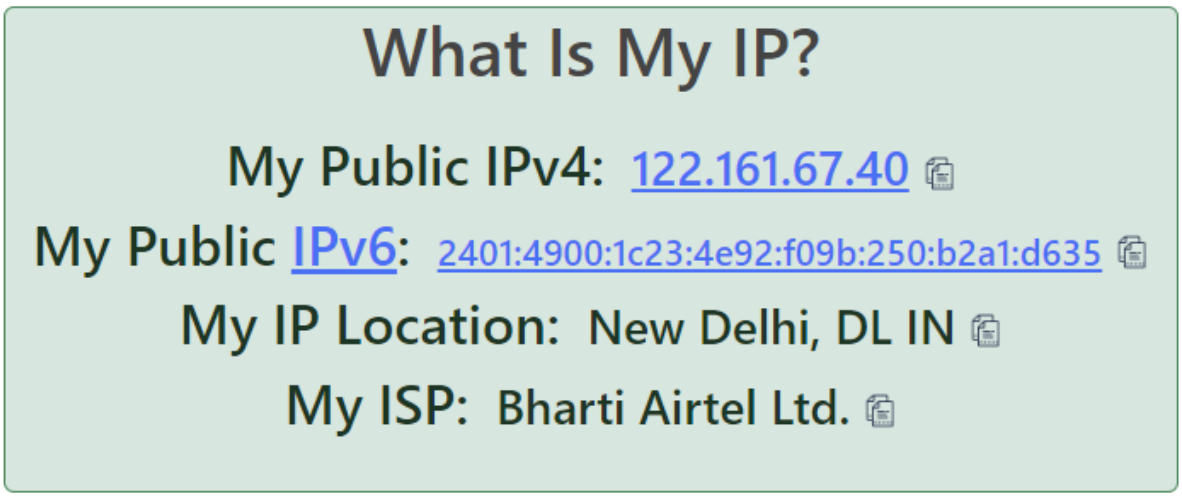
Q1)

a) IP address: 172.30.22.38

```
kartikeya@Kartikeya:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1400
        inet 172.30.22.38  netmask 255.255.240.0  broadcast 172.30.31.255
        inet6 fe80::215:5dff:fe77:958f  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:77:95:8f  txqueuelen 1000  (Ethernet)
        RX packets 2168  bytes 541231 (541.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 266  bytes 60381 (60.3 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 150  bytes 14345 (14.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 150  bytes 14345 (14.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

b) No, my IP address through ifconfig is different from IP address shown on https://www.whatismyip.com because the IP address through ifconfig command is the private IP address that is used for the local network and cannot be used as a public IP address, it is assigned by the router for communication between the devices on the same network. The IP address on the website shown is different because it is assigned by the internet service provider and is used to for accessing data online.



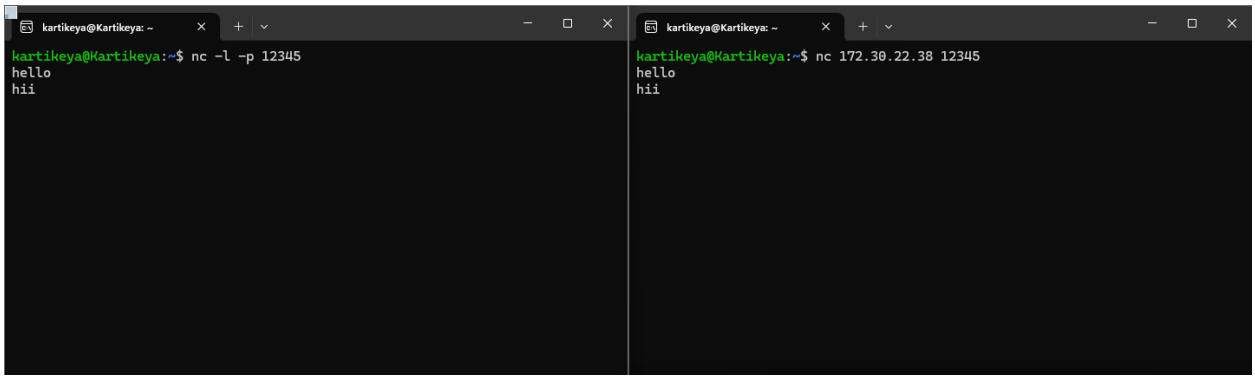
Q2)

a)

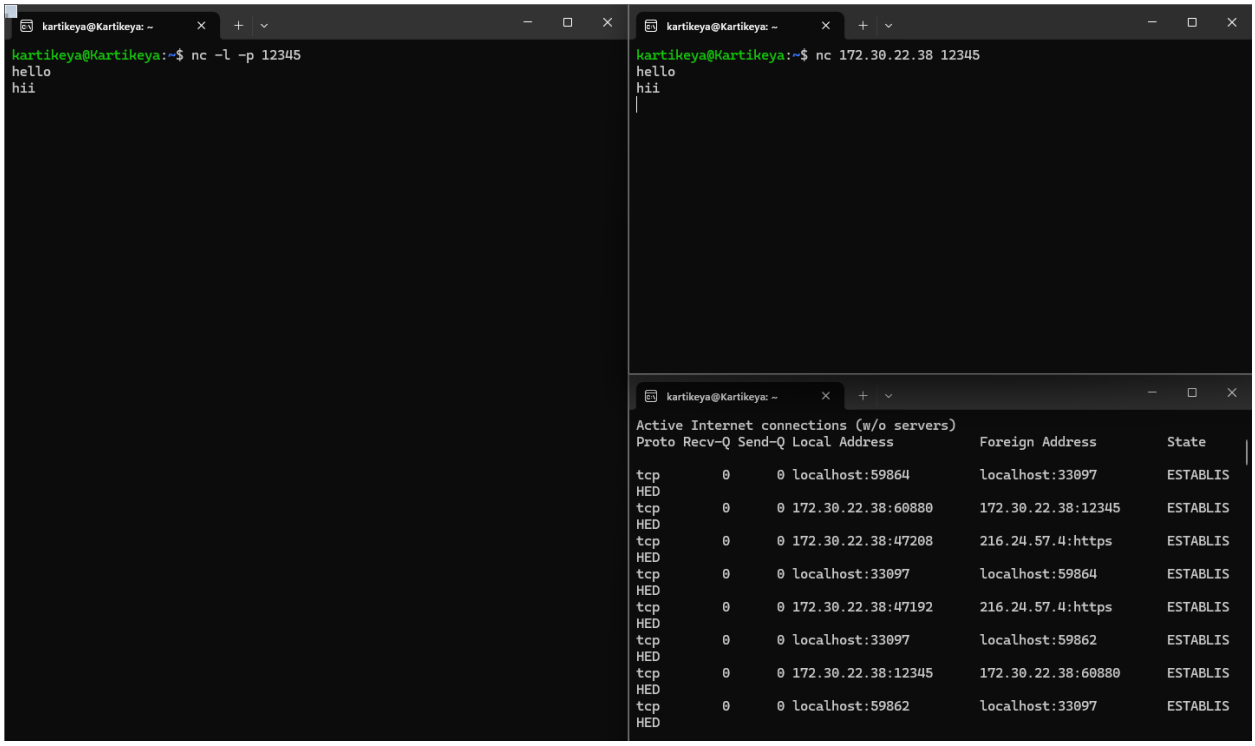
```
kartikeya@Kartikeya:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1400
        inet 172.30.22.38  netmask 255.255.0.0  broadcast 172.30.255.255
        inet6 fe80::215:5dff:fe77:958f  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:77:95:8f  txqueuelen 1000  (Ethernet)
        RX packets 6597  bytes 4776973 (4.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1169  bytes 132985 (132.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kartikeya@Kartikeya:~$ sudo ifconfig eth0 191.23.34.69
kartikeya@Kartikeya:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1400
        inet 191.23.34.69  netmask 255.255.0.0  broadcast 191.23.255.255
        inet6 fe80::215:5dff:fe77:958f  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:77:95:8f  txqueuelen 1000  (Ethernet)
        RX packets 6601  bytes 4777420 (4.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1169  bytes 132985 (132.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kartikeya@Kartikeya:~$ sudo ifconfig eth0 172.30.22.38
kartikeya@Kartikeya:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1400
        inet 172.30.22.38  netmask 255.255.0.0  broadcast 172.30.255.255
        inet6 fe80::215:5dff:fe77:958f  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:77:95:8f  txqueuelen 1000  (Ethernet)
        RX packets 6602  bytes 4777506 (4.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1169  bytes 132985 (132.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kartikeya@Kartikeya:~$
```

Q3)

a)



b) The state of the TCP connection is ESTABLISHED.



(in the right bottom tab we can see
tcp 0 0 172.30.22.38:60880 172.30.22.38:12345 ESTABLISHED)

Q4)

a)

```
kartikeya@Kartikeya:~$ nslookup -type=ns google.in
Server:         10.255.255.254
Address:        10.255.255.254#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

kartikeya@Kartikeya:~$ nslookup google.in ns3.google.com
Server:         ns3.google.com
Address:        216.239.36.10#53

Name:   google.in
Address: 142.250.194.196
Name:   google.in
Address: 2404:6800:4002:824::2004
```

I have set the flag type to `ns` because we wanted to retrieve the name servers for the domain `google.in`. After that, I used `nslookup` again with one of those name servers to obtain an authoritative answer for "google.in."

Q4)

b)

```
kartikeya@Kartikeya:~$ nslookup -debug google.com
Server:         10.255.255.254
Address:        10.255.255.254#53

------------
    QUESTIONS:
        google.com, type = A, class = IN
    ANSWERS:
    ->  google.com
        internet address = 142.250.206.174
        ttl = 48
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Non-authoritative answer:
Name:   google.com
Address: 142.250.206.174
------------
    QUESTIONS:
        google.com, type = AAAA, class = IN
    ANSWERS:
    ->  google.com
        has AAAA address 2404:6800:4002:82d::200e
        ttl = 215
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Name:   google.com
Address: 2404:6800:4002:82d::200e
```

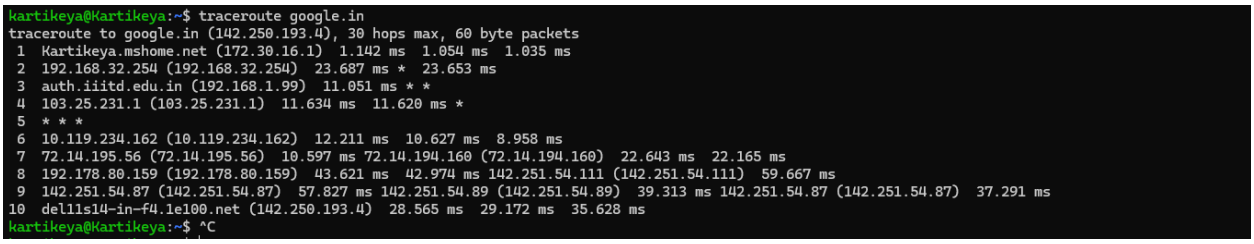
I have used the nslookup -debug google.com to query DNS records for google.com entry which provides the ip address along with the TTL value.

The TTL value for IPv4 address is 48 seconds and the TTL value for IPv6 address is 215 seconds and these entries will expire from local DNS after this time.

Q5)

a) We have total 10 visible intermediate hosts:
    1) 172.30.16.1
    2) 192.168.32.254
    3) 192.168.1.99
    4) 103.25.231.1
    5) 10.119.234.162

6) 72.14.195.56 and 72.14.194.160
7) 192.178.80.159 and 142.251.54.111
8) 142.251.54.87 and 142.251.54.89



Average Latency to Each Intermediate Host:

Hop 1 (172.30.16.1): Average Latency: 1.077 ms

Hop 2 (192.168.32.254): Average Latency: 23.67 ms

Hop 3 (192.168.1.99): Average Latency: 11.051 ms

Hop 4 (103.25.231.1): Average Latency: 11.627 ms

Hop 5 (10.119.234.162): Average Latency: 10.59867 ms

Hop6:

Intermediate IP1(72.14.195.56)
Intermediate IP2(72.14.194.160)
Average Latency: 18.4683 ms

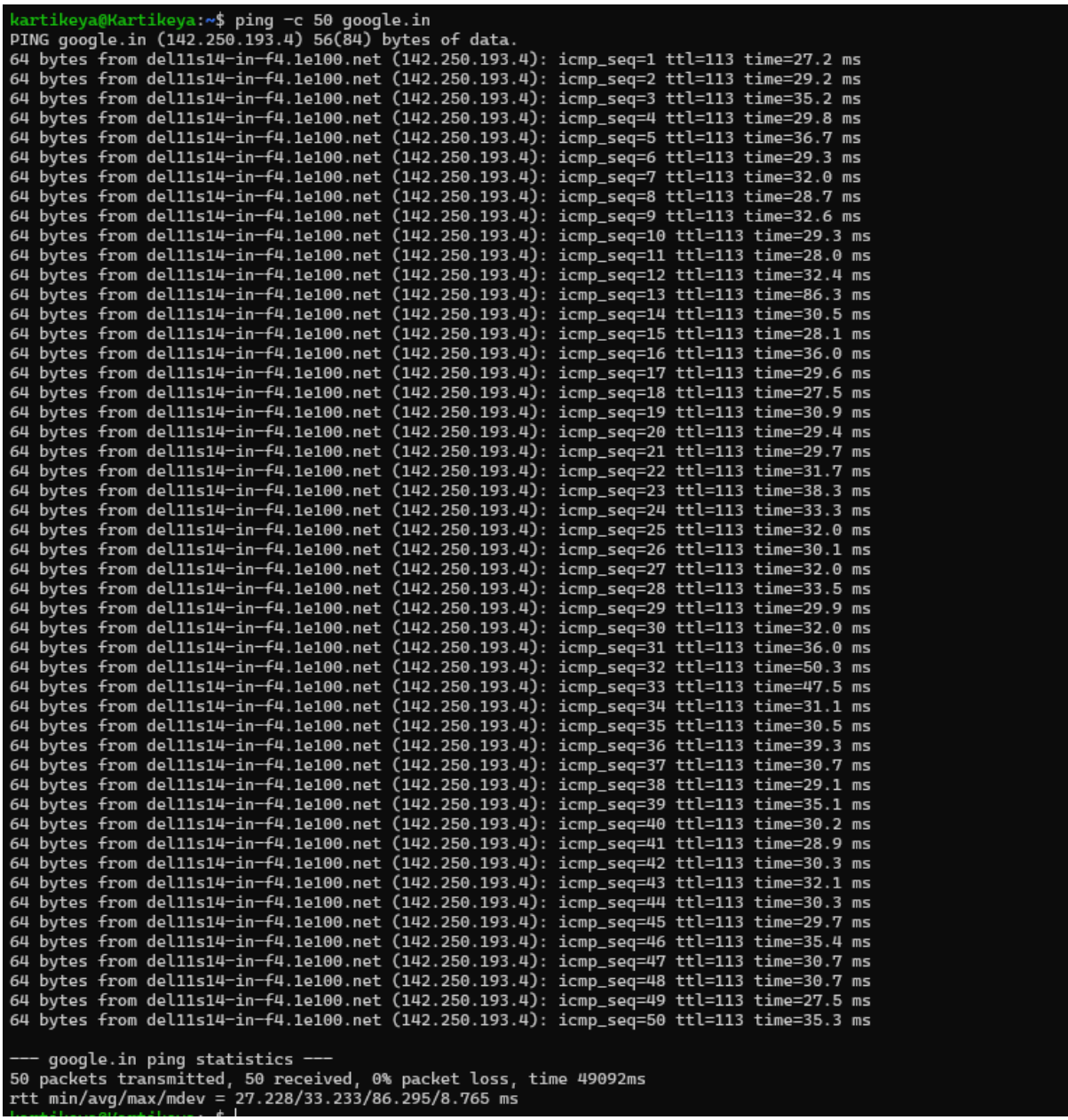
Hop7:

Intermediate IP1(192.178.80.159)
Intermediate IP2(142.251.54.111)
Average Latency: 48.754 ms

Hop8:

Intermediate IP1(142.251.54.87)
Intermediate IP2(142.251.54.89)
Average Latency: 44.8103 ms

b)



Average latency: 33.233 ms as shown in the photo in the end

c) Sum of the latencies of part(a) = 170.05627 ms

traceroute measures cumulative delays as packets traverse multiple hops, which can increase the total time as each hop adds a small delay. ping directly measures only the round trip to the final destination, not accounting for the delay at each intermediate hop. The sum of the latencies from traceroute is generally larger because it represents the cumulative delay of each hop to the destination. In contrast, ping provides a direct measure to the destination's average round-trip time, making the results different.

d) Maximum latency in traceout=48.754 ms
Average latency in ping=33.233 ms

Traceout command maximum latency is greater than the average ping command latency because of its additional delays in each hop.

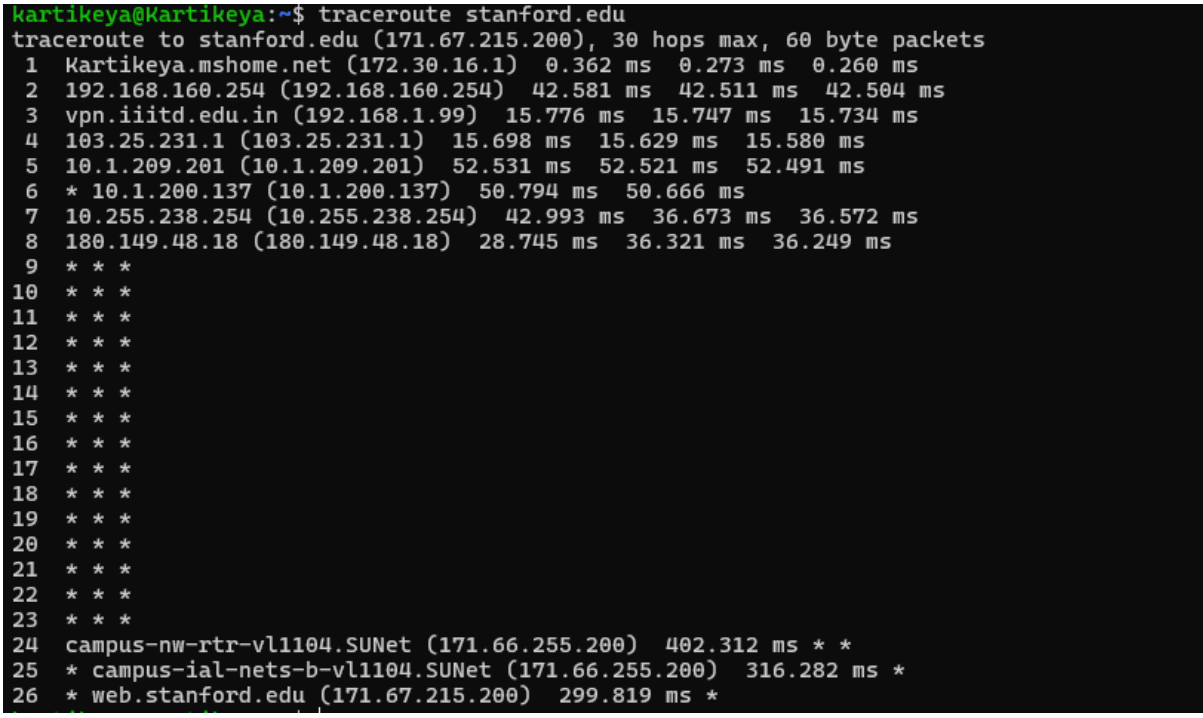
e) Multiple entries for a single hop in a traceroute result indicate that the traceroute command sends multiple packets to the same hop to measure the time it takes for each packet to reach that hop. This helps in identifying network congestion, packet loss, or variability in the path taken by the packets.

f)

```
kartikeya@Kartikeya:~$ 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=241 time=294 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=2 ttl=241 time=308 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=3 ttl=241 time=341 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=4 ttl=241 time=296 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=5 ttl=241 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=6 ttl=241 time=294 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=7 ttl=241 time=333 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=8 ttl=241 time=349 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=9 ttl=241 time=366 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=10 ttl=241 time=393 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=11 ttl=241 time=316 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=12 ttl=241 time=293 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=13 ttl=241 time=290 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=14 ttl=241 time=375 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=15 ttl=241 time=297 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=16 ttl=241 time=317 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=17 ttl=241 time=341 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=18 ttl=241 time=290 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=19 ttl=241 time=290 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=20 ttl=241 time=307 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=21 ttl=241 time=330 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=22 ttl=241 time=355 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=23 ttl=241 time=376 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=24 ttl=241 time=301 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=25 ttl=241 time=297 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=26 ttl=241 time=340 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=27 ttl=241 time=363 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=28 ttl=241 time=291 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=29 ttl=241 time=307 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=30 ttl=241 time=326 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=31 ttl=241 time=290 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=32 ttl=241 time=377 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=33 ttl=241 time=395 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=34 ttl=241 time=314 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=35 ttl=241 time=494 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=36 ttl=241 time=365 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=37 ttl=241 time=384 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=38 ttl=241 time=306 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=39 ttl=241 time=330 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=40 ttl=241 time=348 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=41 ttl=241 time=291 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=42 ttl=241 time=349 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=43 ttl=241 time=317 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=44 ttl=241 time=337 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=45 ttl=241 time=359 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=46 ttl=241 time=349 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=47 ttl=241 time=299 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=48 ttl=241 time=324 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=49 ttl=241 time=308 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=50 ttl=241 time=379 ms

--- stanford.edu ping statistics ---
50 packets transmitted, 50 received, 0% packet loss, time 49070ms
rtt min/avg/max/mdev = 289.227/331.586/494.277/39.307 ms
```

Average Latency = 331.586 ms as we can see at the end of the image.

g)



For Stanford.edu there are 25 hops where as for google.in there are 9 hops.

h) Latency for google.in = 33.233 ms
Latency for Stanford.edu = 331.586 ms
We can see that to reach the google.in server we need 9 hops and for reaching Stanford.edu we need 25 hops. This may be because the direct routing path of google.in is more closer to my network as compared to standford.edu.

Q6)

```
kartikeya@Kartikeya:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.30.22.38  netmask 255.255.240.0  broadcast 172.30.31.255
        inet6 fe80::215:5dff:fe22:c86f  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:22:c8:6f  txqueuelen 1000  (Ethernet)
        RX packets 3355  bytes 646534 (646.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 590  bytes 86517 (86.5 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 440  bytes 40054 (40.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 440  bytes 40054 (40.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kartikeya@Kartikeya:~$ sudo ifconfig lo down
kartikeya@Kartikeya:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.30.22.38  netmask 255.255.240.0  broadcast 172.30.31.255
        inet6 fe80::215:5dff:fe22:c86f  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:22:c8:6f  txqueuelen 1000  (Ethernet)
        RX packets 3355  bytes 646534 (646.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 591  bytes 86587 (86.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kartikeya@Kartikeya:~$ 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 ---
10 packets transmitted, 0 received, 100% packet loss, time 9323ms
```

So in this we have disabled the lookback interface (lo) because it is responsible for internal communication within the machine and 127.0.0.1 is its IPv4 address. Since it is disabled so in this case we would suffer 100% packet loss.