CSE 232: Assignment 1

Annu Kumari | 2021312

Q1. [1 + 1]

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

```
Processing triggers for man-db (2.9.1-1) ...
annukum@Annu:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.215.228  netmask 255.255.240.0  broadcast 192.168.223.255
        inet6 fe80::215:5dff:fe17:a6de  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:17:a6:de  txqueuelen 1000  (Ethernet)
        RX packets 242  bytes 220445 (220.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 102  bytes 7056 (7.0 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 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

annukum@Annu:~$
```

IP Address of my network interface is 192.168.215.228

(inet is the ip address)

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?

103.170.158.88

My machine's IP address differs from the IP address shown at https://www.whatismyip.com. This is because there are two types of IP addresses:

Public IP address: This is the address visible to the outside world. Our Internet service provider (ISP) assigns it to our router. (shown at https://www.whatismyip.com)

Private IP address: This is the address used for communication between devices on our local network. Our router assigns it. (shown by the ipconfig command)

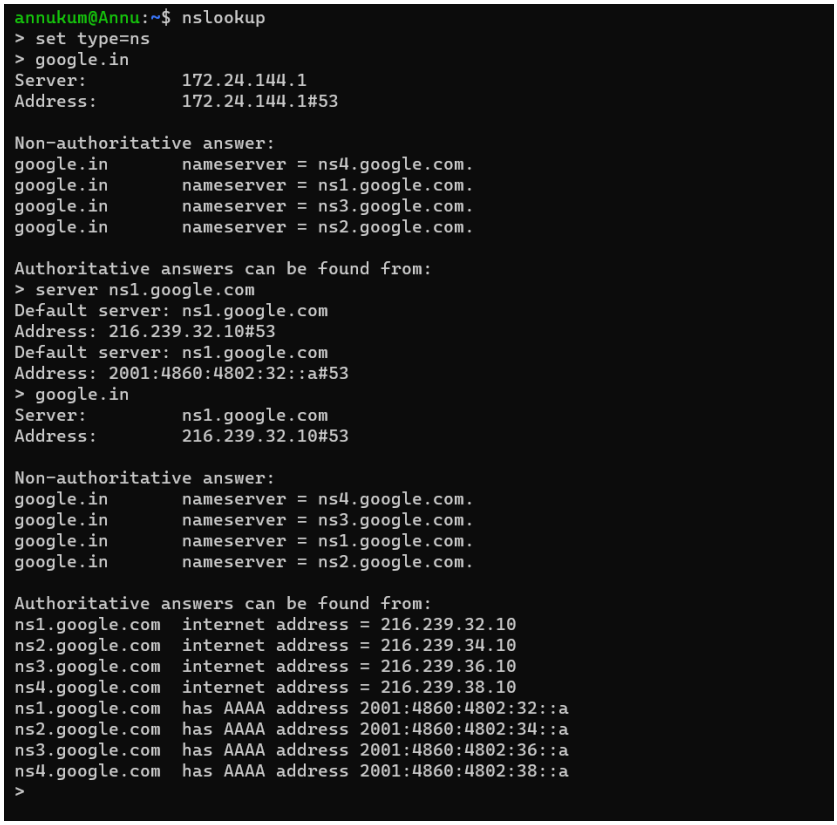
Q2. nslookup ([2+1] + [1+1])

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

To obtain an authoritative result for "google.in" using nslookup, I followed these steps:

1. Opened the terminal.
2. Typed "nslookup" and press Enter. This opened the nslookup tool.
3. Typed "set type=ns" and press Enter. This sets the query type to NS (Name Server).
4. Typed "google.in" and press Enter. This displayed the authoritative name servers for the "google.in" domain.

This returned the following:



The authoritative result for "google.in" is 172.24.144.1.

Explanation:

Nslookup is a command-line tool used to query DNS (Domain Name System) servers to obtain information about a specific domain or IP address. Setting the query type to “NS” instructs nslookup to return the authoritative name servers for the domain "google.in." These authoritative name servers are responsible for providing the correct DNS information for the domain.

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

The TTL value for the domain "howtouselinux.com" is 3600 seconds. This means that the DNS record for "www.howtouselinux.com" will expire and be removed from the cache of my local DNS server after 3600 seconds or 1 hour.

This means that after 3600 seconds, the local DNS server will need to contact an authoritative DNS server to get the latest information about "howtouselinux.com".

Below is the result in the Windows terminal-

```
PS C:\Users\annuk> nslookup -debug google.com
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 1, rcode = NXDOMAIN
        header flags:  response, auth. answer, want recursion, recursion avail.
        questions = 1,  answers = 0,  authority records = 1,  additional = 0

    QUESTIONS:
        9.1.1.1.in-addr.arpa, type = PTR, class = IN
    AUTHORITY RECORDS:
    ->  1.1.1.in-addr.arpa
        ttl = 3600 (1 hour)
        primary name server = win-egd96904trc
        responsible mail addr = hostmaster
        serial  = 318
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 86400 (1 day)
        default TTL = 3600 (1 hour)

------------
Server:  UnKnown
Address:  1.1.1.9

------------
Got answer:
    HEADER:
        opcode = QUERY, id = 2, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 1,  authority records = 0,  additional = 0

    QUESTIONS:
        google.com, type = A, class = IN
    ANSWERS:
    ->  google.com
        internet address = 142.250.206.174
        ttl = 113 (1 min 53 secs)

------------
Non-authoritative answer:
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 3, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 1,  authority records = 0,  additional = 0

    QUESTIONS:
        google.com, type = AAAA, class = IN
    ANSWERS:
    ->  google.com
        AAAA IPv6 address = 2404:6800:4002:82d::200e
        ttl = 41 (41 secs)

------------
Name:    google.com
Addresses:  2404:6800:4002:82d::200e
          142.250.206.174

PS C:\Users\annuk>
```

Q3. [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]

Note that some of the intermediate hosts might not be visible; their IP addresses

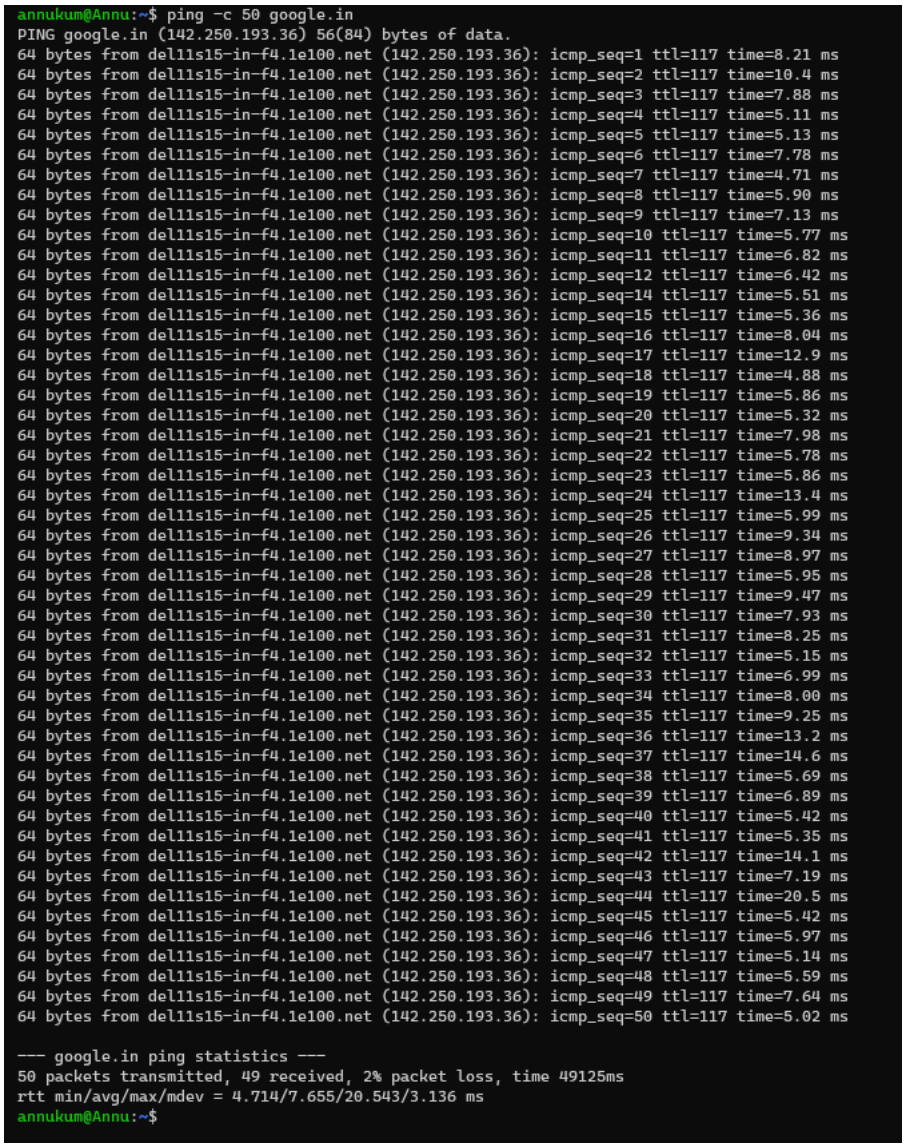
will come as "", ignore those hosts for this assignment.***

```
annukum@Annu:~$ traceroute google.in
traceroute to google.in (172.217.166.36), 30 hops max, 60 byte packets
 1  Annu.mshome.net (192.168.208.1)  0.704 ms  0.682 ms  0.677 ms
 2  192.168.0.1 (192.168.0.1)  13.958 ms  11.271 ms  12.517 ms
 3  10.10.98.1 (10.10.98.1)  4.544 ms  6.236 ms  15.705 ms
 4  103.190.8.1 (103.190.8.1)  40.865 ms  18.791 ms  17.223 ms
 5  192.168.229.37 (192.168.229.37)  7.823 ms  40.886 ms  11.211 ms
 6  72.14.219.216 (72.14.219.216)  20.318 ms  18.906 ms  20.576 ms
 7  * * *
 8  172.253.67.96 (172.253.67.96)  33.283 ms 172.253.67.100 (172.253.67.100)  29.886 ms 142.251.54.96 (142.251.54.96)  29.871 ms
 9  74.125.244.205 (74.125.244.205)  28.328 ms 108.170.251.102 (108.170.251.102)  17.714 ms 74.125.244.205 (74.125.244.205)  9.451 ms
10  172.253.69.58 (172.253.69.58)  25.278 ms 142.250.234.126 (142.250.234.126)  43.048 ms 209.85.250.56 (209.85.250.56)  11.846 ms
11  216.239.54.93 (216.239.54.93)  36.658 ms 216.239.50.23 (216.239.50.23)  28.476 ms 108.170.248.209 (108.170.248.209)  43.152 ms
12  108.170.248.193 (108.170.248.193)  31.368 ms 108.170.235.51 (108.170.235.51)  35.186 ms 108.170.248.193 (108.170.248.193)  30.137 ms
13  108.170.235.51 (108.170.235.51)  42.992 ms 108.170.234.209 (108.170.234.209)  46.361 ms  33.252 ms
14  bom07s18-in-f4.1e100.net (172.217.166.36)  44.146 ms  26.543 ms  130.414 ms
annukum@Annu:~$ ping -c 50 google.in
```

14 intermediate hosts.

Hop	IP Address	Average Latency(ms)
1	192.168.208.1	0.688
2	192.168.0.1	12.582
3	10.10.98.1	8.828
4	103.190.8.1	25.626
5	192.168.229.37	19.973
6	72.14.219.216	19.933
7	-	-
8	172.253.67.96	31.013
9	74.125.244.205	18.498
10	172.253.69.58	26.724
11	216.239.54.93	34.429
12	108.170.248.193	32.230
13	108.170.235.51	40.868
14	172.217.166.36(bom07s18-in-f4.1e100.net)	67.034

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



The average latency is 7.655 milliseconds.

c) Add up the ping latency of all the intermediate hosts obtained in (a) and compare with (b). Are they matching, explain?[1+1]

Sum of latencies = 338.426ms

Average latency from `ping` command = 7.655ms

The difference in latency measurements between the traceroute and ping commands can be attributed to two main factors:

Measurement Scope:

- Traceroute measures latency for each hop along the route, including processing time at intermediate hosts.
- Ping measures round-trip latency between source and destination without considering intermediate hosts' processing time.

Network Configuration:

- Traceroute may encounter redundant paths or load balancing, causing variations in latencies across hops.
- Ping measures a direct round-trip, while traceroute might take different routes with different latencies.

d) Take the maximum of ping latency amongst the intermediate hosts (in (a)) and compare with (b). Are they matching, explain? [1+1]

Maximum latency from the traceroute(a) = 67.034ms

Maximum latency from the ping command(b) = 20.543ms

The disparity between maximum latencies from traceroute (a) and ping (b) arises due to their distinct measurement approaches:

- Traceroute gauges latency at each hop, summing incremental TTL values and ICMP responses.
- Ping calculates round-trip latency between source and destination, offering a more accurate overall measurement.

e) You may see multiple entries for a single hop while using traceroute command. What do these entries mean? [1]

Multiple entries for a single hop in the traceroute command show different routers or devices in the network path. Each entry represents a device forwarding the packet, indicating various routes the packet could take. It highlights redundancy and path options, aiding in each hop's path analysis and latency assessment.

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

```
annukum@Annu:~$ ping stanford.edu -c 50
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=235 time=306 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=2 ttl=235 time=267 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=3 ttl=235 time=275 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=4 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=5 ttl=235 time=266 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=6 ttl=235 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=7 ttl=235 time=266 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=8 ttl=235 time=264 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=9 ttl=235 time=269 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=10 ttl=235 time=270 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=11 ttl=235 time=270 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=12 ttl=235 time=307 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=13 ttl=235 time=270 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=14 ttl=235 time=268 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=15 ttl=235 time=267 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=16 ttl=235 time=264 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=17 ttl=235 time=274 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=18 ttl=235 time=323 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=19 ttl=235 time=264 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=20 ttl=235 time=272 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=21 ttl=235 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=22 ttl=235 time=266 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=23 ttl=235 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=24 ttl=235 time=267 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=25 ttl=235 time=307 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=26 ttl=235 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=27 ttl=235 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=28 ttl=235 time=273 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=29 ttl=235 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=30 ttl=235 time=266 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=31 ttl=235 time=266 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=32 ttl=235 time=270 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=33 ttl=235 time=266 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=34 ttl=235 time=267 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=35 ttl=235 time=294 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=36 ttl=235 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=37 ttl=235 time=266 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=38 ttl=235 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=39 ttl=235 time=266 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=40 ttl=235 time=267 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=41 ttl=235 time=266 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=42 ttl=235 time=267 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=43 ttl=235 time=266 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=44 ttl=235 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=45 ttl=235 time=268 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=46 ttl=235 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=47 ttl=235 time=266 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=48 ttl=235 time=266 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=49 ttl=235 time=266 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=50 ttl=235 time=286 ms

--- stanford.edu ping statistics ---
50 packets transmitted, 50 received, 0% packet loss, time 49062ms
rtt min/avg/max/mdev = 263.919/271.544/323.436/12.887 ms
annukum@Annu:~$
```

Average latency= 271.544

g) Run the command, traceroute stanford.edu. Compare the number of hops between google.in and stanford.edu (between the traceroute result of google.in and stanford.edu). [1]

```
annukum@Annu:~$ traceroute stanford.edu
traceroute to stanford.edu (171.67.215.200), 30 hops max, 60 byte packets
 1  Annu.mshome.net (192.168.208.1)  0.365 ms  0.838 ms  0.824 ms
 2  192.168.0.1 (192.168.0.1)  14.722 ms  16.091 ms  17.175 ms
 3  10.10.98.1 (10.10.98.1)  20.683 ms  18.849 ms  22.320 ms
 4  103.190.8.1 (103.190.8.1)  25.299 ms  27.768 ms  26.679 ms
 5  * * *
 6  static-153.168.194.14-tataidc.co.in (14.194.168.153)  30.324 ms  22.606 ms  28.093 ms
 7  14.141.116.253.static-Delhi.vsnl.net.in (14.141.116.253)  16.861 ms  7.703 ms  8.154 ms
 8  172.31.244.45 (172.31.244.45)  94.558 ms  89.585 ms  92.485 ms
 9  ix-ae-4-2.tcore2.cxr-chennai.as6453.net (180.87.37.1)  86.796 ms  88.131 ms  94.505 ms
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  dc-stanford--svl-agg4-100ge.cenic.net (137.164.23.145)  289.115 ms  410.251 ms  410.305 ms
16  woa-west-rtr-vl3.SUNet (171.66.255.132)  309.450 ms  270.264 ms  338.662 ms
17  * * *
18  web.stanford.edu (171.67.215.200)  269.281 ms  269.275 ms  260.338 ms
annukum@Annu:~$ traceroute google.in
traceroute to google.in (142.250.193.36), 30 hops max, 60 byte packets
 1  Annu.mshome.net (192.168.208.1)  0.430 ms  0.356 ms  0.747 ms
 2  192.168.0.1 (192.168.0.1)  6.139 ms  3.398 ms  4.692 ms
 3  10.10.98.1 (10.10.98.1)  9.666 ms  11.609 ms  8.751 ms
 4  103.190.8.1 (103.190.8.1)  15.596 ms  18.720 ms  14.172 ms
 5  192.168.229.37 (192.168.229.37)  19.695 ms  21.084 ms  18.574 ms
 6  72.14.219.216 (72.14.219.216)  13.234 ms  20.035 ms  18.123 ms
 7  * * *
 8  142.251.54.88 (142.251.54.88)  7.469 ms 142.251.52.198 (142.251.52.198)  20.586 ms 142.251.54.88 (142.251.54.88)  23.982 ms
 9  108.170.251.123 (108.170.251.123)  22.058 ms 108.170.251.108 (108.170.251.108)  27.023 ms 142.251.54.91 (142.251.54.91)  13.850 ms
10  del11s15-in-f4.1e100.net (142.250.193.36)  20.188 ms 74.125.243.97 (74.125.243.97)  25.746 ms del11s15-in-f4.1e100.net (142.250.193.36)  12.177 ms
annukum@Annu:~$
```

The traceroute results for `google.in` and `stanford.edu` indicate different numbers of hops between the source and destination:

1. google.in: The traceroute shows 10 hops.
2. stanford.edu: The traceroute shows 18 hops.

So, the number of hops between google.in and stanford.edu is 8. This difference in the number of hops suggests that there are more intermediary routers and network devices between the source and stanford.edu compared to google.in. The reasons for this variation include differing network configurations, routing paths, traffic loads, and ISP routing policies for each destination.

h) Can you explain the reason for the latency difference between google.in and stanford.edu (see (b) & (f))? [1]

The latency to google.in is 7.655 ms, while the latency to stanford.edu is 271.544 ms. This means that it takes about 32 times longer for a packet to travel from my computer to stanford.edu than it takes to travel from my computer to google.in.

The reason for the difference in latency is the distance between my computer and the two destinations. Stanford University is located in California, while Google's servers are located all over the world. The distance between my computer and Stanford University is much greater than the distance between my computer and Google's servers.

The other factor that can affect latency is the congestion on the network. If the network is congested, the packets may have to wait in line to be transmitted. This can increase the RTT and the latency.

Q4. [2+1] Make your ping command fail for 127.0.0.1 (with 100% packet loss). Explain how you do it. Put a screenshot that it failed.

```
annukum@Annu:~$ ping -I eth0 127.0.0.1 -c 10
PING 127.0.0.1 (127.0.0.1) from 192.168.220.215 eth0: 56(84) bytes of data.

--- 127.0.0.1 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9380ms
```

Through the "ping -I eth0 127.0.0.1 -c 10" command, I am attempting to send ICMP echo request packets to the loopback address 127.0.0.1 using the network interface eth0. However, since the loopback address is a local interface that never leaves the system, the packets are instantly looped back. Creating a firewall rule to block ICMP for the loopback address wouldn't affect this behaviour. The 100% packet loss results from the inherent nature of loopback communication.

Other ways:

```
annukum@Annu:~$ sudo iptables -A INPUT -i lo -p icmp -j DROP
annukum@Annu:~$ 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 ---
63 packets transmitted, 0 received, 100% packet loss, time 64470ms

annukum@Annu:~$
```

```
annukum@Annu:~$ ping -f -i 1 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
.....
.....
.....^C
--- 127.0.0.1 ping statistics ---
350 packets transmitted, 0 received, 100% packet loss, time 362998ms

annukum@Annu:~$
```

Q.5 [0.5*4 + 1] Use telnet to perform an HTTP get request on a webpage hosted at 192.168.24.12

telnet 192.168.24.12 9900
GET /secret HTTP/1.1
Host: 192.168.24.12
Connection: close
(two times press enter)

```
annukum@Annu:~$ 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
Connection: close

HTTP/1.1 200 OK
Content-Type: text/plain
ip: 192.168.43.151
X-secret: U2FsdGVkX1+7S5C6HExqhUprJqeX0URiU59Dj0++AvfR3jjiPh4roDEFXBSHwe3K
Date: Wed, 23 Aug 2023 05:58:35 GMT
Connection: close
Content-Length: 8

Success
Connection closed by foreign host.
annukum@Annu:~$
```

X-secret: U2FsdGVkX1+7S5C6HExqhUprJqeX0URiU59Dj0++AvfR3jjiPh4roDEFXBSHwe3K

Q6. [0.5*4 + 2 + 0.5*2] Use telnet to send an email to one of the other students using an SMTP server.

telnet 192.168.24.12 smpt
helo cse232.com
mail from: 21312@cse232.com
rcpt to: 21337@cse232.com
data
subject: Connection Check
Hi! Mail send check.
.
quit

Mail Send:

```
annukum@Annu:~$ 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: 21312@cse232.com
250 2.1.0 Ok
rcpt to: 21337@cse232.com
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
subject: Connection Check
Hi! Mail send check.
.
250 2.0.0 Ok: queued as A143B6F643A5
quit
221 2.0.0 Bye
Connection closed by foreign host.
annukum@Annu:~$
```

Mail Received:

```
From 21312@cse232.com  Wed Aug 23 17:22:48 2023
Return-Path: <21312@cse232.com>
X-Original-To: 21337@cse232.com
Delivered-To: 21337@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 A143B6F643A5
        for <21337@cse232.com>; Wed, 23 Aug 2023 17:21:33 +0530 (IST)
subject: Connection Check

Hi! Mail send check.
```

SMTP ID: A143B6F643A5