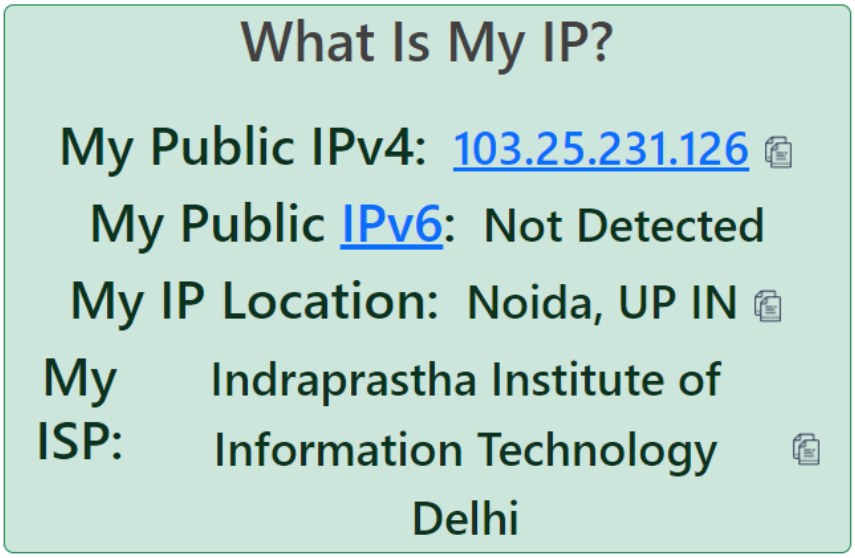
Q1. [1 + 1]

a) Learn to use the ifconfig command, and figure out the IP address of your network interface. Put a screenshot.

```
vidhan@LAPTOP-FO2TSQUA:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.20.14.108  netmask 255.255.240.0  broadcast 172.20.15.255
        inet6 fe80::215:5dff:feef:d46a  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:ef:d4:6a  txqueuelen 1000  (Ethernet)
        RX packets 2525  bytes 3595117 (3.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 331  bytes 40807 (40.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1665  bytes 18669573 (18.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1665  bytes 18669573 (18.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

IP Address: 172.20.14.108

b) Go to the webpage https://www.whatismyip.com and find out what IP is shown for your machine. Are they identical or different? Why?



No, the IPs shown were not identical. This is because my local IP address,

assigned by my router for communication within my local network, is different from the public IP address that is seen by external websites. The public IP is assigned by my Internet Service Provider (ISP) and may be shared among multiple devices on my network due to Network Address Translation (NAT). Additionally, if I were using a VPN or proxy, the IP shown on the website would reflect that service's IP rather than my actual public IP.

Q.2. [1+1+1]

a) Change the IP address of your network interface using the command line. Put a screenshot that shows the change. Revert to the original IP address.

```
vidhan@LAPTOP-FO2TSQUA:~$ sudo ifconfig eth0 172.20.69.69
vidhan@LAPTOP-FO2TSQUA:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.20.69.69  netmask 255.255.0.0  broadcast 172.20.255.255
        inet6 fe80::215:5dff:feef:d46a  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:ef:d4:6a  txqueuelen 1000  (Ethernet)
        RX packets 2572  bytes 3606271 (3.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 335  bytes 41059 (41.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Reverted:

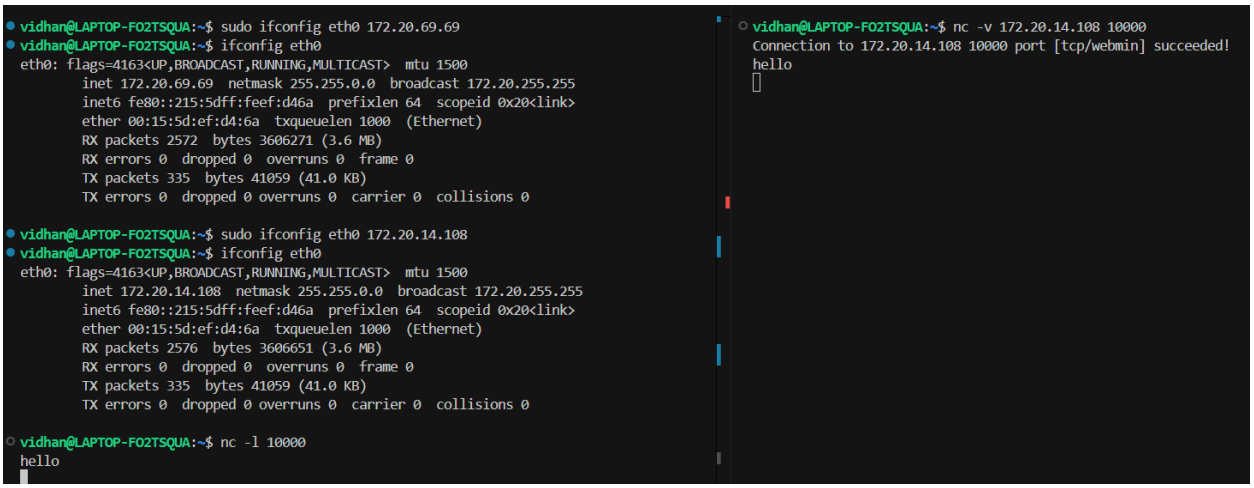
```
vidhan@LAPTOP-FO2TSQUA:~$ sudo ifconfig eth0 172.20.14.108
vidhan@LAPTOP-FO2TSQUA:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.20.14.108  netmask 255.255.0.0  broadcast 172.20.255.255
        inet6 fe80::215:5dff:feef:d46a  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:ef:d4:6a  txqueuelen 1000  (Ethernet)
        RX packets 2576  bytes 3606651 (3.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 335  bytes 41059 (41.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Q.3. [4]

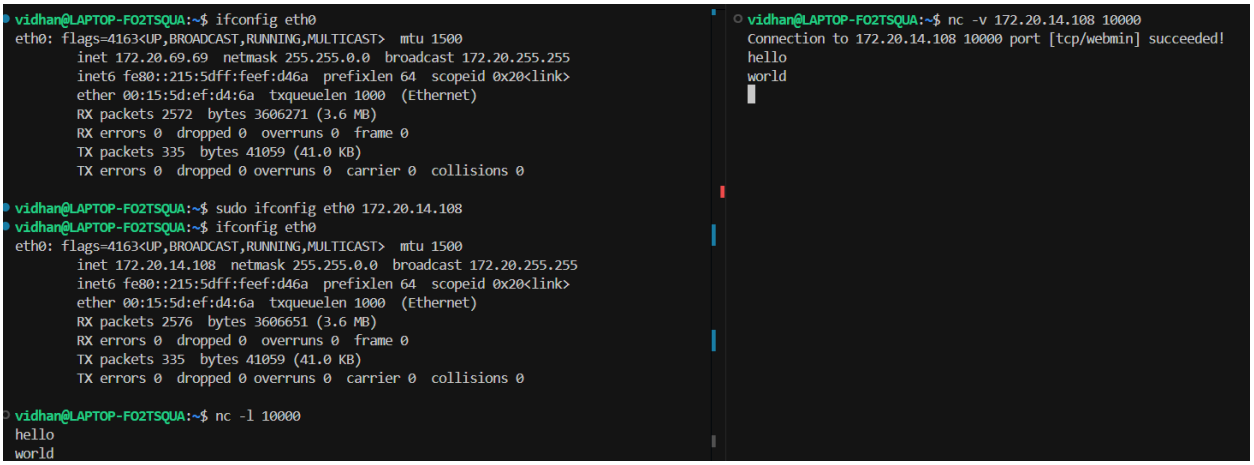
a) Use "netcat" to set up a TCP client/server connection between your VM and host machine. If you are not using a VM, you can set up the connection with *localhost*. Put a screenshot. [1+1]

```
vidhan@LAPTOP-FO2TSQUA:~$ nc -l 10000
```

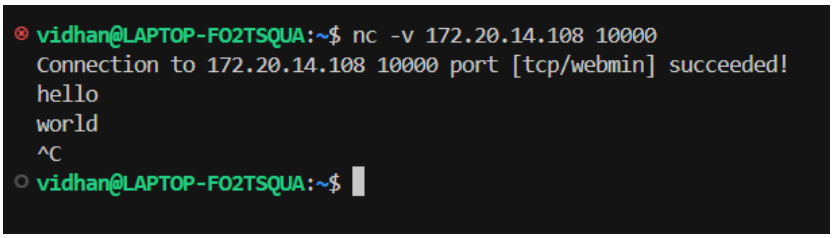
```
vidhan@LAPTOP-FO2TSQUA:~$ nc -v 172.20.14.108 10000
Connection to 172.20.14.108 10000 port [tcp/webmin] succeeded!
```



Sending message from server to the client

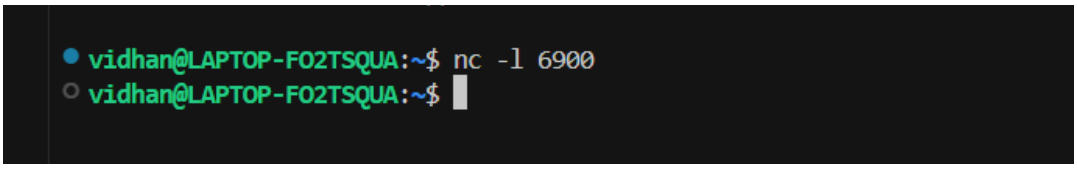


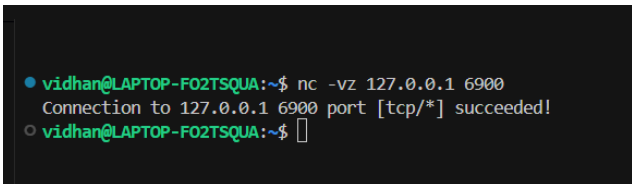
Sending message from client to the server

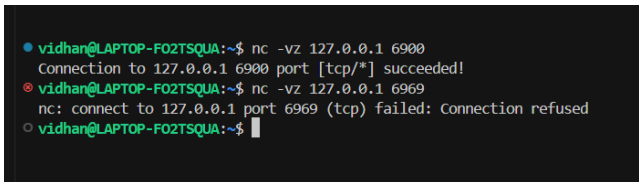


Terminated

b) Determine the state of this TCP connection(s) at the client node. Put a screenshot. [1+1]



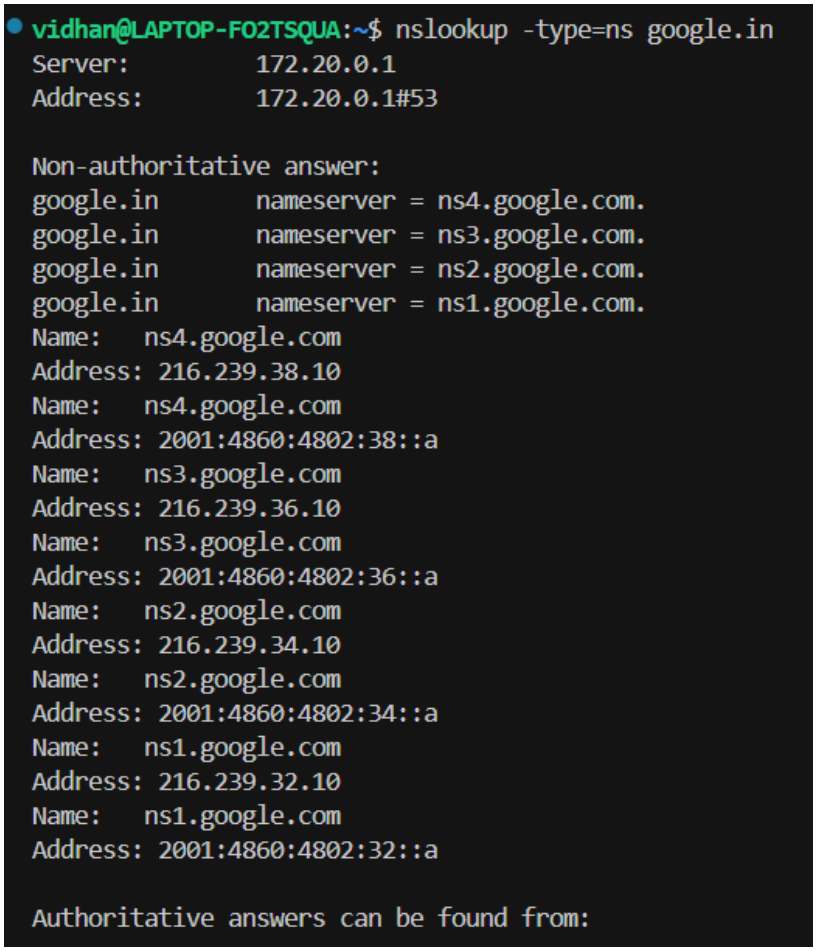




The message on the client terminal shows that the connection has been established and the port is open. If no listening service is found, it will show an error message, which can be caused by the server not running or the port number being incorrect.

Q.4. nslookup ([2+1] + [1+1])

a) Get an authoritative result for “google.in” using nslookup. Put a screenshot. Explain how you did it.



```
vidhan@LAPTOP-FO2TSQUA:~$ nslookup google.in ns1.google.com
Server:         ns1.google.com
Address:        216.239.32.10#53

Name:   google.in
Address: 142.250.182.164
Name:   google.in
Address: 2404:6800:4002:815::2004
```

To get an authoritative result for "google.in" using `nslookup`, I used the `nslookup` command in the command prompt or terminal. By entering `nslookup -type=ns google.in`, the tool queried the DNS to find the authoritative name servers responsible for the domain. These servers provide the most accurate and up-to-date DNS records for "google.in." The result displayed the names and IP addresses of Google's authoritative name servers. I took a screenshot of this output to include in my response.

b) Find out the time to live for any website on the local DNS. Put a screenshot. Explain in words (with unit) after how much time this entry would expire from the local DNS server.

```
vidhan@LAPTOP-FO2TSQUA:~$   nslookup -debug google.in
Server:         172.20.0.1
Address:        172.20.0.1#53

------------
    QUESTIONS:
        google.in, type = A, class = IN
    ANSWERS:
    ->  google.in
        internet address = 142.250.193.4
        ttl = 0
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Non-authoritative answer:
Name:   google.in
Address: 142.250.193.4
------------
    QUESTIONS:
        google.in, type = AAAA, class = IN
    ANSWERS:
    ->  google.in
        has AAAA address 2404:6800:4002:819::2004
        ttl = 0
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Name:   google.in
Address: 2404:6800:4002:819::2004
```

Q.5. [13]

a) Run the command, *traceroute google.in.* How many intermediate hosts do you see? What are the IP addresses? Compute the average latency to each intermediate host. Put a screenshot. [1+2+1]

```
Tracing route to google.in [142.250.194.132]
over a maximum of 30 hops:

  1     1 ms    <1 ms     1 ms  192.168.1.1
  2     2 ms     2 ms     2 ms  noi-netm-bngs-09 [205.254.162.10]
  3     5 ms     3 ms     3 ms  205.254.162.1
  4     4 ms     4 ms     4 ms  205.254.162.41
  5     7 ms     7 ms     6 ms  72.14.208.36
  6     4 ms     3 ms     4 ms  142.251.66.169
  7     3 ms     4 ms     3 ms  142.251.52.203
  8     6 ms     3 ms    11 ms  del12s05-in-f4.1e100.net [142.250.194.132]

Trace complete.
```

1. IP address: 192.168.1.1
   Avg latency:0.833 ms
2. IP address: 205.254.162.10
   Avg latency:2 ms
3. IP address: 205.254.162.1
   Avg latency:3.66 ms
4. IP address: 205.254.162.41
   Avg latency:4 ms
5. IP address: 72.14.208.36
   Avg latency:6.66 ms
6. IP address: 142.251.6.169
   Avg latency:3.6 ms
7. IP address: 142.251.52.203
   Avg latency:1.33 ms
8. IP address: 142.250.194.132
   Avg latency:3.66 ms

b) Send 50 ping messages to google.in, Determine the average latency. Put a screenshot. [1]

```
vidhan@LAPTOP-FO2TSQUA:~$ ping -c 50 google.in
PING google.in (142.250.206.100) 56(84) bytes of data.
64 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=1 ttl=58 time=4.69 ms
64 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=2 ttl=58 time=5.69 ms
64 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=3 ttl=58 time=4.37 ms
64 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=4 ttl=58 time=5.76 ms
64 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=5 ttl=58 time=5.05 ms
64 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=6 ttl=58 time=4.50 ms
64 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=7 ttl=58 time=5.72 ms
64 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=8 ttl=58 time=43.8 ms
64 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=9 ttl=58 time=4.89 ms
```

```
64 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=44 ttl=58 time=4.91 ms
64 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=45 ttl=58 time=5.42 ms
64 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=46 ttl=58 time=5.45 ms
64 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=47 ttl=58 time=5.12 ms
64 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=48 ttl=58 time=4.60 ms
64 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=49 ttl=58 time=5.57 ms
64 bytes from del11s20-in-f4.1e100.net (142.250.206.100): icmp_seq=50 ttl=58 time=4.88 ms

--- google.in ping statistics ---
50 packets transmitted, 50 received, 0% packet loss, time 49076ms
rtt min/avg/max/mdev = 4.165/5.946/43.809/5.435 ms
```

Avg latency = 5.946

c) The total ping latency over all the intermediate hosts obtained in a) is 25.68 ms, much higher than the average latency of 5.946 ms for the ping command. In general, the latency of the ping command is lower than the traceroute command as the ping only measures the time from the destination and back. On the other hand, the traceroute command measures the latency to each hop separately. Each of these hops involves different routers, which may induce additional latency which is not present in the ping command

d) The maximum latency amongst the intermediate hosts was 6.66 ms, which is higher than the average latency of 5.946 ms for the ping command. This is because the maximum latency amongst the intermediate host for the traceroute command can appear to be inflated because of congestion on a particular intermediate host, whereas the average latency of the ping command is calculated over multiple packets and thus is less affected by the impact of a particularly slow hop

e) When using the traceroute command, multiple entries for a single hop indicate several paths to reach the destination host. This suggests that packets may follow different routes through the network, even when directed at the same hop.

f) Send 50 ping messages to stanford.edu, Determine the average latency. Put a screenshot. [1]

```
vidhan@LAPTOP-FO2TSQUA:~$ ping -c 50 stanford.edu
PING stanford.edu (171.67.215.200) 56(84) bytes of data.
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=1 ttl=240 time=270 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=2 ttl=240 time=269 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=3 ttl=240 time=270 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=4 ttl=240 time=269 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=5 ttl=240 time=270 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=6 ttl=240 time=270 ms
```

```
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=44 ttl=240 time=269 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=45 ttl=240 time=270 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=46 ttl=240 time=270 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=47 ttl=240 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=48 ttl=240 time=270 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=49 ttl=240 time=270 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=50 ttl=240 time=270 ms

--- stanford.edu ping statistics ---
50 packets transmitted, 50 received, 0% packet loss, time 49013ms
rtt min/avg/max/mdev = 268.749/270.447/289.161/2.784 ms
```

Avg latency: 270.447

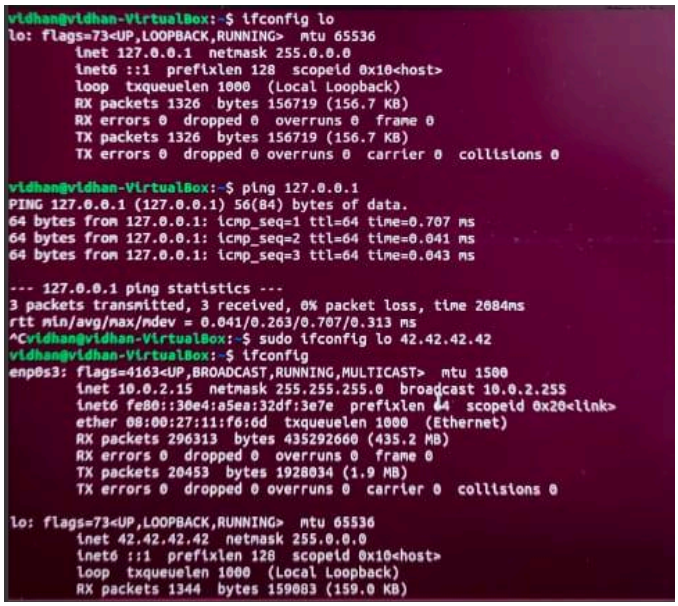
g)

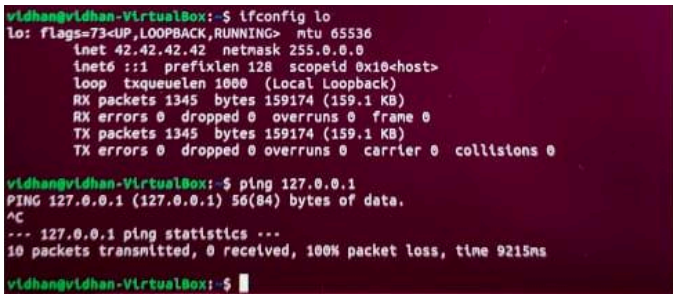
```
Tracing route to stanford.edu [171.67.215.200]
over a maximum of 30 hops:

  1     1 ms     2 ms     2 ms  192.168.1.1
  2     3 ms     1 ms     2 ms  noi-netm-bngs-09 [205.254.162.10]
  3     3 ms     2 ms     3 ms  205.254.162.1
  4     3 ms     2 ms     3 ms  121.240.3.13
  5    26 ms    26 ms    25 ms  172.23.183.134
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *      268 ms     *     port-channel7.core2.pao1.he.net [184.104.198.254]
 12   286 ms   280 ms   273 ms  stanford-university.e0-62.core2.pao1.he.net [184.105.177.238]
 13   270 ms   270 ms   270 ms  campus-east-rtr-vl1018.SUNet [171.64.255.228]
 14     *        *        *     Request timed out.
 15   268 ms   269 ms   269 ms  web.stanford.edu [171.67.215.200]

Trace complete.
```

The number of hops for stanford.edu is 15, which is higher than the 8 hops for google.in .

h) The average latency for stanford.edu is significantly higher than for Google.in which could be attributed to several factors. Firstly, geographical location plays a role; the physical distance to Google's servers in India is much shorter than the distance to Stanford's servers in the USA. Secondly, the number of hops also affects latency; more intermediate hops typically lead to higher latency, as each hop adds processing and forwarding time.

Q.6.





I checked the current IP address of the loopback interface and pinged it to verify connectivity. Then, I used `sudo ifconfig lo 42.42.42.42` to change the loopback interface's IP address. Afterward, I pinged `127.0.0.1` again to observe the failure. Finally, I reverted the loopback interface back to `127.0.0.1`.