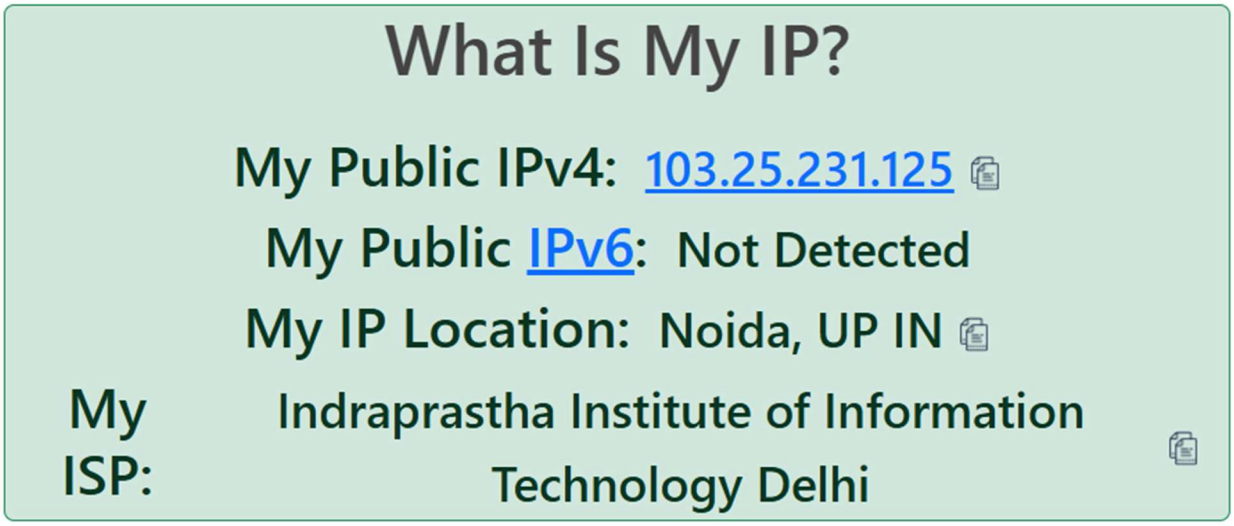
Question 1)

a) Ip address marked with box

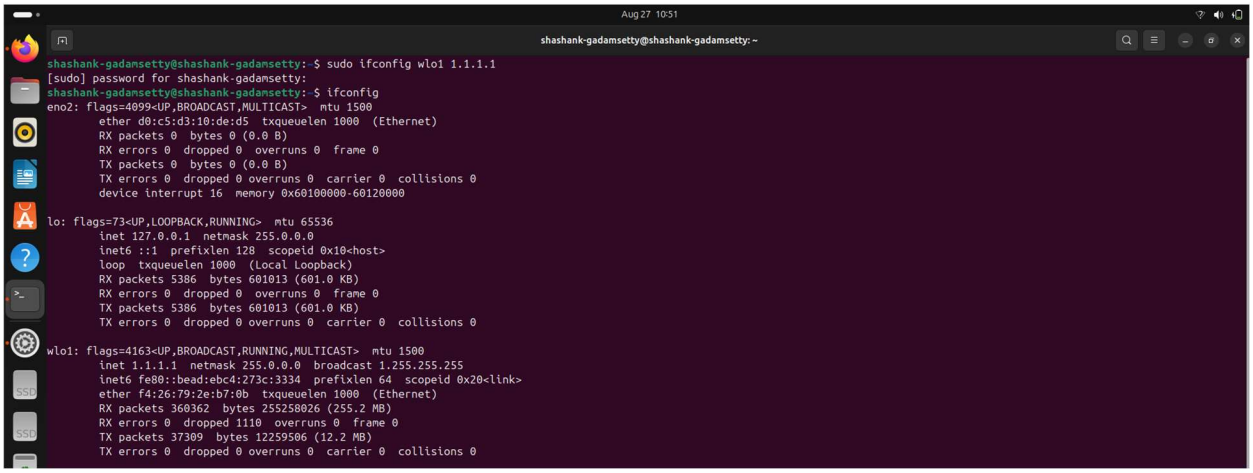
```
shashank-gadamsetty@shashank-gadamsetty:~$ ifconfig
eno2: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether d0:c5:d3:10:de:d5  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  memory 0x60100000-60120000

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 1018  bytes 111933 (111.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1018  bytes 111933 (111.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.42.190  netmask 255.255.224.0  broadcast 192.168.63.255
        inet6 fe80::bead:ebc4:273c:3334  prefixlen 64  scopeid 0x20<link>
        ether f4:26:79:2e:b7:0b  txqueuelen 1000  (Ethernet)
        RX packets 51196  bytes 28842593 (28.8 MB)
        RX errors 0  dropped 164  overruns 0  frame 0
        TX packets 5803  bytes 1992283 (1.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

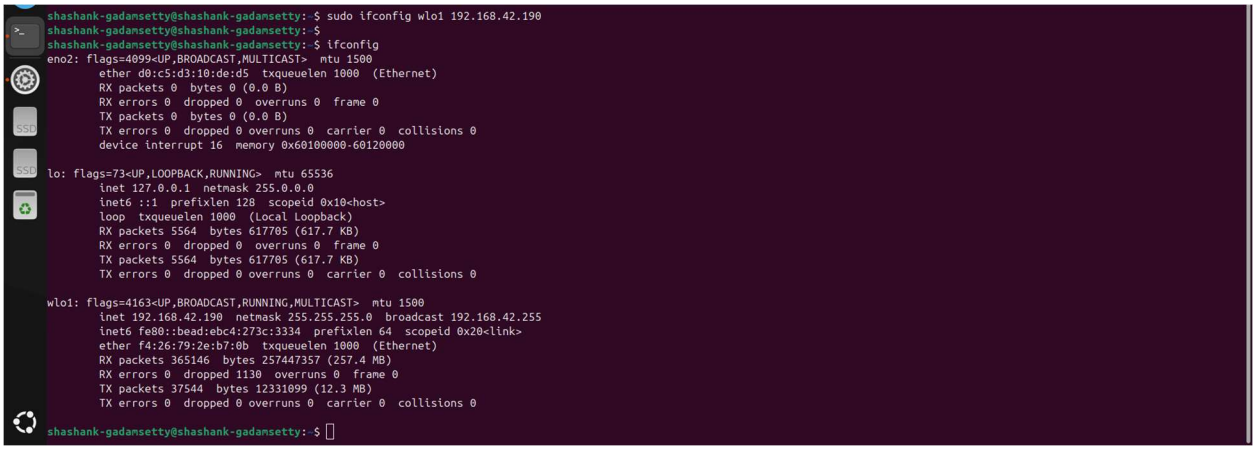
b) They are different. This is because the IP address in the ifconfig is for a private network. But the second one is IP address for a public network. IP address are unique over a network.



# Question 2)

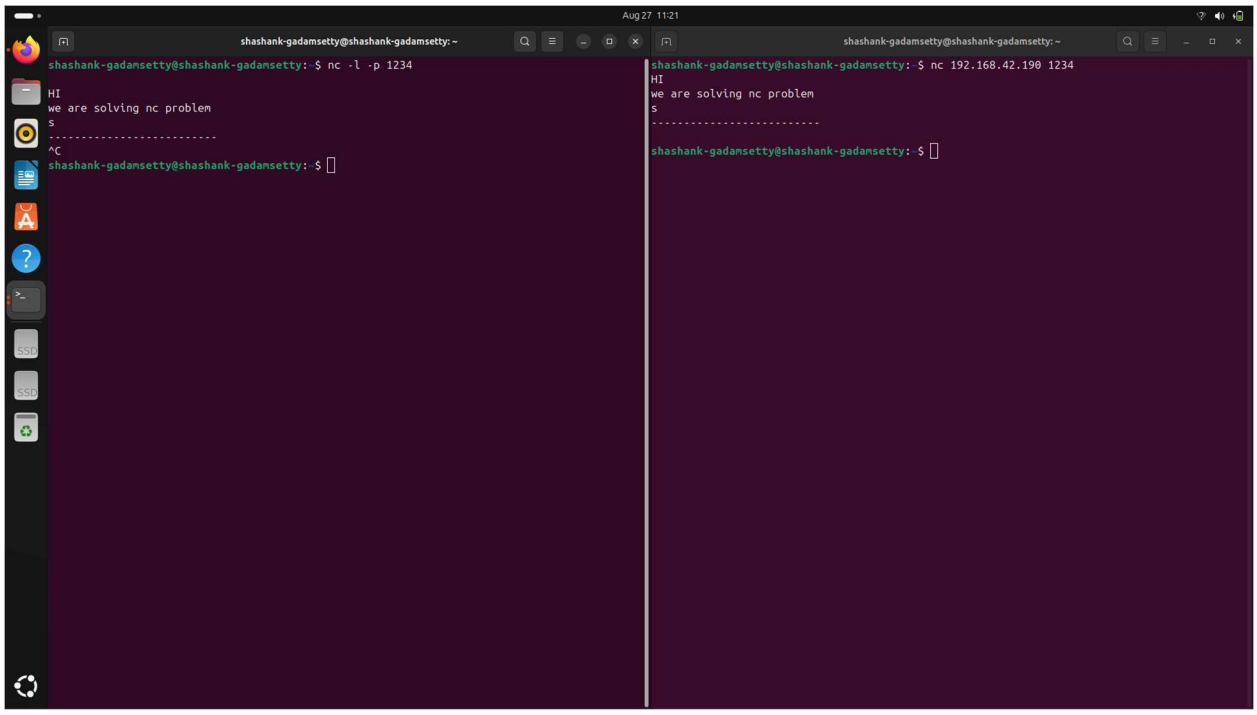
a)


Aug 27 10:51
shashank-gadamsetty@shashank-gadamsetty: ~
shashank-gadamsetty@shashank-gadamsetty:~$ sudo ifconfig wlo1 1.1.1.1
[sudo] password for shashank-gadamsetty:
shashank-gadamsetty@shashank-gadamsetty:~$ ifconfig
eno2: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
ether d0:c5:d3:10:de:d5  txqueuelen 1000  (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
device interrupt 16  memory 0x60100000-60120000
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 5386  bytes 601013 (601.0 KB)
RX errors 0  dropped 0  overruns 0  frame 0
TX packets 5386  bytes 601013 (601.0 KB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 1.1.1.1  netmask 255.0.0.0  broadcast 1.255.255.255
inet6 fe80::bead:ebc4:273c:3334  prefixlen 64  scopeid 0x20<link>
ether f4:26:79:2e:b7:0b  txqueuelen 1000  (Ethernet)
RX packets 360362  bytes 255258026 (255.2 MB)
RX errors 0  dropped 1110  overruns 0  frame 0
TX packets 37309  bytes 12259506 (12.2 MB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

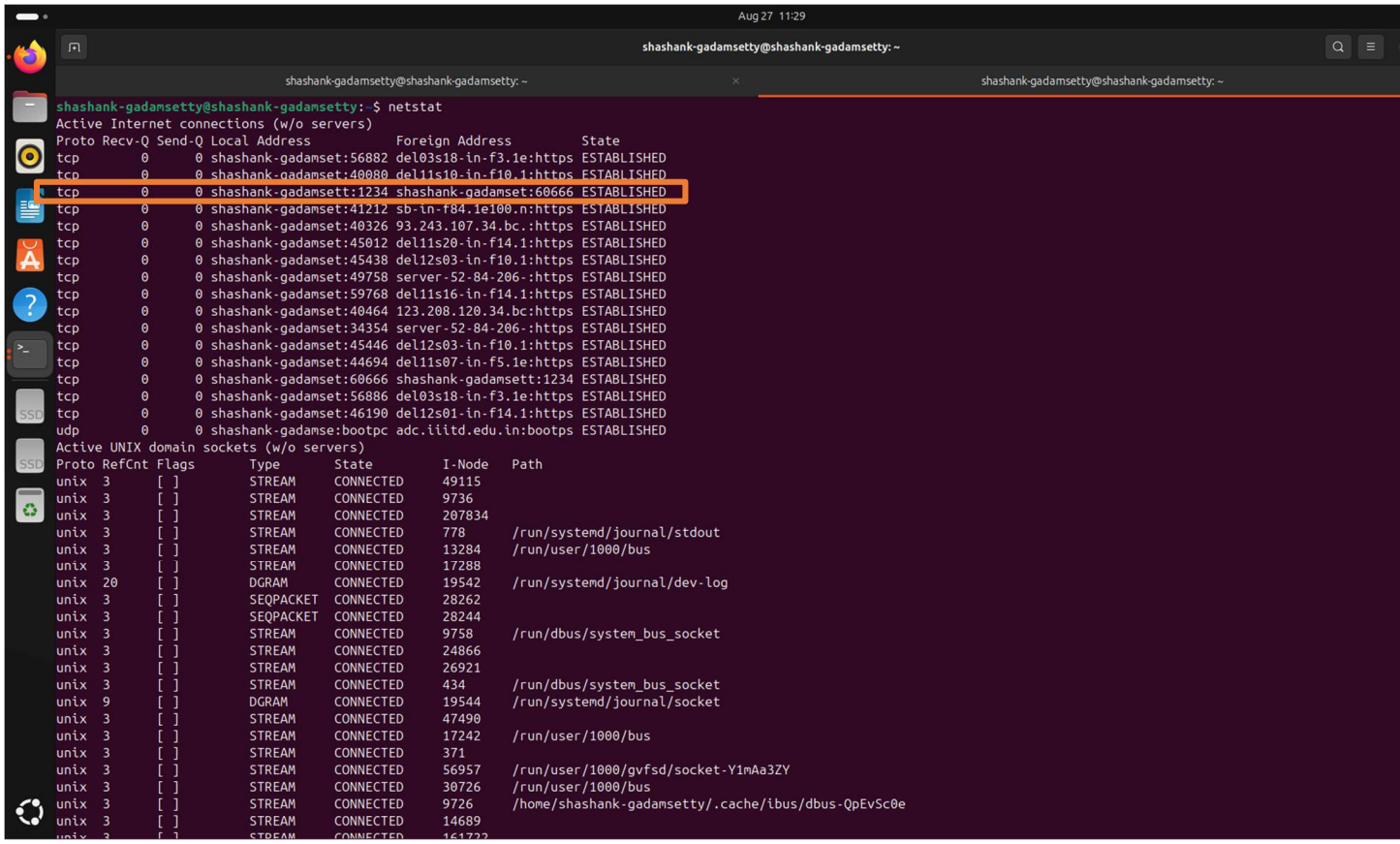

shashank-gadamsetty@shashank-gadamsetty:~$ sudo ifconfig wlo1 192.168.42.190
shashank-gadamsetty@shashank-gadamsetty:~$
shashank-gadamsetty@shashank-gadamsetty:~$ ifconfig
eno2: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
ether d0:c5:d3:10:de:d5  txqueuelen 1000  (Ethernet)
RX packets 0  bytes 0 (0.0 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
device interrupt 16  memory 0x60100000-60120000
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 5564  bytes 617705 (617.7 KB)
RX errors 0  dropped 0  overruns 0  frame 0
TX packets 5564  bytes 617705 (617.7 KB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 192.168.42.190  netmask 255.255.255.0  broadcast 192.168.42.255
inet6 fe80::bead:ebc4:273c:3334  prefixlen 64  scopeid 0x20<link>
ether f4:26:79:2e:b7:0b  txqueuelen 1000  (Ethernet)
RX packets 365146  bytes 257447357 (257.4 MB)
RX errors 0  dropped 1130  overruns 0  frame 0
TX packets 37544  bytes 12331099 (12.3 MB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
shashank-gadamsetty@shashank-gadamsetty:~$

# Question 3)

a)




b)



# Question 4)

- **Run nslookup in Interactive Mode:** Start nslookup without any arguments to enter interactive mode
- **Set the Query Type to NS (Name Server):** Specify that you want to query for the name servers
- **Query for the Domain:** Now, enter the domain name to query.

a)

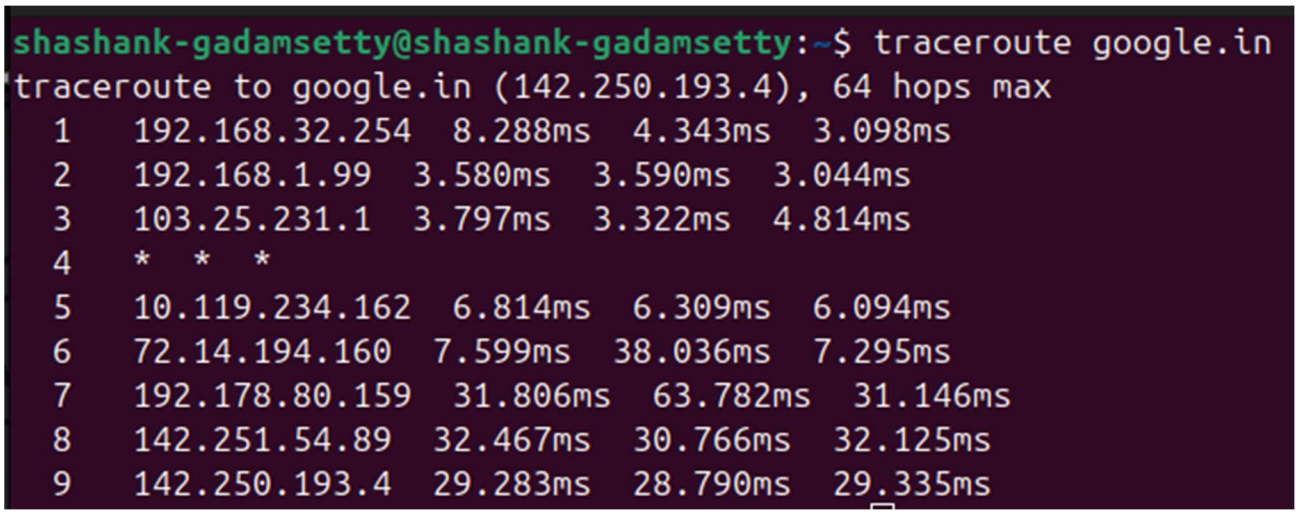
```
shashank-gadamsetty@shashank-gadamsetty:~$ nslookup
> set type=ns
> google.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.in       nameserver = ns3.google.com.
google.in       nameserver = ns2.google.com.
google.in       nameserver = ns1.google.com.
google.in       nameserver = ns4.google.com.

Authoritative answers can be found from:
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  has AAAA address 2001:4860:4802:36::a
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  has AAAA address 2001:4860:4802:34::a
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  has AAAA address 2001:4860:4802:32::a
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  has AAAA address 2001:4860:4802:38::a
>
```

b)

```
shashank-gadamsetty@shashank-gadamsetty:~$ nslookup -debug google.in
Server:         127.0.0.53
Address:        127.0.0.53#53

------------
    QUESTIONS:
        google.in, type = A, class = IN
    ANSWERS:
    ->  google.in
        internet address = 142.250.193.4
        ttl = 300
    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 = 300
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Name:   google.in
Address: 2404:6800:4002:819::2004
```

Question 5)

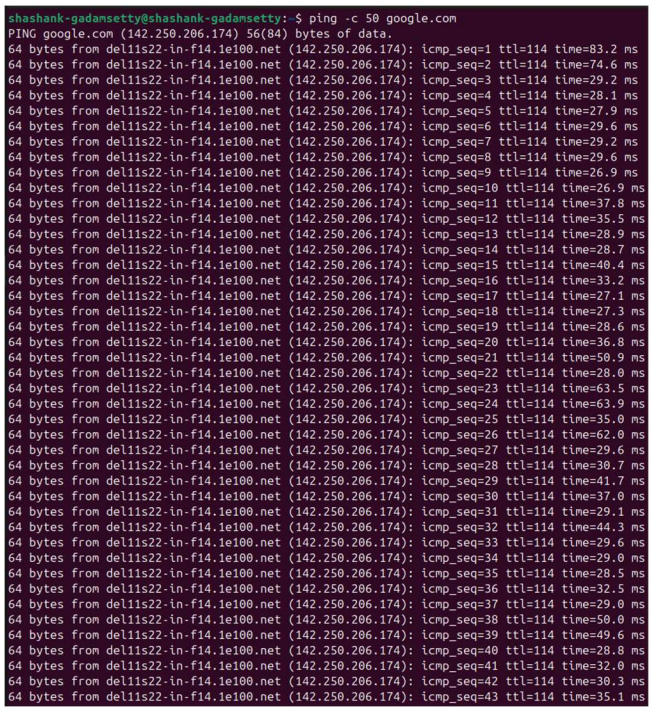
a)




There are 6 intermediate hosts as we are ignoring the *** for this assignment. Their IP addresses are:

| | |
|---|---|
| 192.168.1.99 | 3.404 |
| 103.25.231.1 | 3.977 |
| 10.119.234.162 | 6.406 |
| 72.14.194.160 | 17.643 |
| 192.178.80.159 | 42.244 |
| 142.251.54.89 | 31.786 |

b)




c) The average is 36.213 ms for ping, while fore trace route it is 139.842 ms. This is because ping measures direct round-trip time to the destination without detailing every hop, while traceroute breaks down the trip into multiple hops and measures the time taken to each intermediate host.

d) Comparison of Maximum Traceroute Latency with Ping Latency

The highest average latency from the traceroute results is 42.245 ms (Hop 7: 192.178.80.159). But the average latency from the ping command is 36.213 ms.

They are not matching.

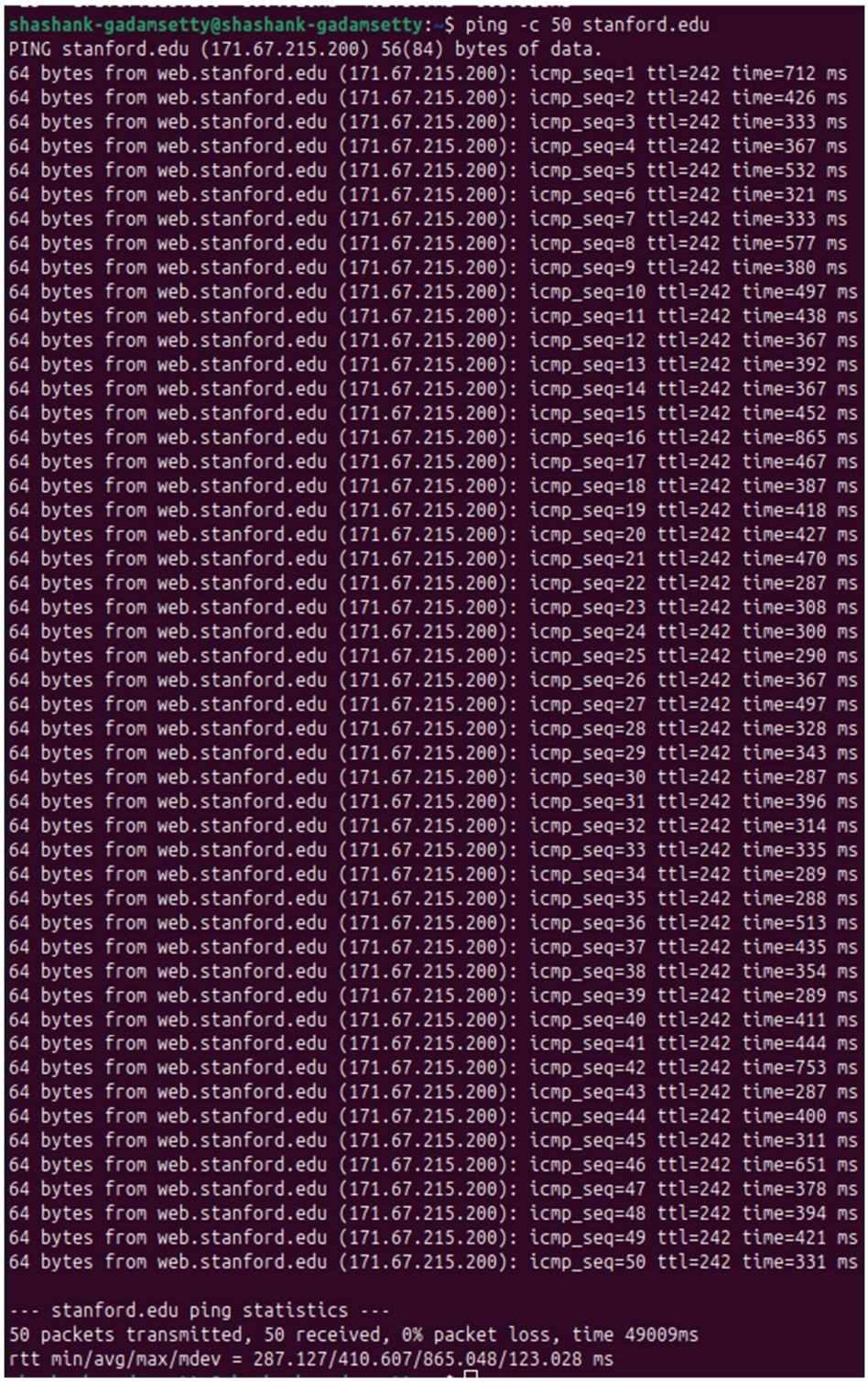
The maximum latency in traceroute could be due to specific network congestion or delays at that particular hop (Hop 7). The ping command measures the latency for the entire round trip to the destination, which might take a different path or be optimized, thus showing a lower average latency.

e) When using the traceroute command, you might see multiple entries for a single hop. These multiple entries indicate that the router or device at that hop is using load balancing or has multiple network interfaces.

- Load Balancing: The router may have multiple paths (routes) to the next hop or the destination, and it distributes packets across these paths to balance the load.
- Multiple Interfaces: The router might have several interfaces (e.g., different physical or virtual ports), and each probe from the traceroute command takes a different route through these interfaces.

This results in multiple round-trip times being recorded for the same hop. Each RTT corresponds to a different path that the probe packets have taken to get through that hop. These entries help to diagnose network behavior such as redundant paths or network resilience but may complicate direct comparisons of latency across hops.

f)




Average latency is 410.607

g)

```
shashank-gadamsetty@shashank-gadamsetty:~$ traceroute stanford.edu
traceroute to stanford.edu (171.67.215.200), 64 hops max
  1   192.168.32.254  4.433ms  8.237ms  14.289ms
  2   192.168.1.99  2.656ms  2.970ms  2.840ms
  3   103.25.231.1  5.828ms  3.403ms  3.947ms
  4   10.1.209.201  31.785ms  30.349ms  31.547ms
  5   10.1.200.137  50.265ms  34.373ms  33.639ms
  6   10.255.238.122  33.986ms  32.917ms  34.757ms
  7   180.149.48.18  31.537ms  28.319ms  28.506ms
  8   *  *  *
  9   *  *  *
 10   *  *  *
 11   *  *  *
 12   *  *  *
 13   *  *  *
 14   *  *  *
 15   *  *  *
 16   *  *  *
 17   *  *  *
 18   *  *  *
 19   *  *  *
 20   *  *  *
 21   *  *  *
 22   *  *  *
 23   171.64.255.232  674.859ms  518.057ms  437.200ms
 24   171.66.255.200  625.793ms  368.197ms  325.715ms
 25   171.67.215.200  399.920ms  402.599ms  301.325ms
```

There are 9 hops (not counting * * *) as outputted by traceroute Stanford.edu. There are 7 hops in traceroute google.in. This can be because of direct route may not be available so readily in router tables for Stanford.edu as compared to google.in.

Google.in might have more optimized or direct routes available due to Google's extensive and well-distributed global infrastructure, which could lead to fewer hops. Google, being a global tech giant, likely has servers that are closer to your location or more integrated into various ISP networks. This result in fewer hops.

g) The servers for google.in are likely geographically closer to your location, possibly even within your country or region, due to Google's extensive global infrastructure.

The servers for stanford.edu on the other hand are likely located in California, USA, which could be much farther from your location. Greater geographical distance generally results in higher latency due to the longer physical distance that data must travel.

Question 6)

```
shashank-gadamsetty@shashank-gadamsetty:~$ sudo ifconfig lo down
shashank-gadamsetty@shashank-gadamsetty:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
^C
--- 127.0.0.1 ping statistics ---
60 packets transmitted, 0 received, 100% packet loss, time 60434ms
```

First down the local host. Then send a ping to the address.

# OR

```
shashank-gadamsetty@shashank-gadamsetty:~$ sudo iptables -I INPUT -p icmp --icmp-type echo-
request -j DROP
shashank-gadamsetty@shashank-gadamsetty:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
^C
--- 127.0.0.1 ping statistics ---
115 packets transmitted, 0 received, 100% packet loss, time 116750ms

shashank-gadamsetty@shashank-gadamsetty:~$
```

To simulate a ping failure to 127.0.0.1

On Linux systems, you can use iptables or ufw to block ICMP packets.

**Linux Example with iptables:**

sudo iptables -I INPUT -p icmp --icmp-type echo-request -j DROP

This command drops incoming ICMP echo requests (which are used by the ping command).