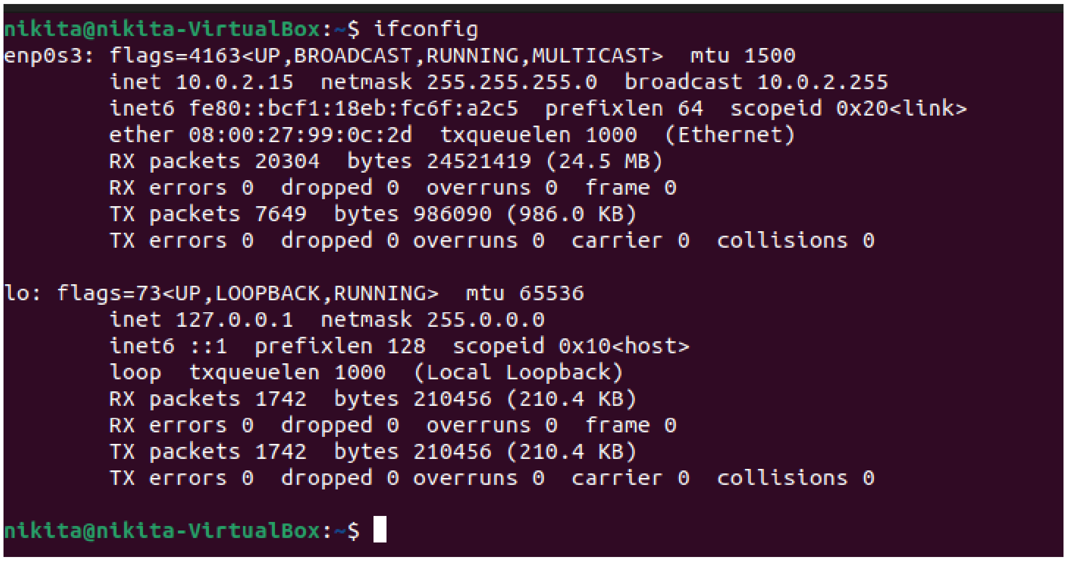
CSE 232: Assignment 1
Nikita Verma | 2021546

Q1)

a)



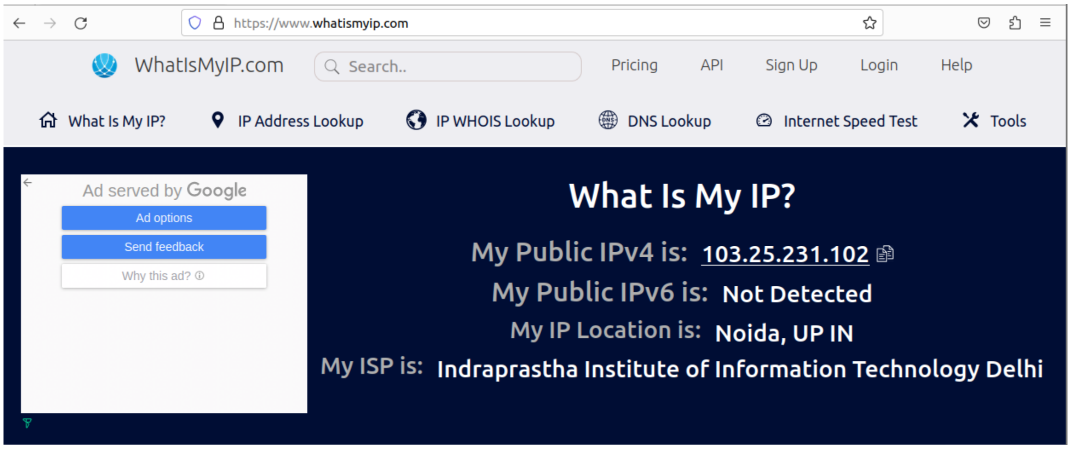
```
nikita@nikita-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::bcf1:18eb:fc6f:a2c5  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:99:0c:2d  txqueuelen 1000  (Ethernet)
        RX packets 20304  bytes 24521419 (24.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7649  bytes 986090 (986.0 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 1742  bytes 210456 (210.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1742  bytes 210456 (210.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

nikita@nikita-VirtualBox:~$ 
```

It displays the currently active network interface configuration information. Here, enp0s3 is the default network interface and lo stands for loopback.

We use enp0s3 to figure out the ip address which is present after inet.

IP address is 10.0.2.15

b)



What Is My IP?

My Public IPv4 is: 103.25.231.102

My Public IPv6 is: Not Detected

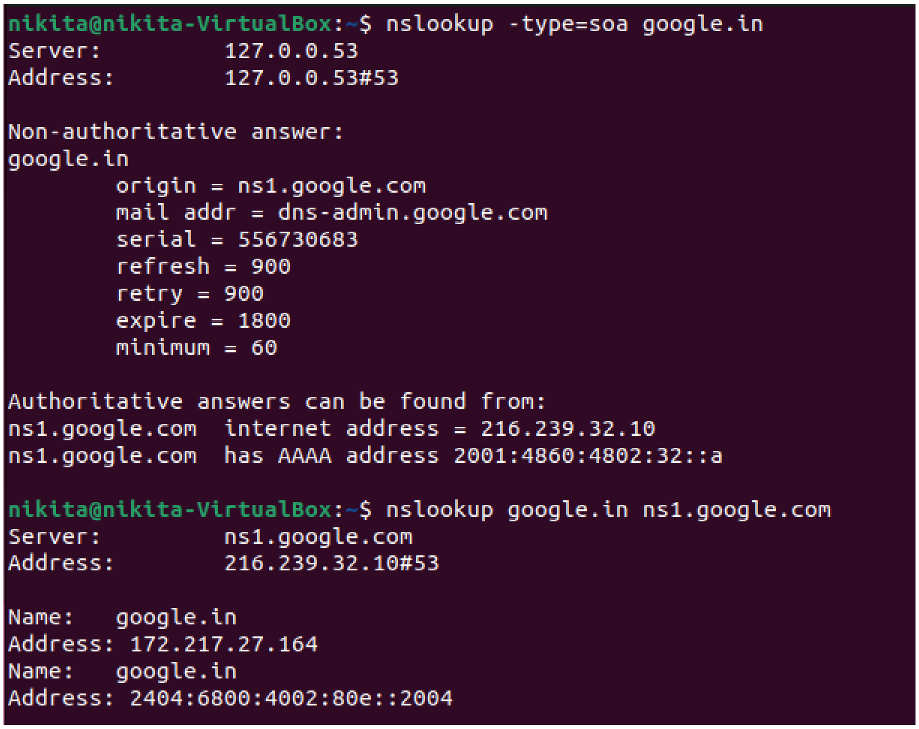
My IP Location is: Noida, UP IN

My ISP is: Indraprastha Institute of Information Technology Delhi

IP Address is 103.25.231.102

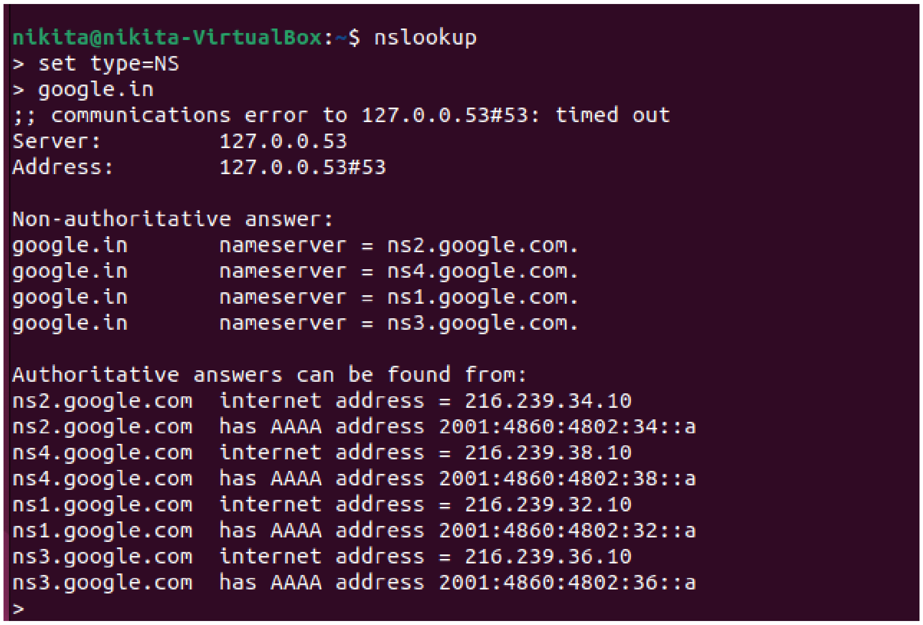
The value of IP address obtained is not the same because ifconfig displays the local/private IP address which is part of LAN whereas the website returns the public IP address of my connection (router or modem) which is part of WAN.

Q2)



```
nikita@nikita-VirtualBox:~$ nslookup -type=soa google.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.in
        origin = ns1.google.com
        mail addr = dns-admin.google.com
        serial = 556730683
        refresh = 900
        retry = 900
        expire = 1800
        minimum = 60

Authoritative answers can be found from:
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  has AAAA address 2001:4860:4802:32::a

nikita@nikita-VirtualBox:~$ nslookup google.in ns1.google.com
Server:         ns1.google.com
Address:        216.239.32.10#53

Name:   google.in
Address: 172.217.27.164
Name:   google.in
Address: 2404:6800:4002:80e::2004
```

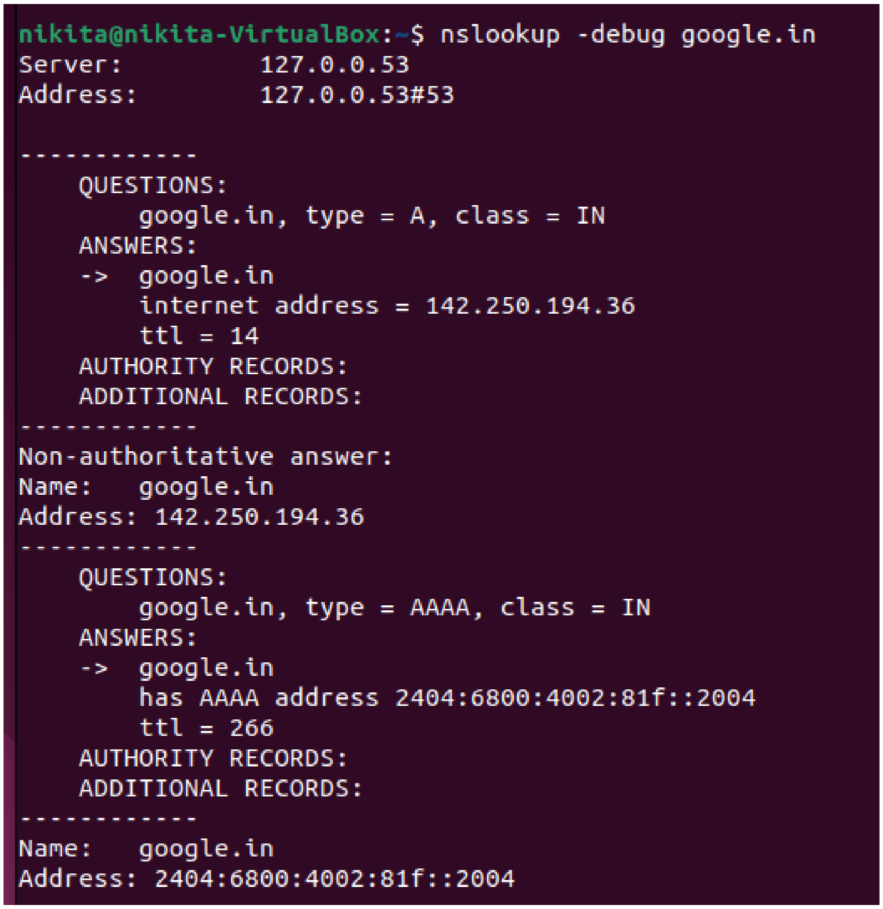
I used the record type SOA (Start of Authority) to obtain information about the authoritative name server for google.in which is ns1.google.com. Then I used nslookup command again with the primary server name which gave me the authoritative result.



```
nikita@nikita-VirtualBox:~$ nslookup
> set type=NS
> google.in
;; communications error to 127.0.0.53#53: timed out
Server:         127.0.0.53
Address:        127.0.0.53#53

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

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

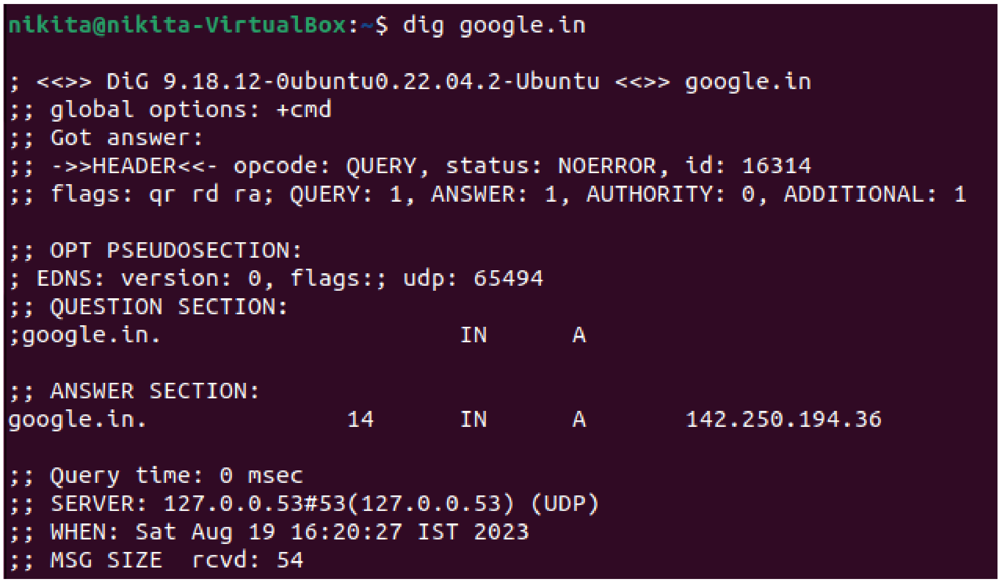
This is another way we can find the primary server from which we can get authoritative result. I set the type as NS(name server) which gave me the list of authoritative name servers which I can further use in nslookup command like I did above.

b) We can find the TTL using nslookup or dig command.



```
nikita@nikita-VirtualBox:~$ 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 = 142.250.194.36
        ttl = 14
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Non-authoritative answer:
Name:   google.in
Address: 142.250.194.36
------------
    QUESTIONS:
        google.in, type = AAAA, class = IN
    ANSWERS:
    ->  google.in
        has AAAA address 2404:6800:4002:81f::2004
        ttl = 266
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Name:   google.in
Address: 2404:6800:4002:81f::2004
```

The TTL is 14 seconds for IPv4 address and 266 seconds for IPv6 address. This entry would expire from the local DNS server of type A in 14 seconds and of type AAAA in 266 seconds.

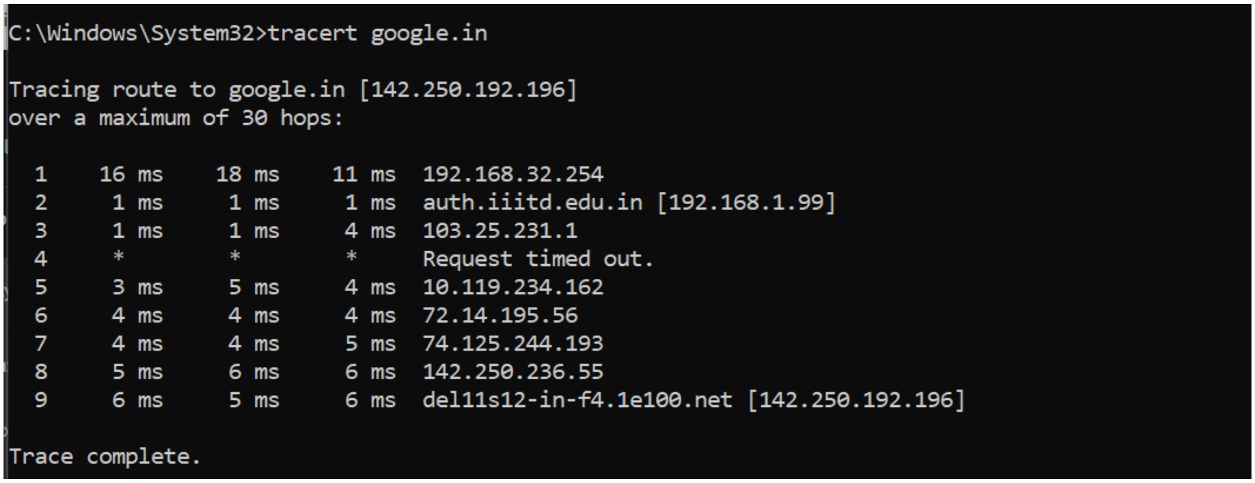


```
nikita@nikita-VirtualBox:~$ dig google.in

; <<>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<>> google.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16314
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.in.                     IN      A

;; ANSWER SECTION:
google.in.              14      IN      A       142.250.194.36

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Aug 19 16:20:27 IST 2023
;; MSG SIZE  rcvd: 54
```

Using dig command we got the TTL as 14 seconds for IPv4 address(type A).

3)

a)



```
C:\Windows\System32>tracert google.in

Tracing route to google.in [142.250.192.196]
over a maximum of 30 hops:

  1    16 ms    18 ms    11 ms  192.168.32.254
  2     1 ms     1 ms     1 ms  auth.iiitd.edu.in [192.168.1.99]
  3     1 ms     1 ms     4 ms  103.25.231.1
  4     *        *        *     Request timed out.
  5     3 ms     5 ms     4 ms  10.119.234.162
  6     4 ms     4 ms     4 ms  72.14.195.56
  7     4 ms     4 ms     5 ms  74.125.244.193
  8     5 ms     6 ms     6 ms  142.250.236.55
  9     6 ms     5 ms     6 ms  del11s12-in-f4.1e100.net [142.250.192.196]

Trace complete.
```

The first IP address is of my system(source) and the last is the destination. So there are 7 intermediate hosts in the route to our destination.(6 after ignoring “***”)

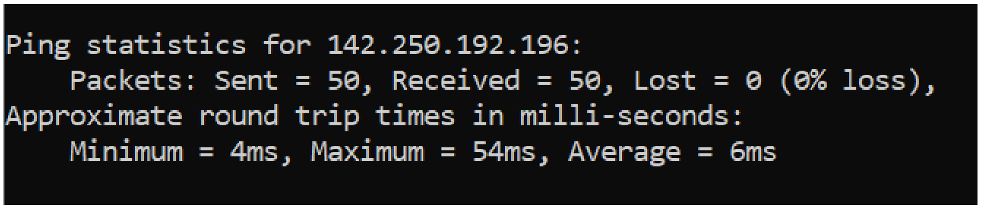
The IP addresses of the hosts are given after the 3 column of RTT for each hop.

The average latency will be half of the average round trip time.

Average latency of all host in order is:

1. Latency = ((16+18+11)/3)/2 = 7.5 ms
2. Latency = ((1+1+1)/3)/2 = 0.5 ms
3. Latency = ((1+1+4)/3)/2 = 1ms
4. Latency = ((3+5+4)/3)/2 = 2 ms
5. Latency = ((4+4+4)/3)/2 = 2 ms
6. Latency = ((4+4+5)/3)/2 = 2.167 ms
7. Latency = ((5+6+6)/3)/2 = 2.83 ms
8. Latency = ((6+5+6)/3)/2 = 2.83 ms

b)



```
Ping statistics for 142.250.192.196:
    Packets: Sent = 50, Received = 50, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 54ms, Average = 6ms
```

Command used to send 50 pings to google.in = ping -n 50 google.in

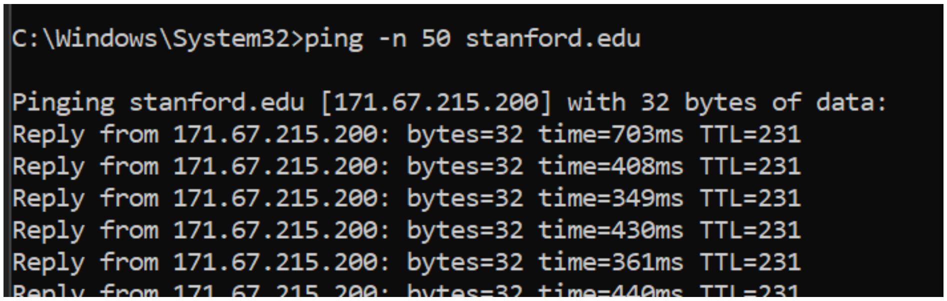
Average latency = (average rtt)/2 = 6/2 = 3ms

c) Sum of average latencies of all hosts in (a) is 20.827 ms however the average latency in (b) is 3 ms which is much lesser. This is because tracert involves sending packets to each node along the way and waiting for its timeout response whereas a ping just forwards packet and doesnt wait for response.

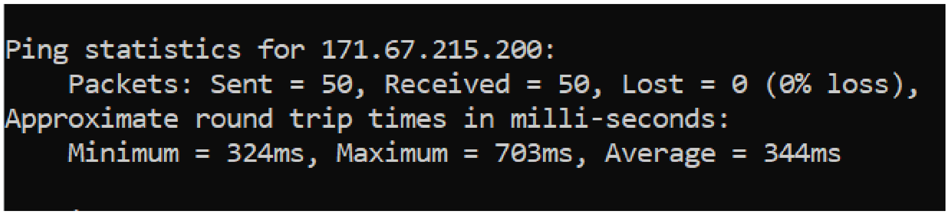
d) The maximum latency in (a) is 7.5ms and average latency in (b) is 3ms. They still don't match but are more comparable now as we are looking at the response time of a single host rather than the sum.

e) The first column is the hop number. The next three column are the RTT for the packet reach that point and return. SInce tracert sends three separate signals, there are three RTT times. Last column is the IP address of router. If domain name is available, it is displayed too. Three signals are sent to display the consistency of network.

f)



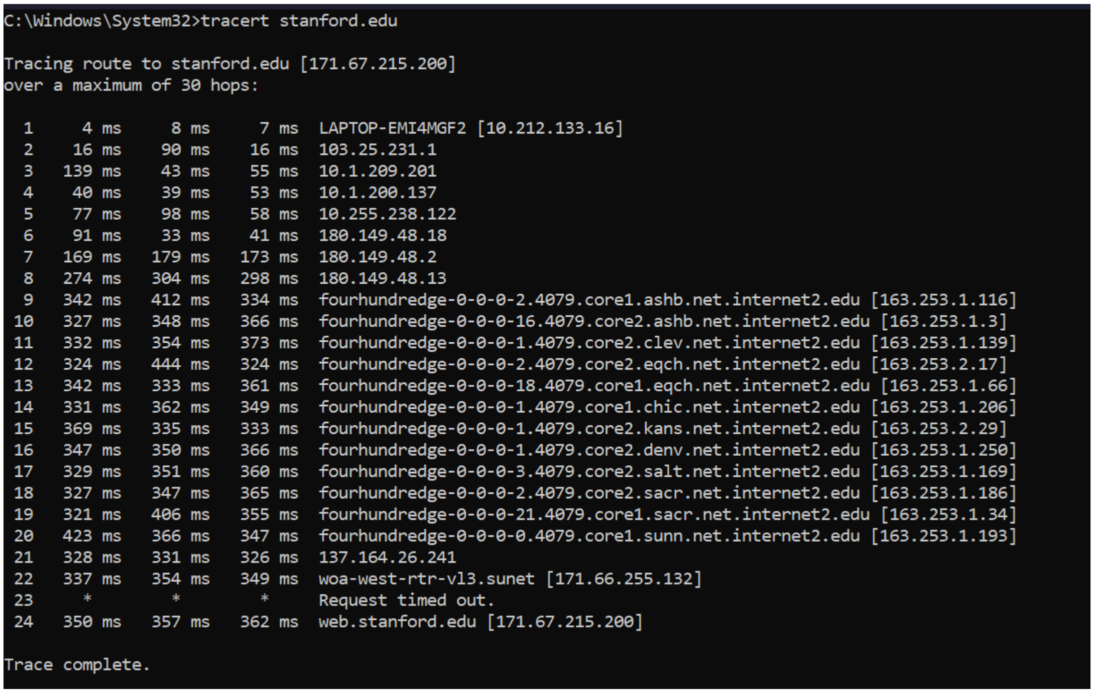
```
C:\Windows\System32>ping -n 50 stanford.edu

Pinging stanford.edu [171.67.215.200] with 32 bytes of data:
Reply from 171.67.215.200: bytes=32 time=703ms TTL=231
Reply from 171.67.215.200: bytes=32 time=408ms TTL=231
Reply from 171.67.215.200: bytes=32 time=349ms TTL=231
Reply from 171.67.215.200: bytes=32 time=430ms TTL=231
Reply from 171.67.215.200: bytes=32 time=361ms TTL=231
Reply from 171.67.215.200: bytes=32 time=440ms TTL=231
```



```
Ping statistics for 171.67.215.200:
    Packets: Sent = 50, Received = 50, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 324ms, Maximum = 703ms, Average = 344ms
```

Average latency = average rtt/2 = 344/2 = 172ms.

g)



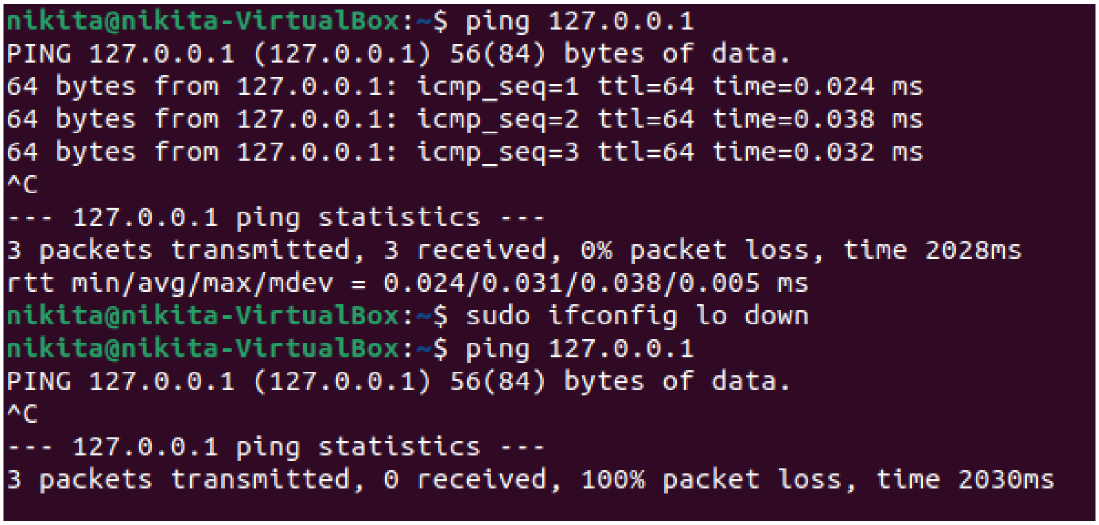
```
C:\Windows\System32>tracert stanford.edu

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

  1     4 ms     8 ms     7 ms  LAPTOP-EMI4MGF2 [10.212.133.16]
  2    16 ms    90 ms    16 ms  103.25.231.1
  3   139 ms    43 ms    55 ms  10.1.209.201
  4    40 ms    39 ms    53 ms  10.1.200.137
  5    77 ms    98 ms    58 ms  10.255.238.122
  6    91 ms    33 ms    41 ms  180.149.48.18
  7   169 ms   179 ms   173 ms  180.149.48.2
  8   274 ms   304 ms   298 ms  180.149.48.13
  9   342 ms   412 ms   334 ms  fourhundredge-0-0-0-2.4079.core1.ashb.net.internet2.edu [163.253.1.116]
 10   327 ms   348 ms   366 ms  fourhundredge-0-0-0-16.4079.core2.ashb.net.internet2.edu [163.253.1.3]
 11   332 ms   354 ms   373 ms  fourhundredge-0-0-0-1.4079.core2.clev.net.internet2.edu [163.253.1.139]
 12   324 ms   444 ms   324 ms  fourhundredge-0-0-0-2.4079.core2.eqch.net.internet2.edu [163.253.2.17]
 13   342 ms   333 ms   361 ms  fourhundredge-0-0-0-18.4079.core1.eqch.net.internet2.edu [163.253.1.66]
 14   331 ms   362 ms   349 ms  fourhundredge-0-0-0-1.4079.core1.chic.net.internet2.edu [163.253.1.206]
 15   369 ms   335 ms   333 ms  fourhundredge-0-0-0-1.4079.core2.kans.net.internet2.edu [163.253.2.29]
 16   347 ms   350 ms   366 ms  fourhundredge-0-0-0-1.4079.core2.denv.net.internet2.edu [163.253.1.250]
 17   329 ms   351 ms   360 ms  fourhundredge-0-0-0-3.4079.core2.salt.net.internet2.edu [163.253.1.169]
 18   327 ms   347 ms   365 ms  fourhundredge-0-0-0-2.4079.core2.sacr.net.internet2.edu [163.253.1.186]
 19   321 ms   406 ms   355 ms  fourhundredge-0-0-0-21.4079.core1.sacr.net.internet2.edu [163.253.1.34]
 20   423 ms   366 ms   347 ms  fourhundredge-0-0-0-0.4079.core1.sunn.net.internet2.edu [163.253.1.193]
 21   328 ms   331 ms   326 ms  137.164.26.241
 22   337 ms   354 ms   349 ms  woa-west-rtr-vl3.sunet [171.66.255.132]
 23     *        *        *     Request timed out.
 24   350 ms   357 ms   362 ms  web.stanford.edu [171.67.215.200]

Trace complete.
```

Number of hops for google.in = 9
Number of hops for stanford.edu = 24
Google has less number of hops which means that google servers are closer to my ISP than the stanford servers.

h) Average latency of google.in = 3ms
Average latency of google.in = 172ms

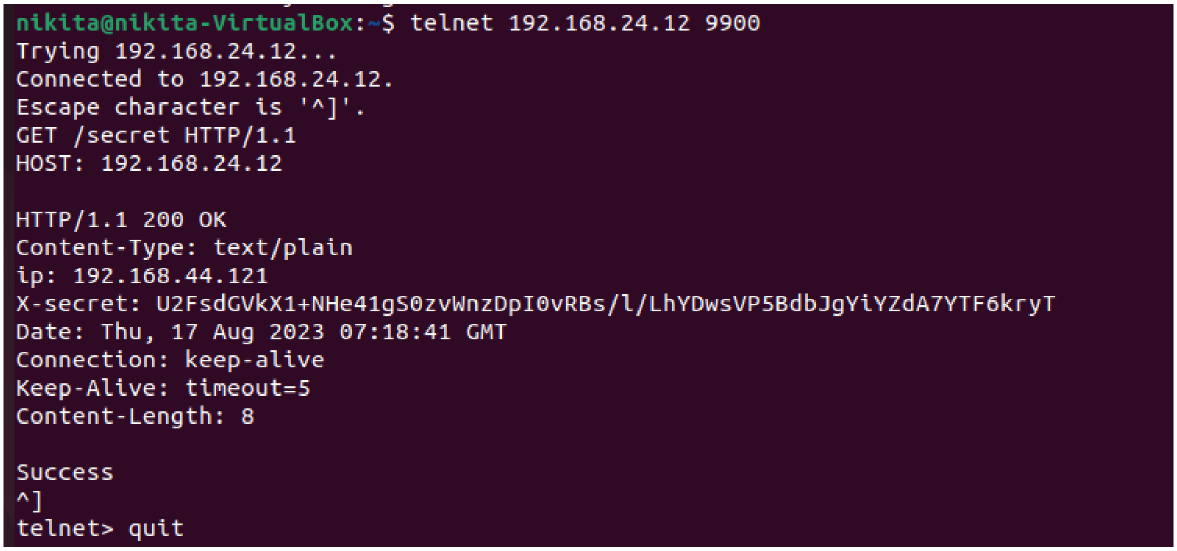
This is because google provides service to millions of users and depends on its performance to keep the users and make profit. This is why fast speed (low latency) is a must for google while stanford caters to a relatively small audience and it speed doesn’t matter as much. Hence, there is a huge difference in their average latencies.

4)
127.0.0.1 is the loopback address of my localhost. To make the ping fail for this with 100% data loss, I can shut my loop back interface down using the command sudo ifconfig lo down.



```
nikita@nikita-VirtualBox:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.024 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.038 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.032 ms
^C
--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2028ms
rtt min/avg/max/mdev = 0.024/0.031/0.038/0.005 ms
nikita@nikita-VirtualBox:~$ sudo ifconfig lo down
nikita@nikita-VirtualBox:~$ 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 ---
3 packets transmitted, 0 received, 100% packet loss, time 2030ms
```

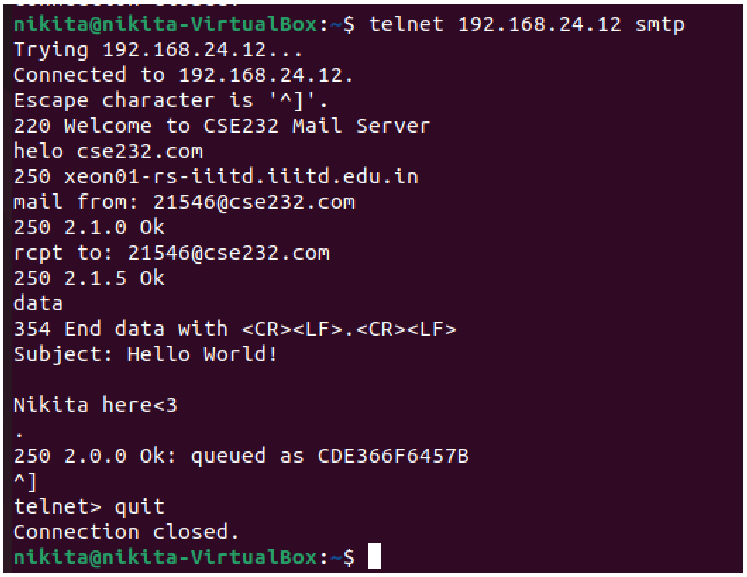
5)



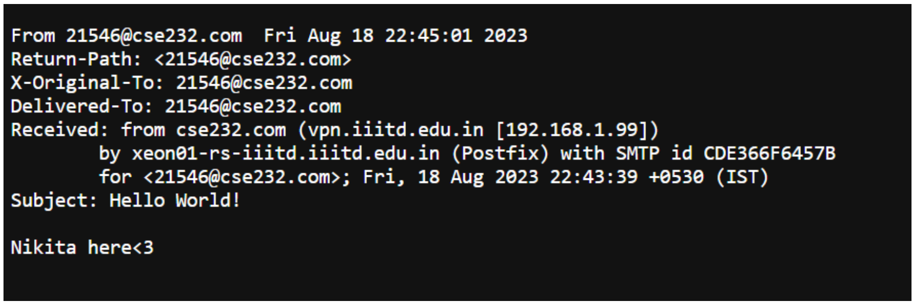
```
nikita@nikita-VirtualBox:~$ telnet 192.168.24.12 9900
Trying 192.168.24.12...
Connected to 192.168.24.12.
Escape character is '^]'.
GET /secret HTTP/1.1
HOST: 192.168.24.12

HTTP/1.1 200 OK
Content-Type: text/plain
ip: 192.168.44.121
X-secret: U2FsdGVkX1+NHe41gS0zvWnzDpI0vRBs/l/LhYDwsVP5BdbJgYiYZdA7YTF6kryT
Date: Thu, 17 Aug 2023 07:18:41 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Content-Length: 8

Success
^]
telnet> quit
```

X-Secret = U2FsdGVkX1+NHe41gS0zvWnzDpI0vRBs/l/LhYDwsVP5BdbJgYiYZdA7YTF6kryT

Q6)

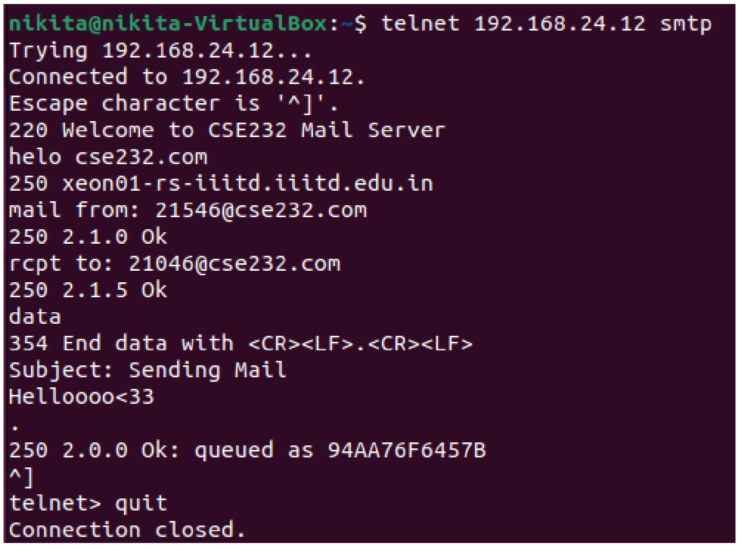


```
nikita@nikita-VirtualBox:~$ telnet 192.168.24.12 smtp
Trying 192.168.24.12...
Connected to 192.168.24.12.
Escape character is '^]'.
220 Welcome to CSE232 Mail Server
helo cse232.com
250 xeon01-rs-iiitd.iiitd.edu.in
mail from: 21546@cse232.com
250 2.1.0 Ok
rcpt to: 21546@cse232.com
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: Hello World!

Nikita here<3

.
250 2.0.0 Ok: queued as CDE366F6457B
^]
telnet> quit
Connection closed.
nikita@nikita-VirtualBox:~$
```

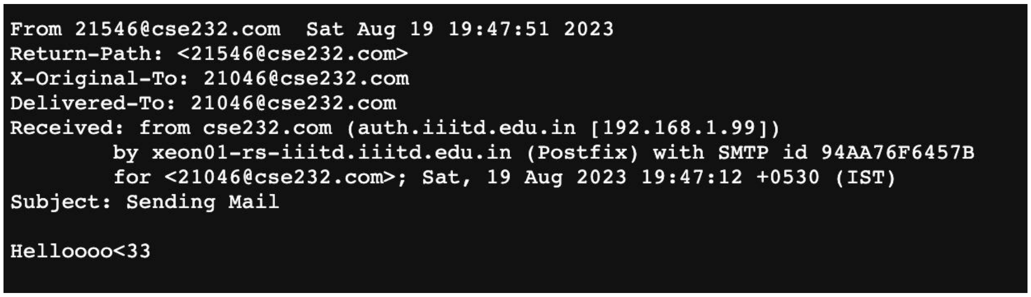


```
From 21546@cse232.com  Fri Aug 18 22:45:01 2023
Return-Path: <21546@cse232.com>
X-Original-To: 21546@cse232.com
Delivered-To: 21546@cse232.com
Received: from cse232.com (vpn.iiitd.edu.in [192.168.1.99])
        by xeon01-rs-iiitd.iiitd.edu.in (Postfix) with SMTP id CDE366F6457B
        for <21546@cse232.com>; Fri, 18 Aug 2023 22:43:39 +0530 (IST)
Subject: Hello World!

Nikita here<3
```

Mail sent to a student and screenshot from them:



```
nikita@nikita-VirtualBox:~$ telnet 192.168.24.12 smtp
Trying 192.168.24.12...
Connected to 192.168.24.12.
Escape character is '^]'.
220 Welcome to CSE232 Mail Server
helo cse232.com
250 xeon01-rs-iiitd.iiitd.edu.in
mail from: 21546@cse232.com
250 2.1.0 Ok
rcpt to: 21046@cse232.com
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: Sending Mail
Helloooo<33
.
250 2.0.0 Ok: queued as 94AA76F6457B
^]
telnet> quit
Connection closed.
```



```
From 21546@cse232.com  Sat Aug 19 19:47:51 2023
Return-Path: <21546@cse232.com>
X-Original-To: 21046@cse232.com
Delivered-To: 21046@cse232.com
Received: from cse232.com (auth.iiitd.edu.in [192.168.1.99])
        by xeon01-rs-iiitd.iiitd.edu.in (Postfix) with SMTP id 94AA76F6457B
        for <21046@cse232.com>; Sat, 19 Aug 2023 19:47:12 +0530 (IST)
Subject: Sending Mail

Helloooo<33
```