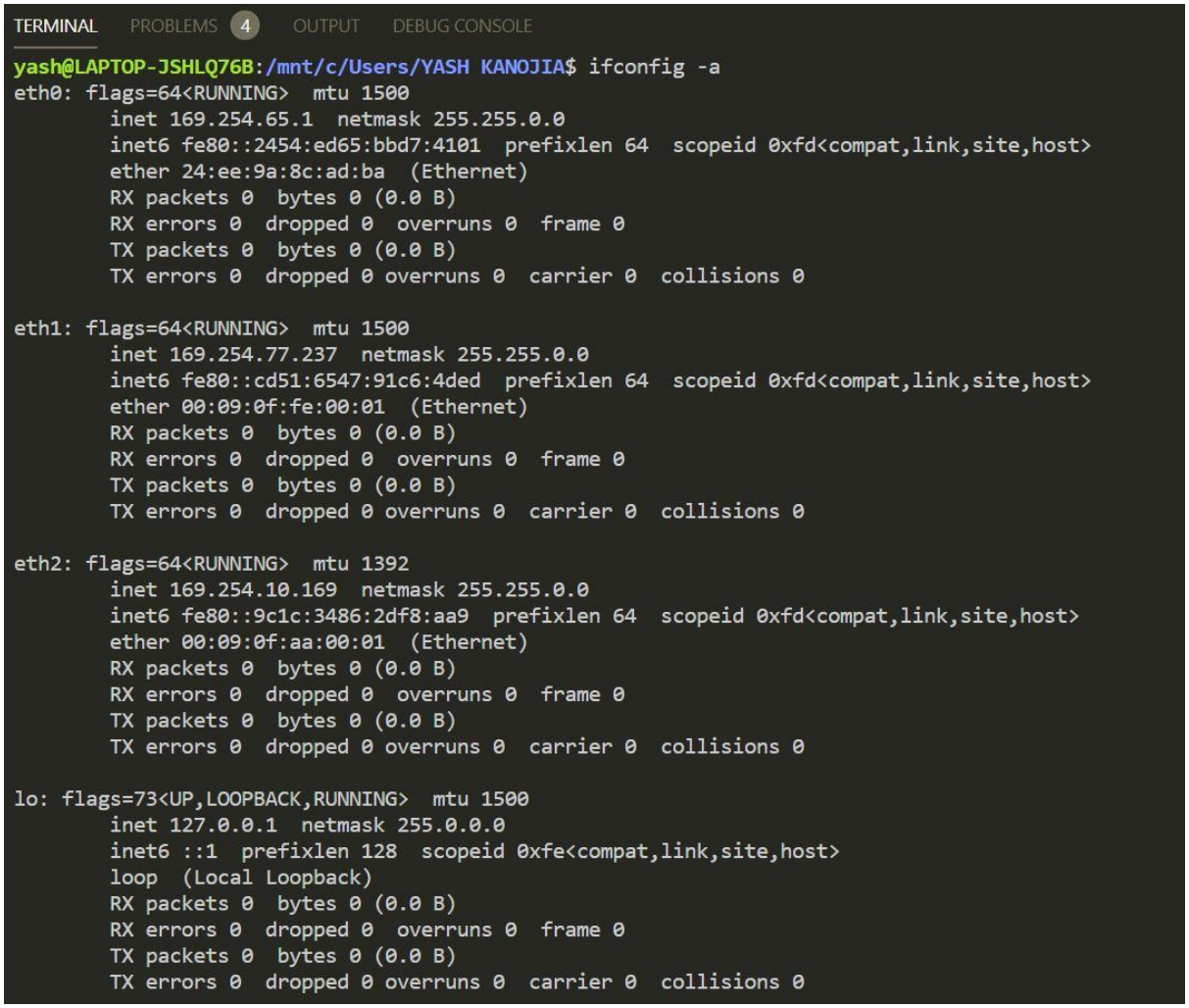
To do this question I had written a small python file ,In which using the "subprocess" run() function I run the command to send the 100 ping to the my other device and save the output of the above command in the "amazon.txt" file then I read the data of the file line by line and extract the time column 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 sended 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)



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 then 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.


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

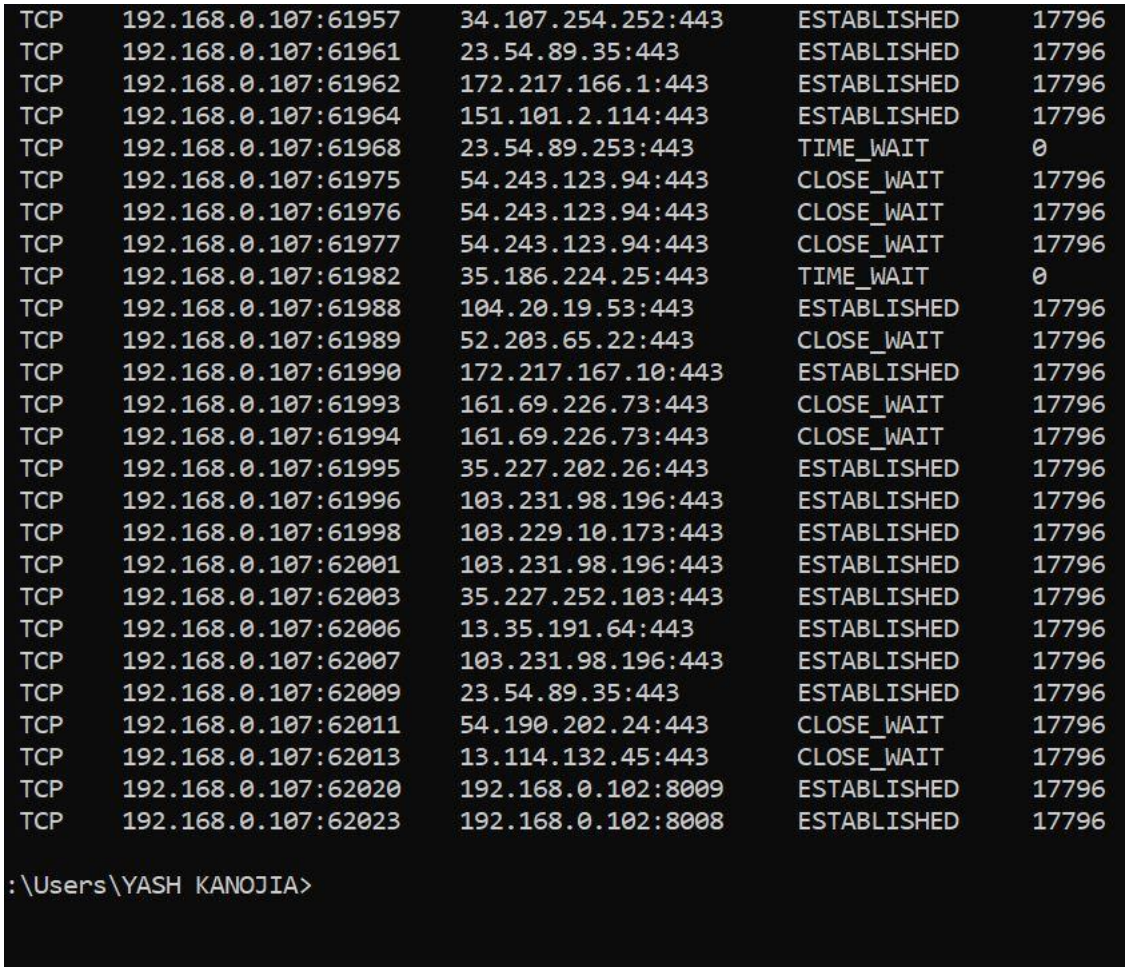
b)

```
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
```



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

where “net” in netstat stands for network

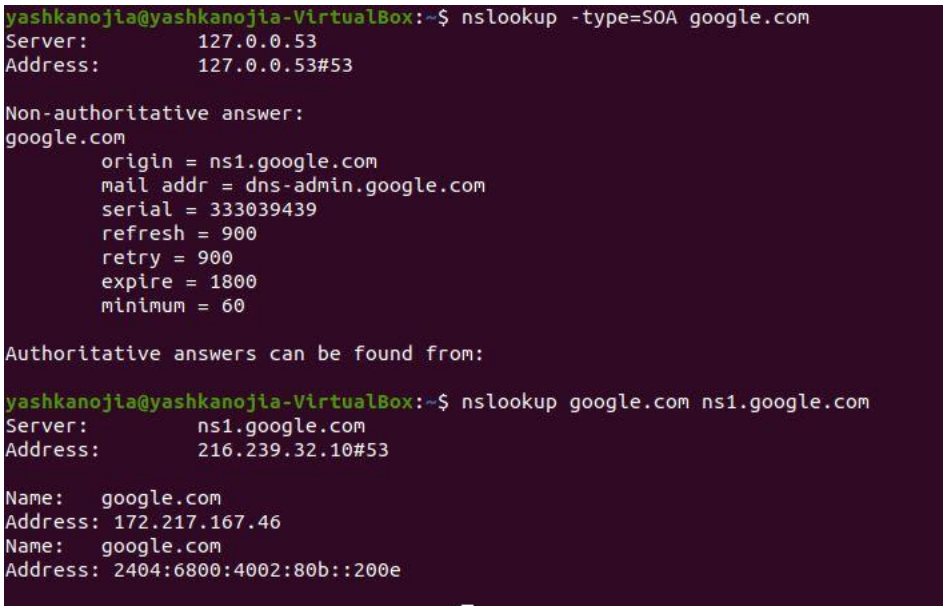
“stat” in netstat stands for statistics

-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.

-0: tells to display the PID.

Ans 4) a)



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
```

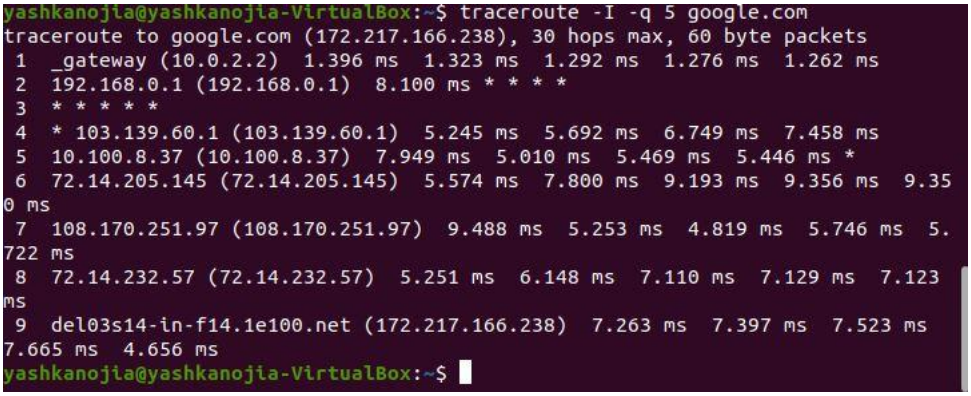
In the output of this command we can see the answer were it has mentioned the refresh time as 900 seconds for google.com in the local DNS cache it means that after 900 seconds it will be removed from the local Dns cache.It is the time at which the secondary servers refersh the files which came from the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

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:~$
```

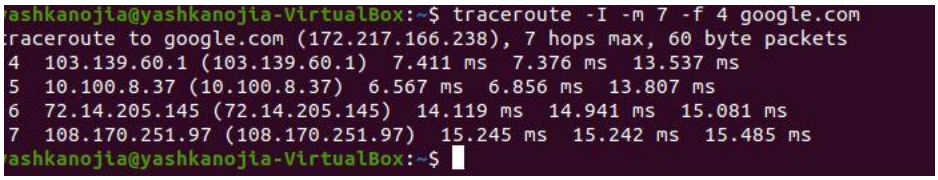
Traceroute “-z” is used to specify the time interval between each probe in milliseconds.here we have set the time interval to 12345 milliseconds.

b)



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)

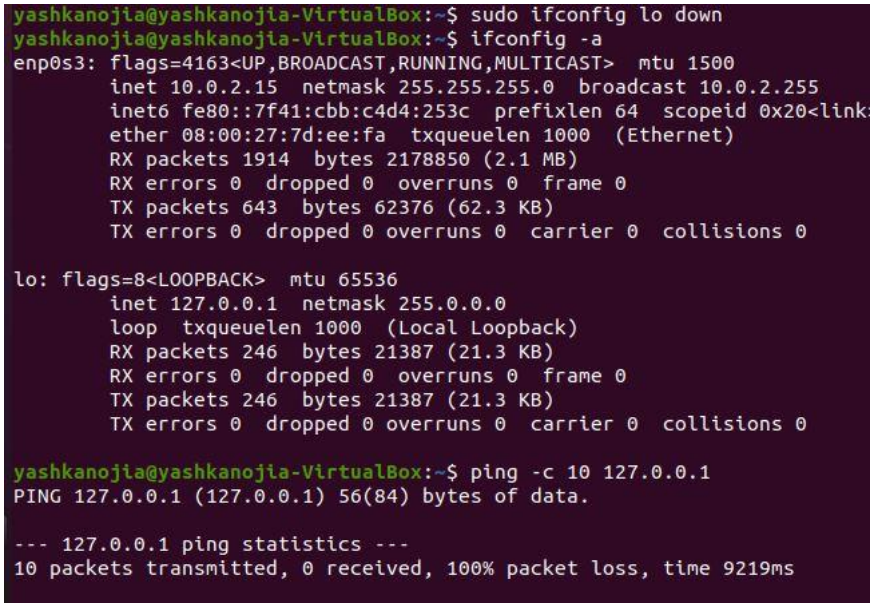


I started a traceroute of the hops from the 4th one and I limited the hops to 7 hops.so,it will only go from 4th router to 7th router.

Traceroute “-m” use specify the max hop.

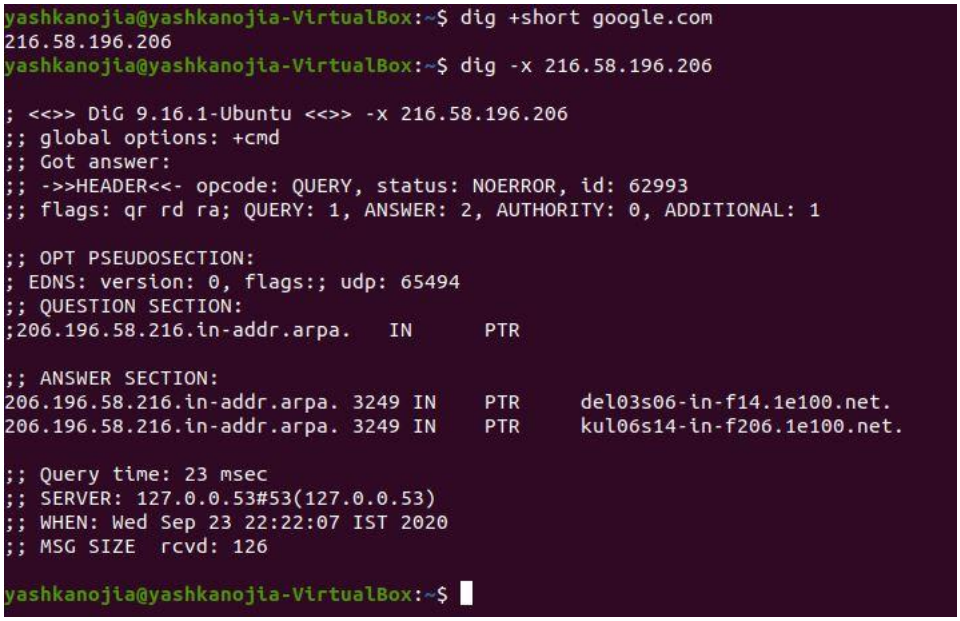
Traceroute “-f” use to specify the first hop from where we have start.

Ans 5)



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

Ans 6)



Reverse DNS is the opposite of the DNS.Here we have performed revrese 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.