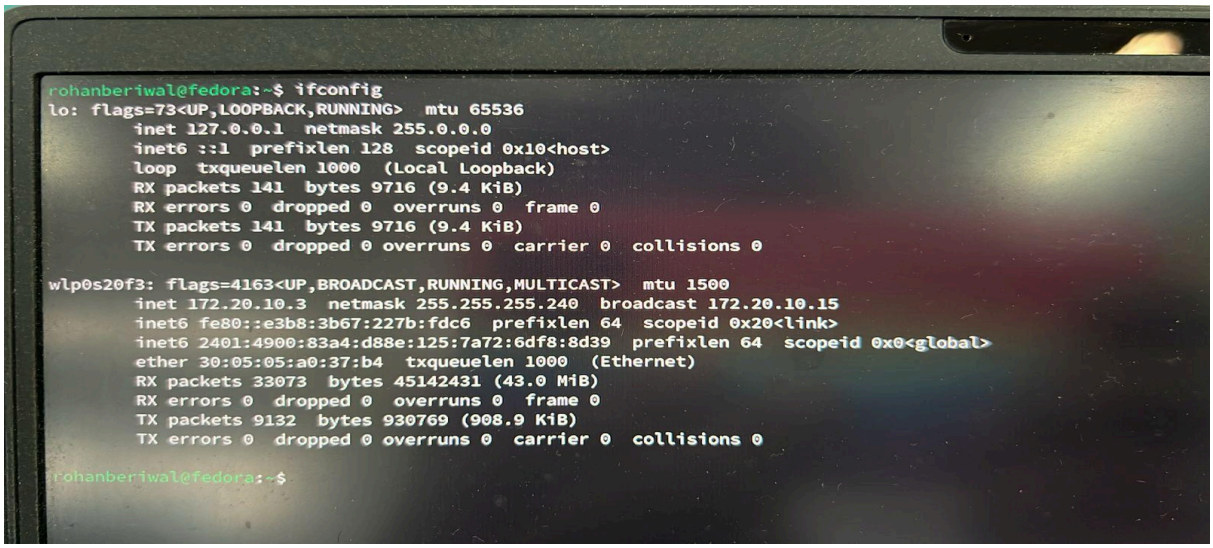
Computer Networks (CSE-232) Report
Programming Assignment -1
(Using command-line utilities for network debugging)

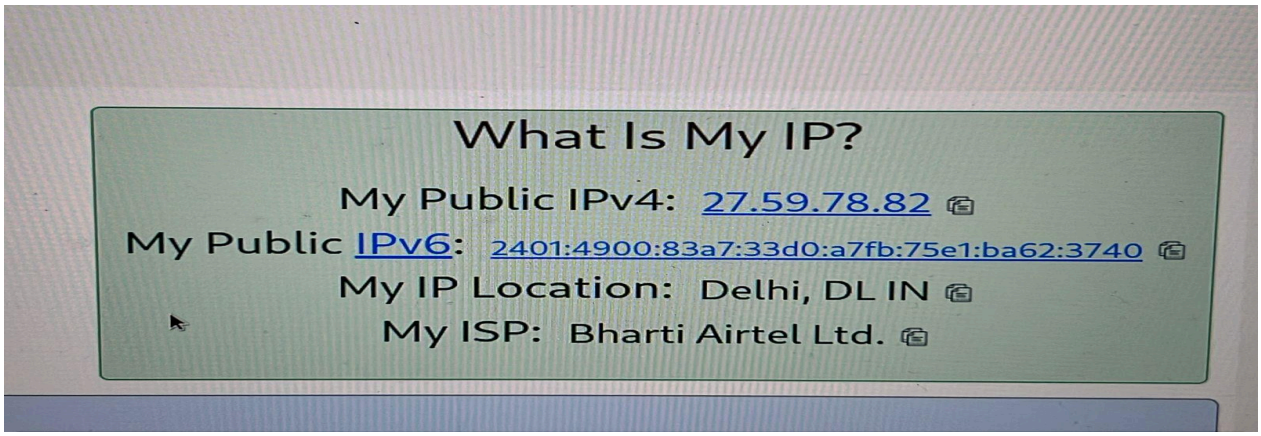
Name : Rohan Beriwal
Roll No : 2022413

Question 1.)
A)



Description :
ifconfig command : This command is used in Unix-like operating systems . This is used to display the network configurations of the machines . I used the Linux shell and used the **ifconfig** command to get the network output of my machines .The ip address of the machine is 172.20.10.3 as it is connected to a wireless interface (Wi-Fi) .

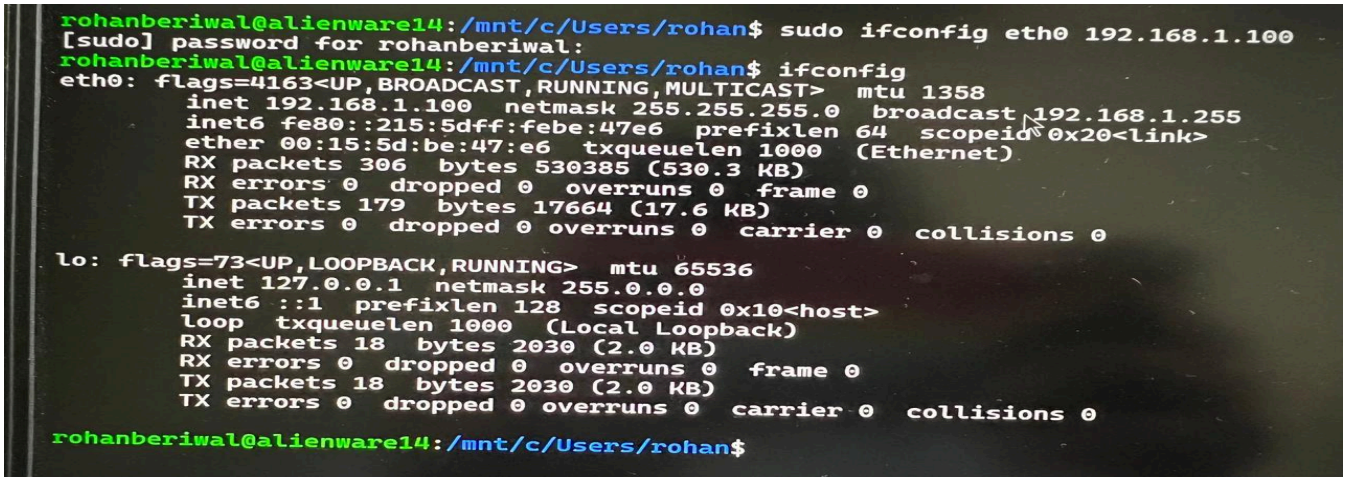
B)



No , the IP for the machine that was found using the **ifconfig command** on the machine and the IP on the website https://www.whatismyip.com are not the same .

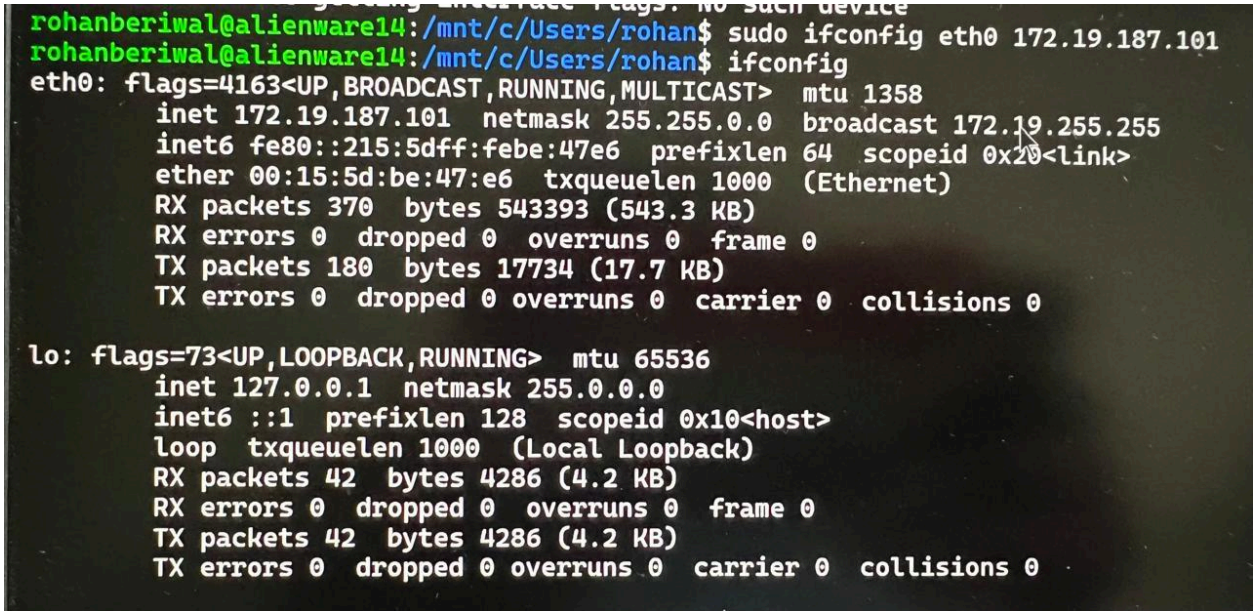
Reason of Different IP :
The IP on the machine found using the **ifconfig command** shows the IP is a private IP that is present in the local network and this IP is assigned using **Dynamic Host Configuration Protocol server (DHCPS)** while the IP present on the website is a IP assigned by the ISP(Internet service provider) and this is use to communicate over the Internet .

Question 2)
Changing IP to New IP :



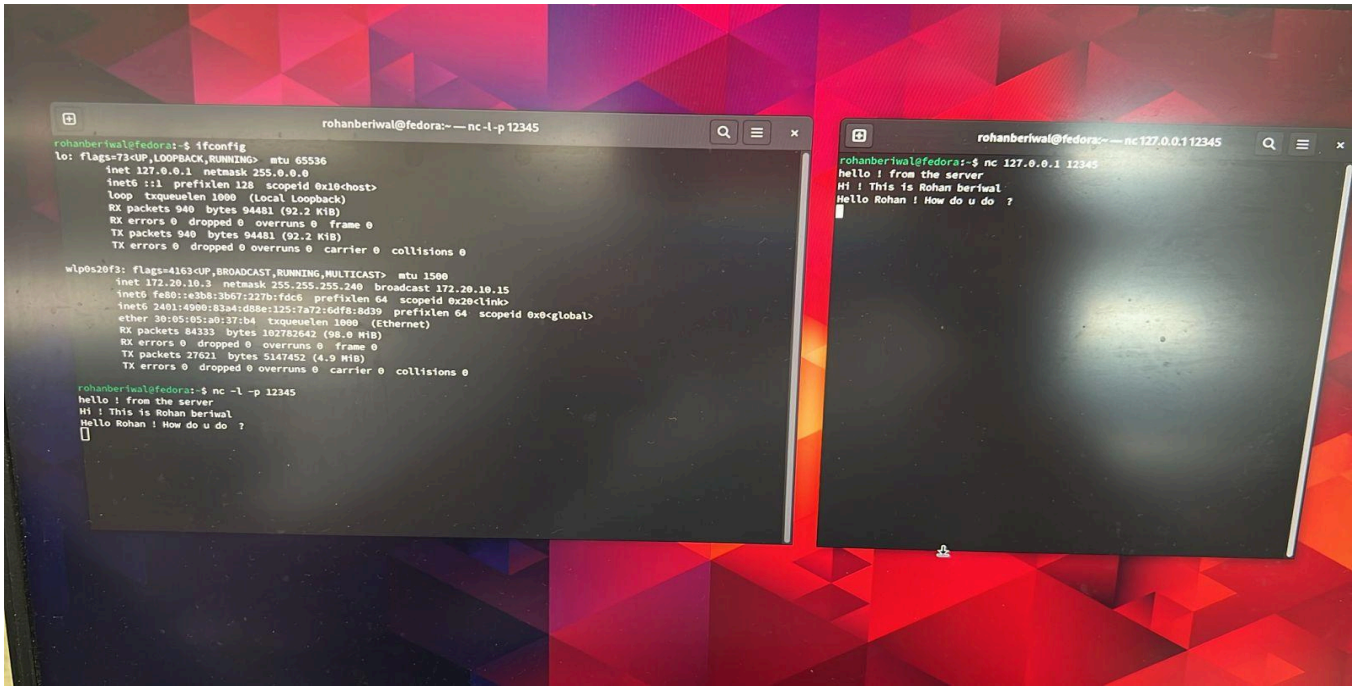
Description :
This screen Shot shows the IP address of the machine getting changed . I first used the Ifconfig **command to** get the Ip address of the machine and saved that IP address . I use the port eth0 to find the inet (172.19.187.101 in this case) which is the IP of the machine . Now to change the IP of the to some other desired address I used
sudo ifconfig eth0 <New_ip address> , I used a random IP address of 192.168.1.100 , I filled the password for the machine as my privilege was changed from the regular user to **"superuser do"(sudo / ~ root)** . Then , using the **ifconfig command** we can print the IP address that got changed .

Reverting the IP address back to Original :



Description :
After changing the IP address from 172.19.187.101 to 192.168.1.100 I used the same **sudo ifconfig eth0 172.19.187.101** here the IP address is the same IP that we had before .

Question3.)
A)



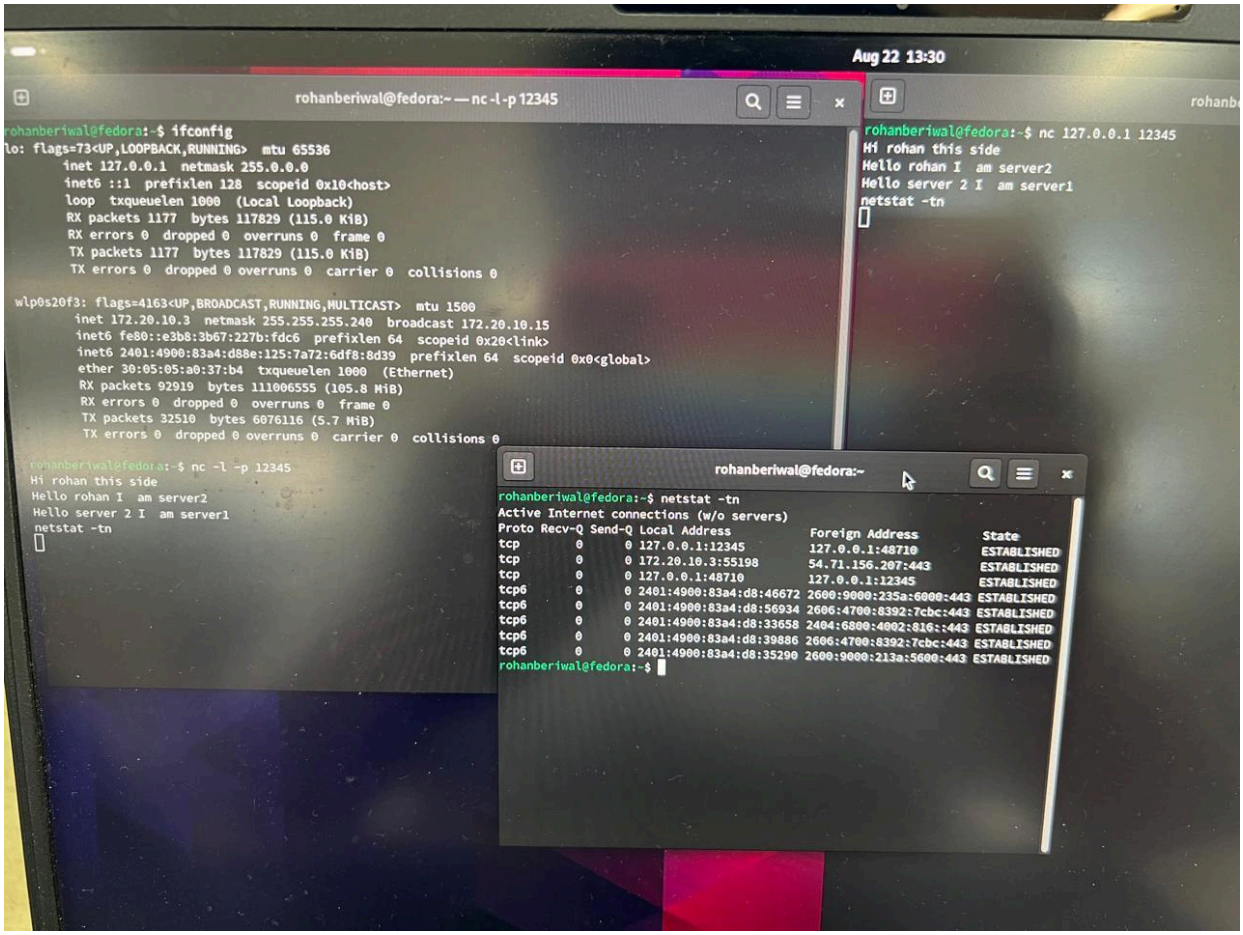
Description:
To Generate a connection between two machines we have to use the IP address to connect two machines for the TCP connections . I opened two different terminal windows . The left side being terminal 1 and right being terminal 2 now using Terminal 1 I found the IP address of the machine using the **ifconfig command** . Now i tried to establish a connection between terminal using the **nc -l -p 12345** .

The **nc** here stands for the **netcat** that is a tool for generating a connection between the two machines / two VMs or two terminals .

The **-l flag** is used to set the netcat in the listening mode .
The **-p** is the flag that denotes the port number .
I have set a random port number of 12345 .

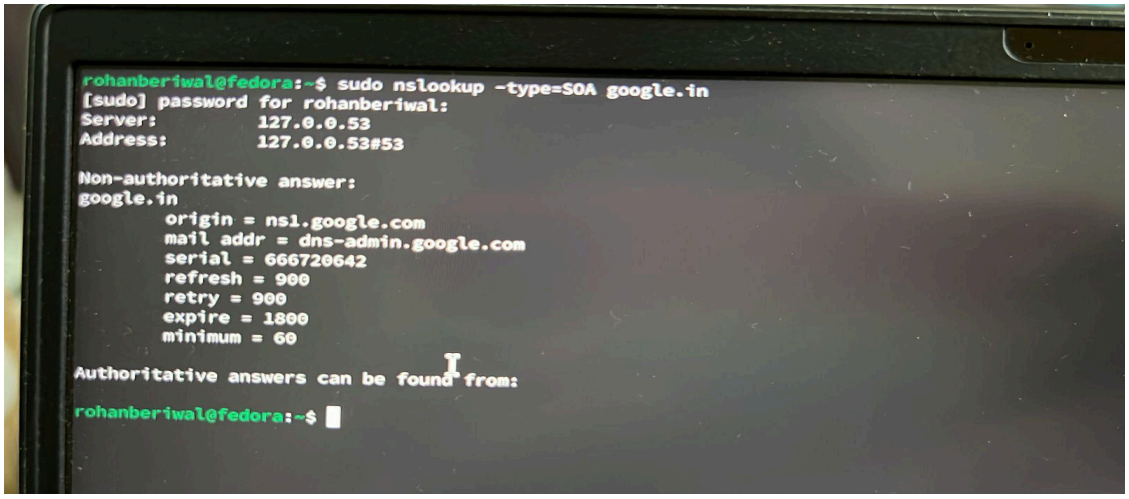
Now in the terminal 2 :
Now in the second terminal we use the **nc IP address (Client) Port No** command and after this we can generate the TCP connection between the two machines .

B)



The status of the TCP client is **“ESTABLISHED”.** That can be found using the **netcat -tn** . In this we use the -t to specify the default mode of the TCP and n for preventing the DNS resolution . The DNS resolution is used to convert the Human readable domain names into the IP addresses .
In the above ss we can see the local client and the foreign client is established .

Question 4.)

A) 

Description :

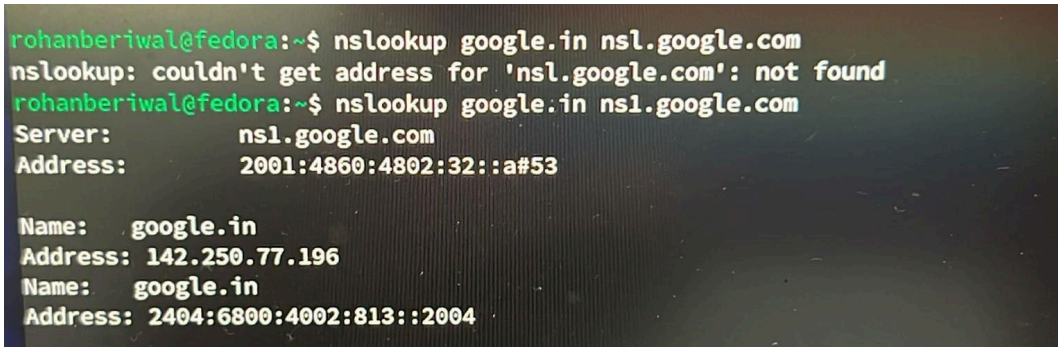
NOTE : I have used sudo in this because in the regular privilege the output was not satisfactory . The authoritative answer was blank before and after the sudo privilege .

In this I use the command **sudo nslookup -type = SOA google.in** to get an authoritative result for the website google.in . The nslookup command is used for the querying on the dns to obtain the IPaddress and information about the given website .

-type = SOA is used to set the query search on the dns to State of Authority(SOA) and get the authoritative result for the website that is getting entered .

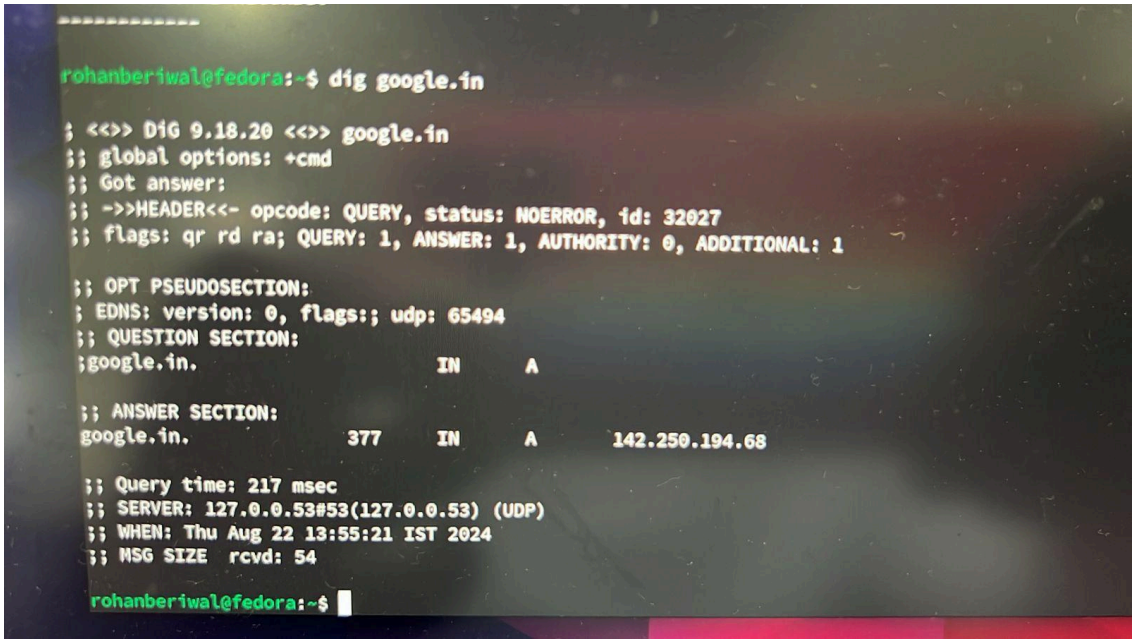
Now since the origin of the website is nsl.google.com we can use that to find the output of the authoritative results .

Continued …



Now after getting the dns query output from the command nslookup google.com. We use the query command of :
nslookup <website domain> <authoritative result>
After using this we can see the output for the authoritative result for the website of google.in .

B)



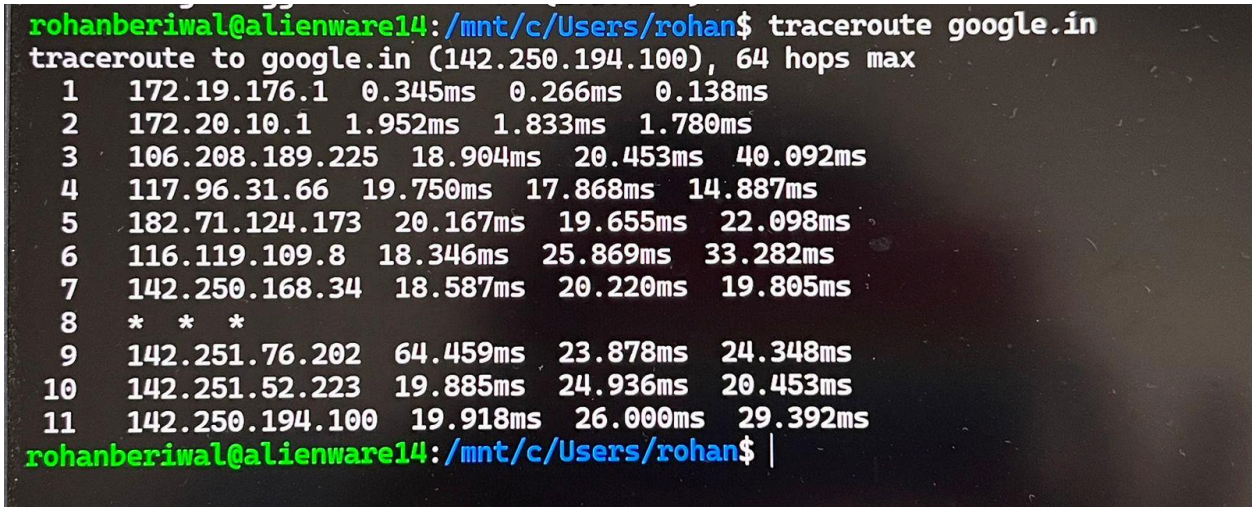
Description :
The dig command is used to query the DNS server and find the information about the domain with the specified names . The typical syntax for the dig is :

dig < website domain>

In the answer section we get the TTL (time to live) value for a website in our case it is google.in .
In our case for the google.in the TTL is 377 so we can infer that the query will be cached or saved for 377 seconds and after 377 second the query will become obsolete .

Question 5)

A)



Description :

The Number of intermediate nodes that I can see are 10.

IP address of each intermediate node / intermediate host

Host 1 : IP(172.19.176.1)-> Tavg = 0.2496667 ms

Host2 : IP(172.20.10.1)-> Tavg = 1.855 ms

Host3 : IP(106.208.189.225) -> Tavg = 26.483 ms

Host4 : IP(117.96.31.66) -> Tavg = 17.5016 ms

Host 5: IP(182.71.124.173) -> Tavg = 20.64 ms

Host 6 : Ip(116.119.109.8) -> Tavg = 25.832 ms

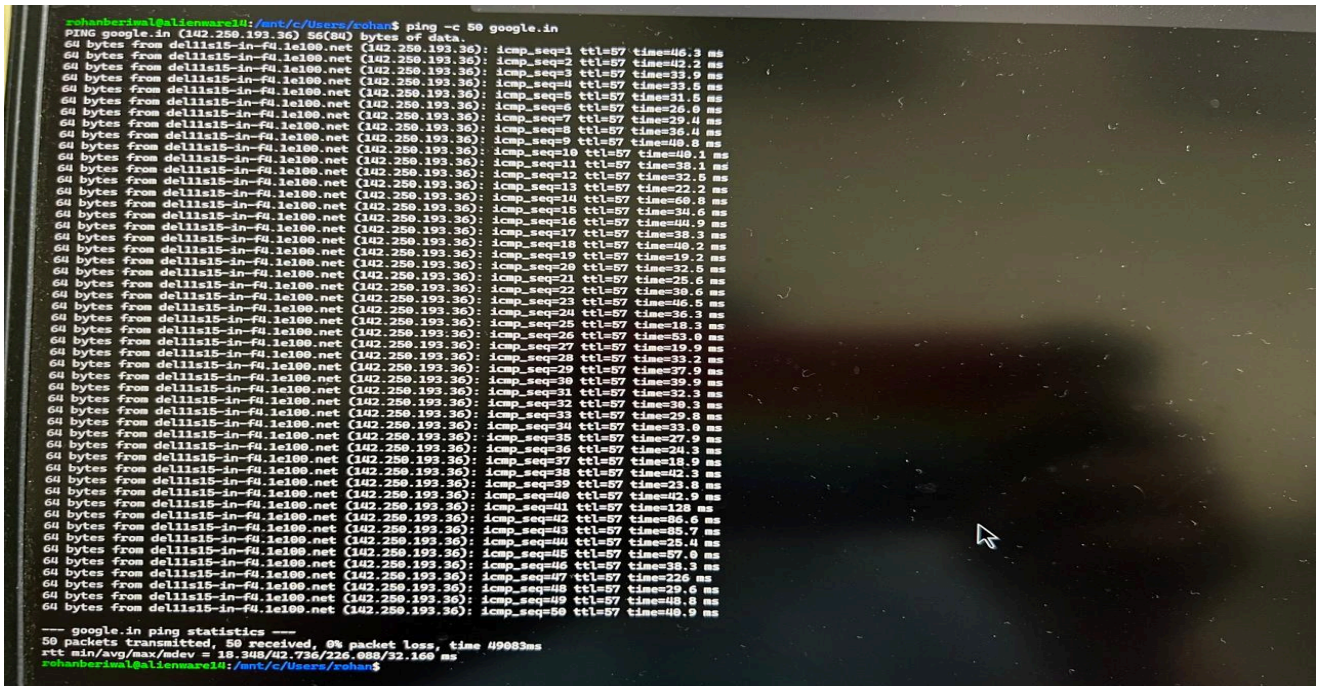
Host 7 : IP(142.250.168.34) -> Tavg = 19.537 ms

Host 8 : IP(142.251.76.202) -> Tavg = 56.3435 ms

Host 9 : IP(142.251.52.223) -> Tavg = 21.578 ms

Host10 : IP(142.250.194.100) -> Tavg = 25.10333 ms

B)



Description : From this above ping command we can infer the following :
Round trip time statistics -
1.)Total time : 49083 ms
2.) Min round trip : 18.348 ms
3.)Average Latency : 42.736 ms
4.) Max round trip time : 226.088 ms
5.) Mean deviation : 32.160 ms

Single route time statistics :
1.)Total time = 49083/2 = 24541.5 ms
2.) Min round trip : 18.348/2 = 9.174 ms
3.)Average Latency : 42.736 = 21.368ms
4.) Max round trip time : 226.088/2 = 113.044 ms

C)
Time_Average = Sum(all the t avg latencies in (a)) / number of intermed node
Tavg = (0.2496667 +1.855 +26.483 + 17.5016 + 20.64 + 25.832+ 19.537 +56.3435 + 21.578 + 25.10333) / 10

Tavg_latency = 21.5123 ms

Average latency in (B) : 42.736 ms

The average latency in part B is double of the time latency in part A . The reason for the two not matching is because the **ping command** returns the round trip time(RTT) of the packet .This means the average latency is the latency of the packet sent from the source to the destination and then back to the source . While the **traceroute command** measures the time from the source to the destination server /machine .

D)

From the Part (a) we can infer the maximum latency of Host 9 having an IP address of (142.251.76.202) that is 64.459 ms .

From part B we can infer the max latency as 226.088 ms.

The max latency from part A and part B does not matches as the due to the difference in their functions :

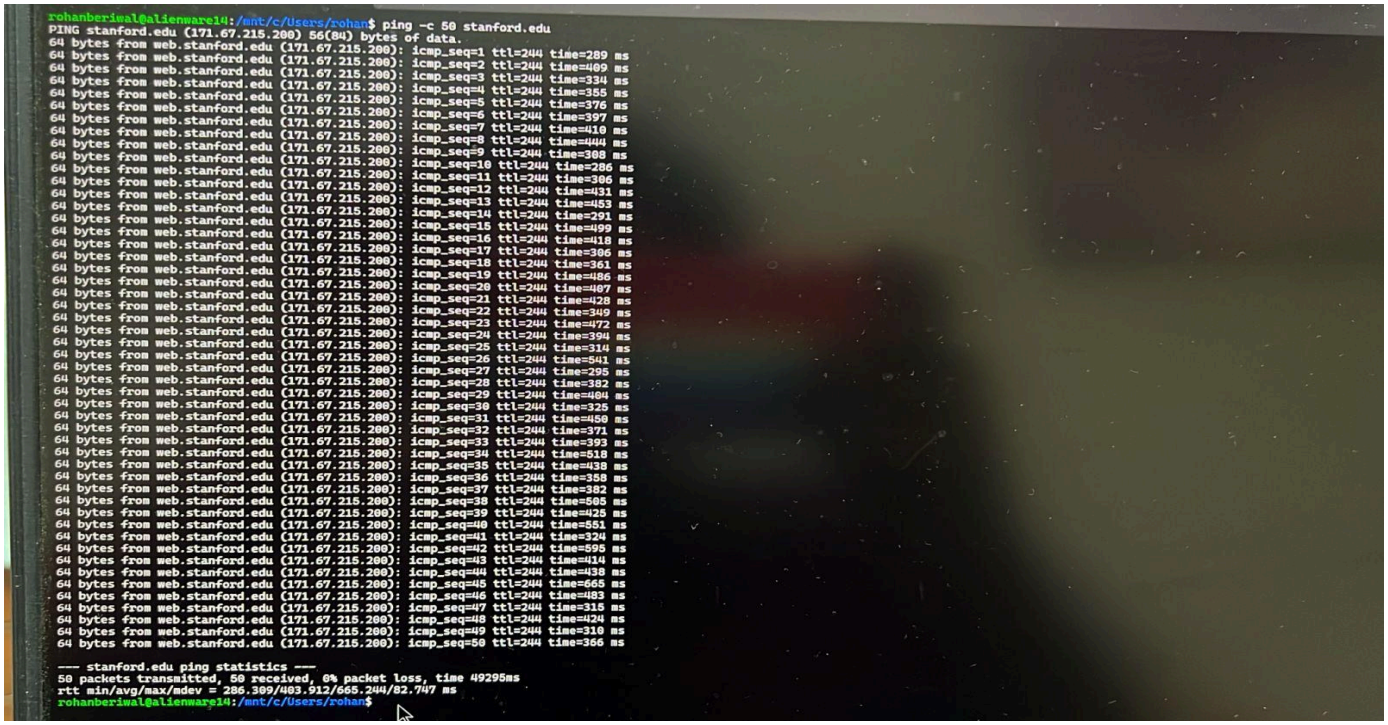
Ping command : This is used to measure the total RTT(Round trip time) from the source to the destination and then back . The ping includes the latency between all the intermediate routers / hops and the destination .

Traceroute command : This command measures the latency between each of the intermediate hop and print the latency individually . Since it does not measure the RTT (round trip time) it is generally lower than the ping output .

E)

For each of the single hop , there are typically 3 (default) entries as the traceroute command sends 3 or multiple packets to find network latency for each hop . The average of the several multiple packets sent gives a broader idea about the network traffic , performance . If we send a single packet the latency might be very high as the packet at a particular time may face congestion . Sending multiple packet gives the average estimate of the network latency within a single hop and the time to transmit the packet from one network device to another network device .

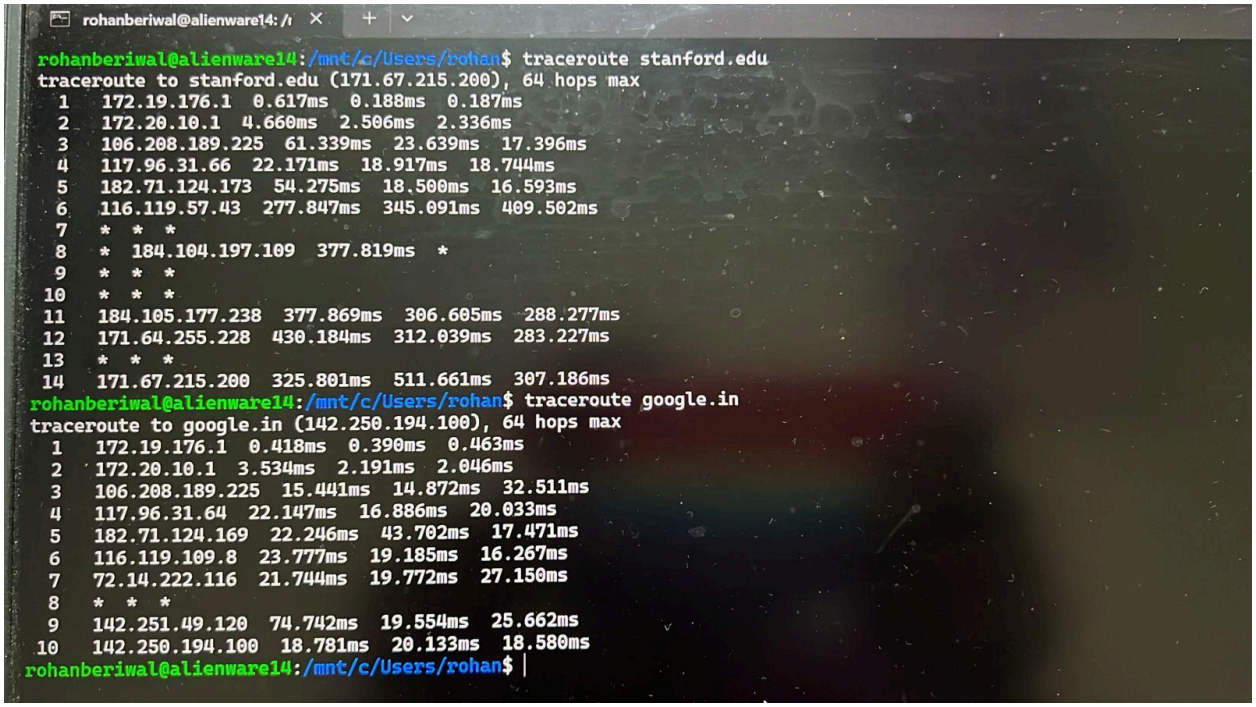
F)



Description:
From the above we can infer the following -
1.) RTT minimum = 286.309 ms
2.)RTT average time = 403.912 ms
3.) max time = 665.244 ms
4.)mdev (mean deviation) = 82.747 ms

Single route statistics
1.) Minimum time (single route) = 286.309/2 = 143.154 ms
2.) Average latency (single route) = 403.912/2 = 201.956 ms
3.) max time (single route) = 665.224/2 = 332.612 ms

G)



Considering the above code of the **traceroute google.in and traceroute stanford.edu**
We can infer the following :
Total number of Hops in stanford.edu = 14
Total number of Hops in google.in = 10

H) Considering the above code for the traceroute command for the stanford.edu and google.in :
The average latency time in stanford.edu is greater than the average time in google.in due to several factor like:

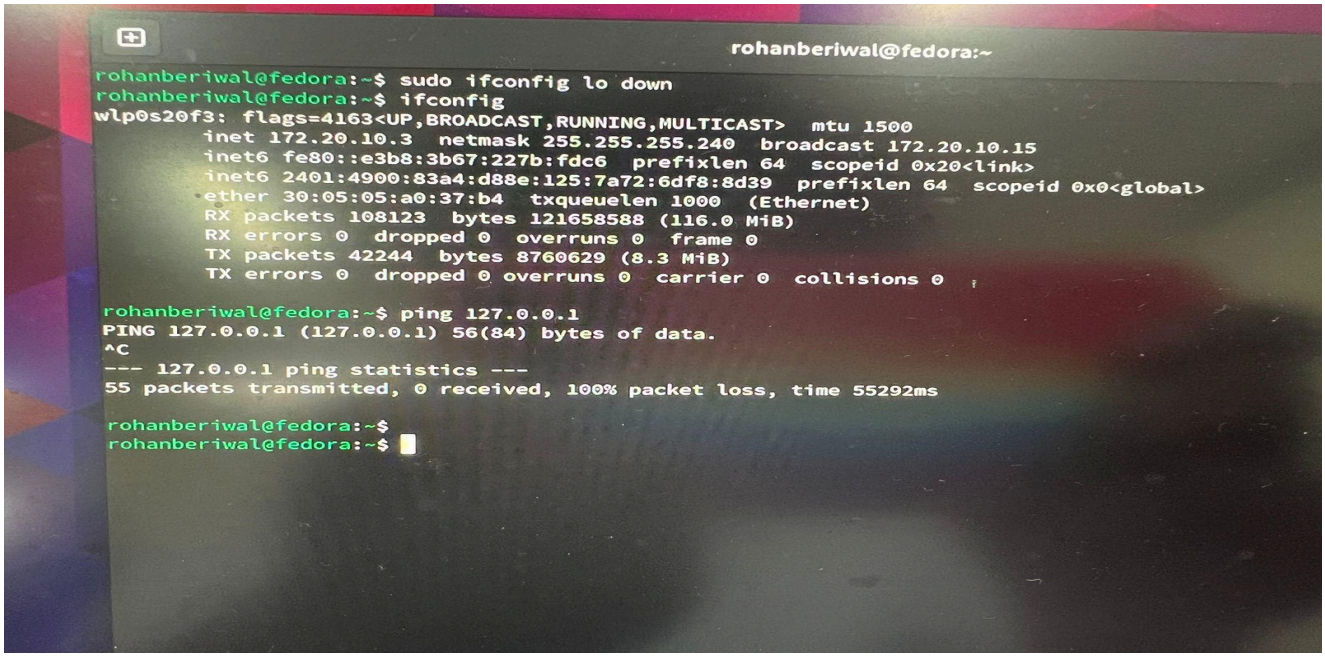
1.) **Geographics** of the destination server . google.in is in India while stanford.edu is situated in California USA . The distance while making a ping command increases the latency .

2.) **Network path and networking algorithm** : While making a ping call the network path is a major factor . The path size increases / decreases the number of the forward pass while doing a seek operation in the routing table . A server situated outside a local or at a distant position is bound to make more search operations in the routing table than a destination server present within a local network . The type of the networking algorithm and routing policies is a major factor that determines the latency of the time .

3.) **Network traffic** : Network traffic determines the amount of the time taken by the router to connect to the destination server . Consider two routers R1,R2 and a packet P1 . If there is a lot of traffic between R1 and R2 then the time taken for the packet to reach R2 to the destination will increase .

4.) **Signal Issue :** Between the two routers there may be bad weather conditions and other climatic factors that could lead to the delay in the packet transmission between the routers , increasing the overall latency of the process .

Question 6)



Description :

To make the ping command fail for the mentioned IP I followed 4 Major step :

Step1 : **<sudo ifconfig lo down>**

This is the command to disable the loopback interface . The loopback is a special interface with the IP of <127.0.0.1> that helps the user to communicate with itself . If we put a port down then the port will be disabled .

Step2 : **<ifconfig>**

This command will show all the network ports available on the machine . Since we have put down / disabled the lo port that port will not be visible in the output section .

Step3 : **<ping <ip address of Lo port> /(given port)>**
When we ping this port the machine will stop and not respond . Since this port helps the machine to make the connection with itself , the machine will not respond for a while until we press control +c .
Step4 : **<Control + c>**
When we process this command we can see the number of the client packet sent through the lo port as the mentioned ip is the ip of the lo port . 0 received as we disabled the Lo port in the step 2 and finally 100% packet loss as none of the transmitted packet is received .