CN Assignment-1

Shobhit Raj (2022482)

1 Question 1

1.1 a)

The ifconfig command output [fig. 1] shows that my network interface enp0s3 is assigned the IP address 10.0.2.15.

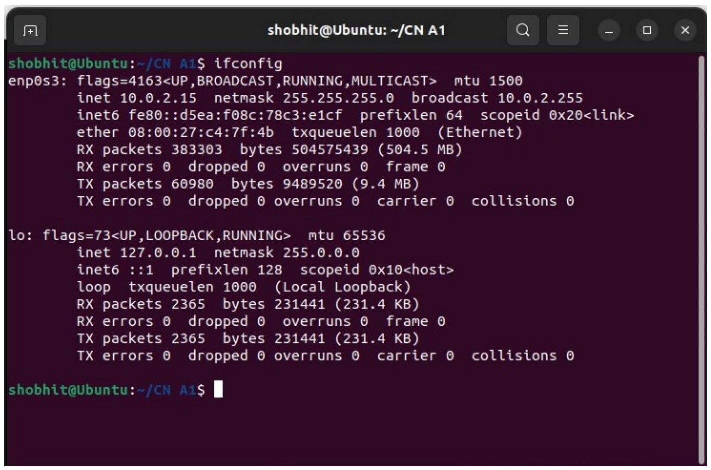


Figure 1: IP Address of network interface enp0s3

1.2 b)

The IP address shown [fig. 2] on the webpage https://www.whatismyip.com is 103.25.231.121.

The two IP addresses are different. '10.0.2.15' is a private IP address assigned to my device's network interface, it is usually done by the router for communication within the local network. Another devices on the same IIITD netowrk sees this IP address for my device. '103.25.231.121' is the public IP address assigned to my network interface by my Internet Service Provider (ISP) which is IIITD in this case. It is the IP address that is visible to the outside world and used for communication over the internet.

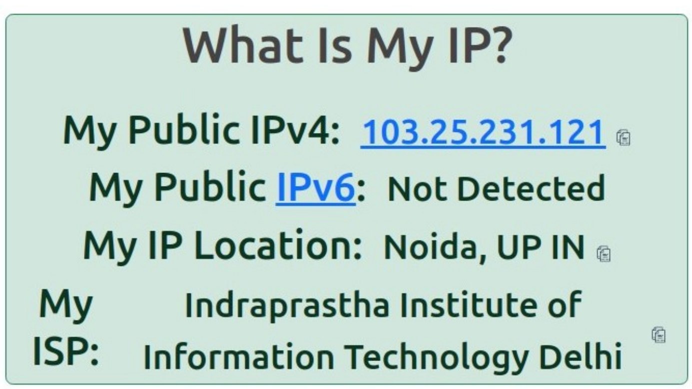


Figure 2: IP Address on https://www.whatismyip.com

2 Question 2

2.1 a)

Changed the IP address [fig. 3] of the enp0s3 interface to ’10.0.2.44’ from ’10.0.2.15’ using ”sudo ifconfig enp0s3 10.0.2.44” command.

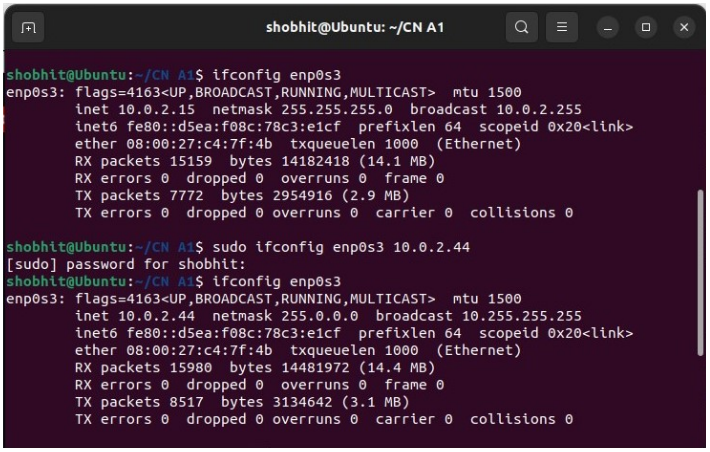


Figure 3: Changed IP Address

Reverted back to the original IP address ’10.0.2.15’ using the same command [fig. 4].

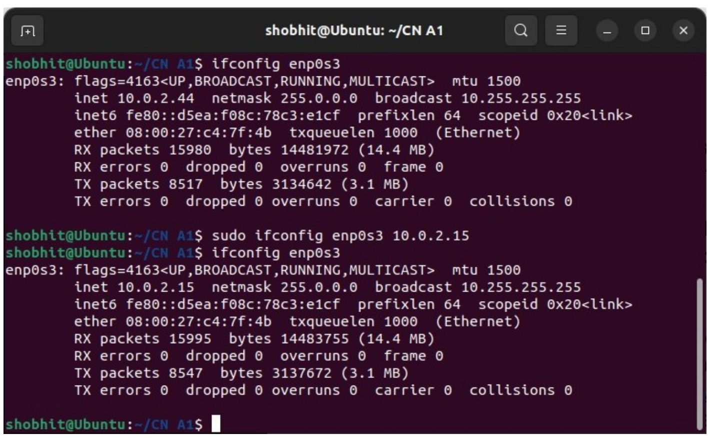


Figure 4: Changed IP Address

3 Question 3

3.1 a)

Setting up a TCP client/server connection using natcat command. ’netcat -l -p 8080’ sets up a connection in listening mode on port 8080 and ’netcat localhost 8080’ connects to this port. The messages verifies that the TCP connection is successfully set up between the two terminals [fig. 5].

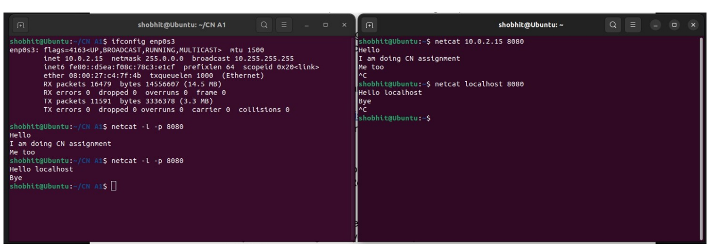


Figure 5: TCP Connection

3.2 b)

The state of this TCP connection can be determined using 'netstat' command and using '-t' flag with it which displays all the TCP connections & '-n' flag which displays the port numbers.
The "ESTABLISHED" state [fig. 6] of the connection for the port 8080 verifies that the connection is successfully established.

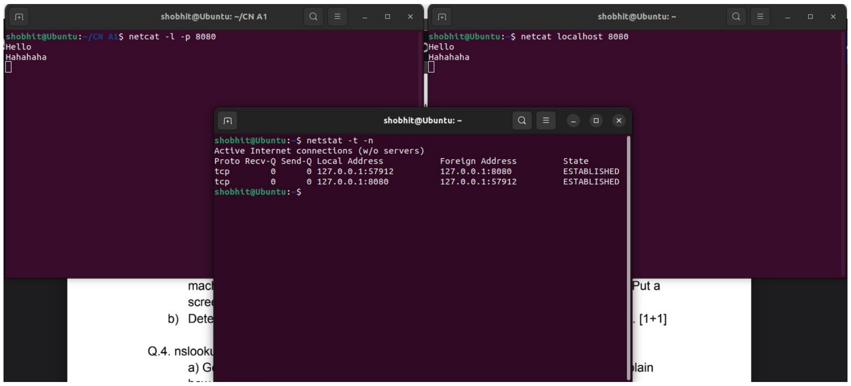


Figure 6: Established State of the TCP Connection

4 Question 4

4.1 a)

To get an authoritative DNS result for "google.in" using the nslookup command, we need to query one of the domain's authoritative DNS servers directly. The command 'nslookup -type=soa google.in' queries for the Start of Authority (SOA) record of the domain "google.in." The SOA record contains administrative information [fig. 7] about the primary DNS server responsible for "google.in", such as the primary name server, email of the domain administrator and other settings. This command indicated that the primary authoritative DNS server for "google.in" is 'ns1.google.com' (Authoritative answers can be found SECTION). So, we query the authoritative DNS server directly to get authoritative DNS records for "google.in" [fig. 7].

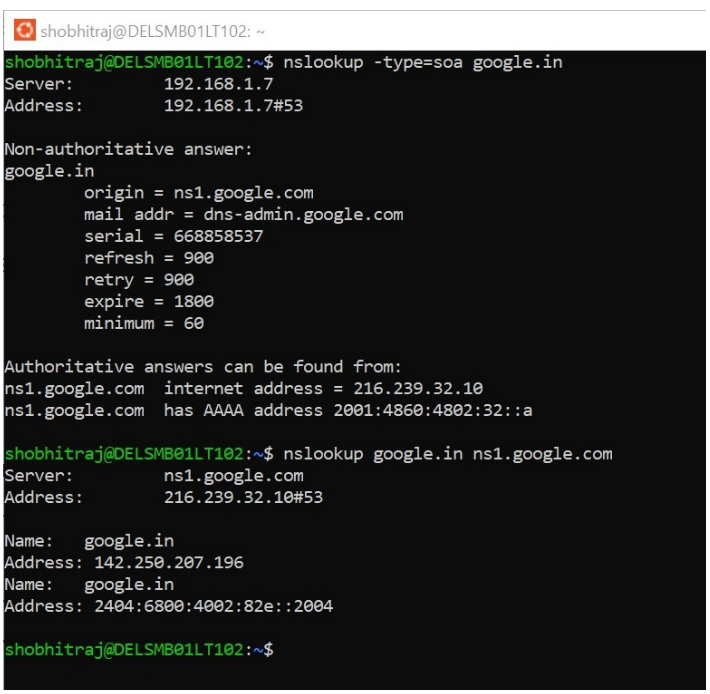


Figure 7: Authoritative result for google.in

4.2 b)

The command 'nslookup' can be used with '-debug' flag to find the Time to Live (TTL) for a website on the local DNS server. Also, 'dig' command can be used which performs same function as 'nslookup' to retrieve domain name information and is more powerful and descriptive than it. When we run 'dig' command for any domain, it displays the TTL value for the website in 'ANSWER SECTION', in seconds, which indicates how long the DNS record is cached by the local DNS server after which it would expire. Here [fig. 8], it shows TTL as 267 seconds, it means that the DNS entry for 'google.in' will expire 267 seconds (4 minutes 27 seconds) after it was cached by the local DNS server. After this period, the local DNS server will need to query the DNS server again to get the updated DNS record.

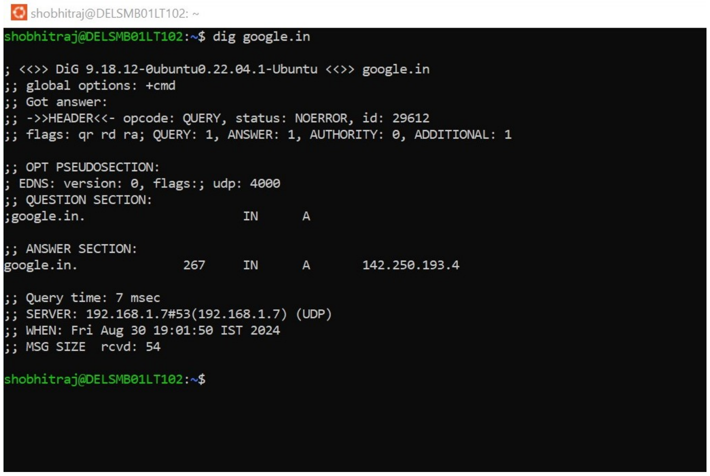


Figure 8: TTL Value for google.in

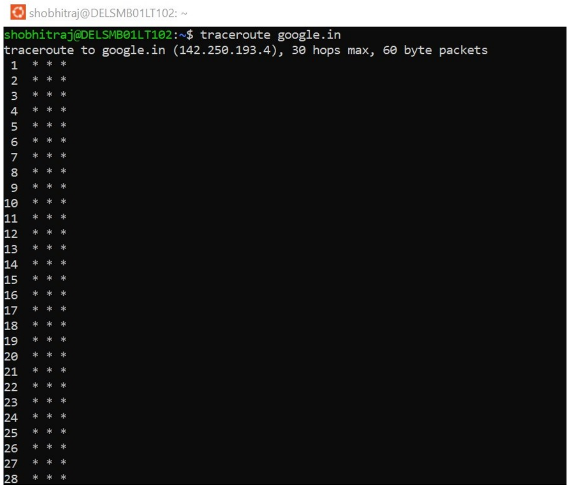
5 Question 5

5.1 a)

As "traceroute google.in" was showing all hosts "***" which means they are all hidden [fig. 9 (a)]. So, I used "tracert google.in" on my Windows cmd [fig. 9 (b)] which is the alternative for the traceroute command and sends ICMP packets to the destination.
The output shows 7 intermediate hosts before reaching the final destination (ignoring the line with ***).

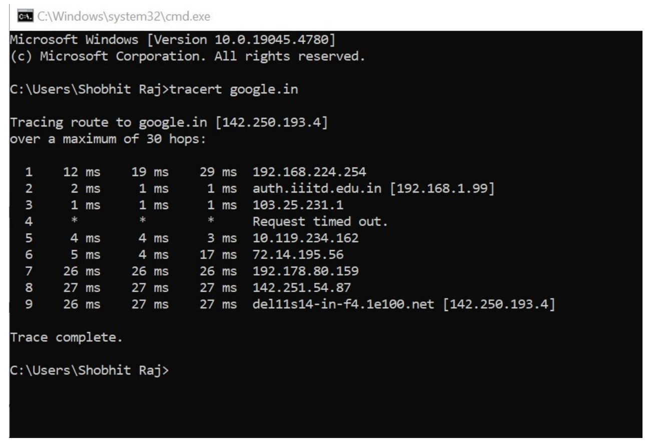
List of Intermediate Hosts (with IP addresses) :-
1) 192.168.224.254
2) auth.iiitd.edu.in [192.168.1.99]
3) 103.25.231.1
4) 10.119.234.162
5) 72.14.195.56
6) 192.178.80.159
7) 142.251.54.87
8) del111s14-in-f4.1e100.net [142.250.193.4] (Destination) – not included as dest. & not intermediate host

The average latency to each intermediate host :-
1) 192.168.224.254: Average = (12 ms + 19 ms + 29 ms) / 3 = 20 ms
2) auth.iiitd.edu.in [192.168.1.99]: Average = (2 ms + 1 ms + 1 ms) / 3 = 1.33 ms
3) 103.25.231.1: Average = (1 ms + 1 ms + 1 ms) / 3 = 1 ms
4) 10.119.234.162: Average = (4 ms + 4 ms + 3 ms) / 3 = 3.67 ms
5) 72.14.195.56: Average = (5 ms + 4 ms + 17 ms) / 3 = 8.67 ms
6) 192.178.80.159: Average = (26 ms + 25 ms + 27 ms) / 3 = 26 ms
7) 142.251.54.87: Average = (27 ms + 27 ms + 27 ms) / 3 = 27 ms



```
shobhitraj@DELSMB01LT102: ~
shobhitraj@DELSMB01LT102:~$ traceroute google.in
traceroute to google.in (142.250.193.4), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
```

(a) Traceroute google.in all hosts ***



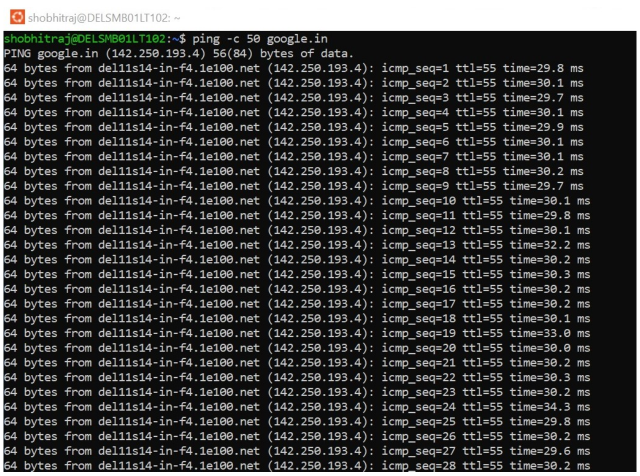
```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.4780]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Shobhit Raj>tracert google.in

Tracing route to google.in [142.250.193.4]
over a maximum of 30 hops:

  1    12 ms    19 ms    29 ms  192.168.224.254
  2     2 ms     1 ms     1 ms  auth.iiitd.edu.in [192.168.1.99]
  3     1 ms     1 ms     1 ms  103.25.231.1
  4     *        *        *     Request timed out.
  5     4 ms     4 ms     3 ms  10.119.234.162
  6     5 ms     4 ms    17 ms  72.14.195.56
  7    26 ms    26 ms    26 ms  192.178.80.159
  8    27 ms    27 ms    27 ms  142.251.54.87
  9    26 ms    27 ms    27 ms  del11s14-in-f4.1e100.net [142.250.193.4]

Trace complete.

C:\Users\Shobhit Raj>
```

(b) Tracert google.in showing tracing route

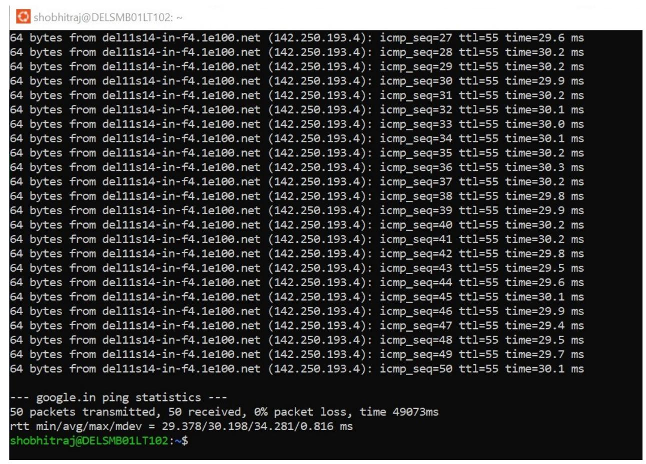
Figure 9: Traceroute results

5.2 b)

We can ping google.in 50 times using the flag '-c 50' which specifies the number of Echo Request packages to be sent to the destination.
As the output shows [fig. 10], the average latency is 30.198 ms.



```
shobhitraj@DELSMB01LT102: ~
shobhitraj@DELSMB01LT102:~$ ping -c 50 google.in
PING google.in (142.250.193.4) 56(84) bytes of data.
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=1 ttl=55 time=29.8 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=2 ttl=55 time=30.1 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=3 ttl=55 time=29.7 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=4 ttl=55 time=30.1 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=5 ttl=55 time=29.9 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=6 ttl=55 time=30.1 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=7 ttl=55 time=30.1 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=8 ttl=55 time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=9 ttl=55 time=29.7 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=10 ttl=55 time=30.1 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=11 ttl=55 time=29.8 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=12 ttl=55 time=30.1 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=13 ttl=55 time=32.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=14 ttl=55 time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=15 ttl=55 time=30.3 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=16 ttl=55 time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=17 ttl=55 time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=18 ttl=55 time=30.1 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=19 ttl=55 time=33.0 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=20 ttl=55 time=30.0 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=21 ttl=55 time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=22 ttl=55 time=30.3 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=23 ttl=55 time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=24 ttl=55 time=34.3 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=25 ttl=55 time=29.8 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=26 ttl=55 time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=27 ttl=55 time=29.6 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=28 ttl=55 time=30.2 ms
```



```
shobhitraj@DELSMB01LT102: ~
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=27 ttl=55 time=29.6 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=28 ttl=55 time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=29 ttl=55 time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=30 ttl=55 time=29.9 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=31 ttl=55 time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=32 ttl=55 time=30.1 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=33 ttl=55 time=30.0 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=34 ttl=55 time=30.1 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=35 ttl=55 time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=36 ttl=55 time=30.3 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=37 ttl=55 time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=38 ttl=55 time=29.8 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=39 ttl=55 time=29.9 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=40 ttl=55 time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=41 ttl=55 time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=42 ttl=55 time=29.8 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=43 ttl=55 time=29.5 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=44 ttl=55 time=29.6 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=45 ttl=55 time=30.1 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=46 ttl=55 time=29.9 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=47 ttl=55 time=29.4 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=48 ttl=55 time=29.5 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=49 ttl=55 time=29.7 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=50 ttl=55 time=30.1 ms

--- google.in ping statistics ---
50 packets transmitted, 50 received, 0% packet loss, time 49073ms
rtt min/avg/max/mdev = 29.378/30.198/34.281/0.816 ms
shobhitraj@DELSMB01LT102:~$
```

Figure 10: Ping google.in results

5.3 c)

Total Ping Latency of Intermediate Hosts as obtained in (a) :-
20 + 1.33 + 1 + 3.67 + 8.67 + 26 + 27 = 87.67 ms
And the average latency as obtained in (b) is 30.198 ms.
Hence, the total ping latency of the intermediate hosts obtained from the traceroute command (87.67 ms) does not match the average latency obtained from the ping command (30.198 ms). The reason being traceroute considers the cumulative delays from each intermediate hop, whereas ping measures the overall average round-trip latency directly to the final destination, not accounting for each hop's delay individually but as a whole, hence lower latency. Also, traceroute generally sends 3 probes with incrementing TTL value, which is why the sum of latencies from traceroute is higher than the direct ping result.

5.4 d)

The maximum ping latency in (a) is 29 ms & the average latency as obtained in (b) is 30.198 ms. These values are very close to each other, which indicates that the hop where the maximum latency occurred (Hop 1) likely had a significant impact on the overall latency observed when pinging google.in, suggesting that there may be a bottleneck at that point in the network.

5.5 e)

Each hop in a traceroute is showing three latency measurements, represeting the three separate ICMP echo requests traceroute sends to each hop in the network path to the destination. These multiple entries represent the times it took for three separate probe packets to reach that hop and return. The reason for sending multiple probes is to provide a more reliable measure of latency and checking the stability of the netowrk path at each stage (hop) of the route to the destination.

5.6 f)

We can ping stanford.edu 50 times using the flag '-c 50' which specifies the number of Echo Request packages to be sent to the destination.
As the output shows [fig.11], the average latency is 271.985 ms.

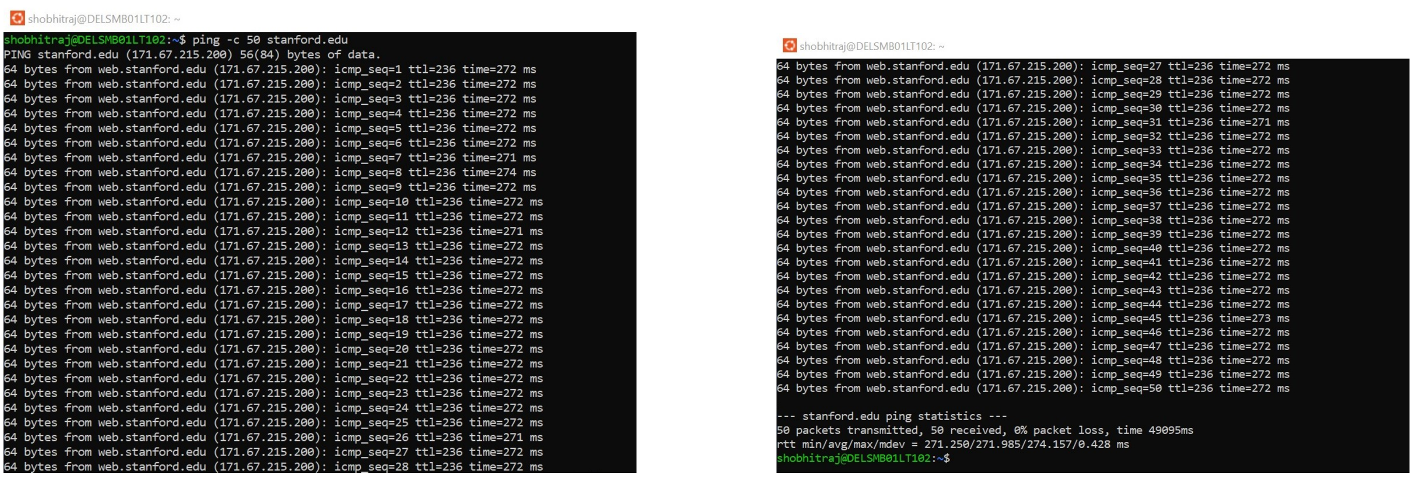
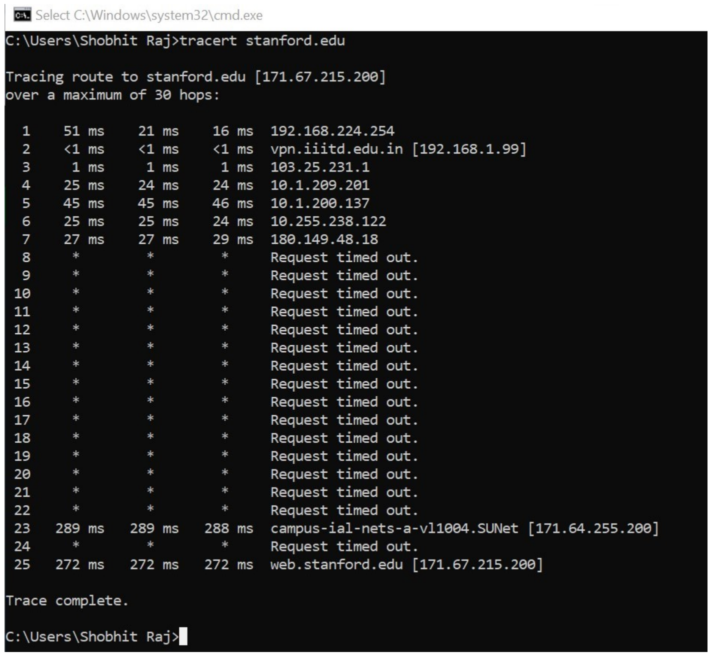


Figure 11: Ping stanford.edu results

5.7 g)

The path to stanford.edu involves 25 hops although many *** (timeouts and hidden) [fig. 12] are present, ignoring them leading to 8 intermediate hosts before reaching the final destination which is 1 more hop than 'traceroute google.in.'

The traceroute to stanford.edu requires significantly more hops compared to google.in, indicating a longer or more complex network path. The presence of numerous timeouts in the traceroute to stanford.edu suggests possible network segments that do not respond to traceroute probes or are hidden, adding to the complexity of the route.



```
Select C:\Windows\system32\cmd.exe
C:\Users\Shobhit Raj>tracert stanford.edu

Tracing route to stanford.edu [171.67.215.200]
over a maximum of 30 hops:

  1    51 ms    21 ms    16 ms  192.168.224.254
  2    <1 ms    <1 ms    <1 ms  vpn.iiitd.edu.in [192.168.1.99]
  3     1 ms     1 ms     1 ms  103.25.231.1
  4    25 ms    24 ms    24 ms  10.1.209.201
  5    45 ms    45 ms    46 ms  10.1.200.137
  6    25 ms    25 ms    24 ms  10.255.238.122
  7    27 ms    27 ms    29 ms  180.149.48.18
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23   289 ms   289 ms   288 ms  campus-ial-nets-a-vl1004.SUNet [171.64.255.200]
 24     *        *        *     Request timed out.
 25   272 ms   272 ms   272 ms  web.stanford.edu [171.67.215.200]

Trace complete.

C:\Users\Shobhit Raj>
```

Figure 12: Traceroute stanford.edu results

5.8 h)

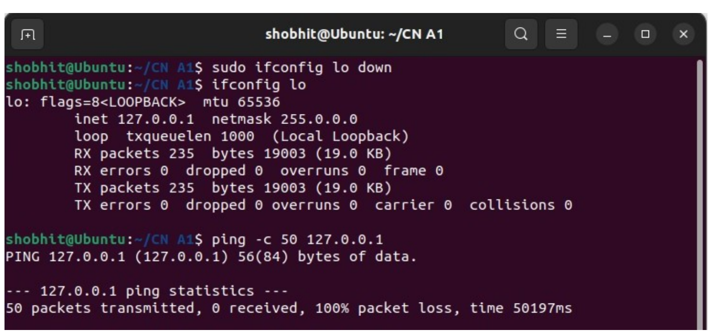
The latency of stanford.edu is 271.985 ms as observed in (f) is significantly greater than latency of google.in which is 30.198 ms as observed in (b). This is because of the difference between the geographical locations of the servers of the 2 websites. The former likely has a server closer, likely in India, resulting in lower latency. And stanford.edu server is located in the United States, which is much farther from my location. Also, Google's networks are more optimised and efficient compared to Stanford's as observed in (g), traceroute of stanford.edu suggest a more complex or less optimized network path, contributing to the higher latency.

6 Question 6

The "127.0.0.1" address is used by a computer to communicate with itself. It's part of the loopback network interface, which is a virtual interface that enables internal netowrk communications within the same machine.

The ping command can be made to fail for 127.0.0.1 by disabling the loopback interface "lo" as the system cannot generate ICMP Echo Replies because the loopback interface is disabled to process the incoming and outgoing packets, disrupting the path for the packets.

The "lo" network interface can be disabled using "sudo ifconfig lo down", checking with "ifconfig lo" will show it is not in "up & running" state and then "ping 127.0.0.1" will fail [fig. 13] with 100% packet lost.



```
shobhit@Ubuntu: ~/CN A1
shobhit@Ubuntu:~/CN A1$ sudo ifconfig lo down
shobhit@Ubuntu:~/CN A1$ ifconfig lo
lo: flags=8<LOOPBACK>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 235  bytes 19003 (19.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 235  bytes 19003 (19.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

shobhit@Ubuntu:~/CN A1$ ping -c 50 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.

--- 127.0.0.1 ping statistics ---
50 packets transmitted, 0 received, 100% packet loss, time 50197ms
```

Figure 13: ping 127.0.0.1 failing with 100% packet lost