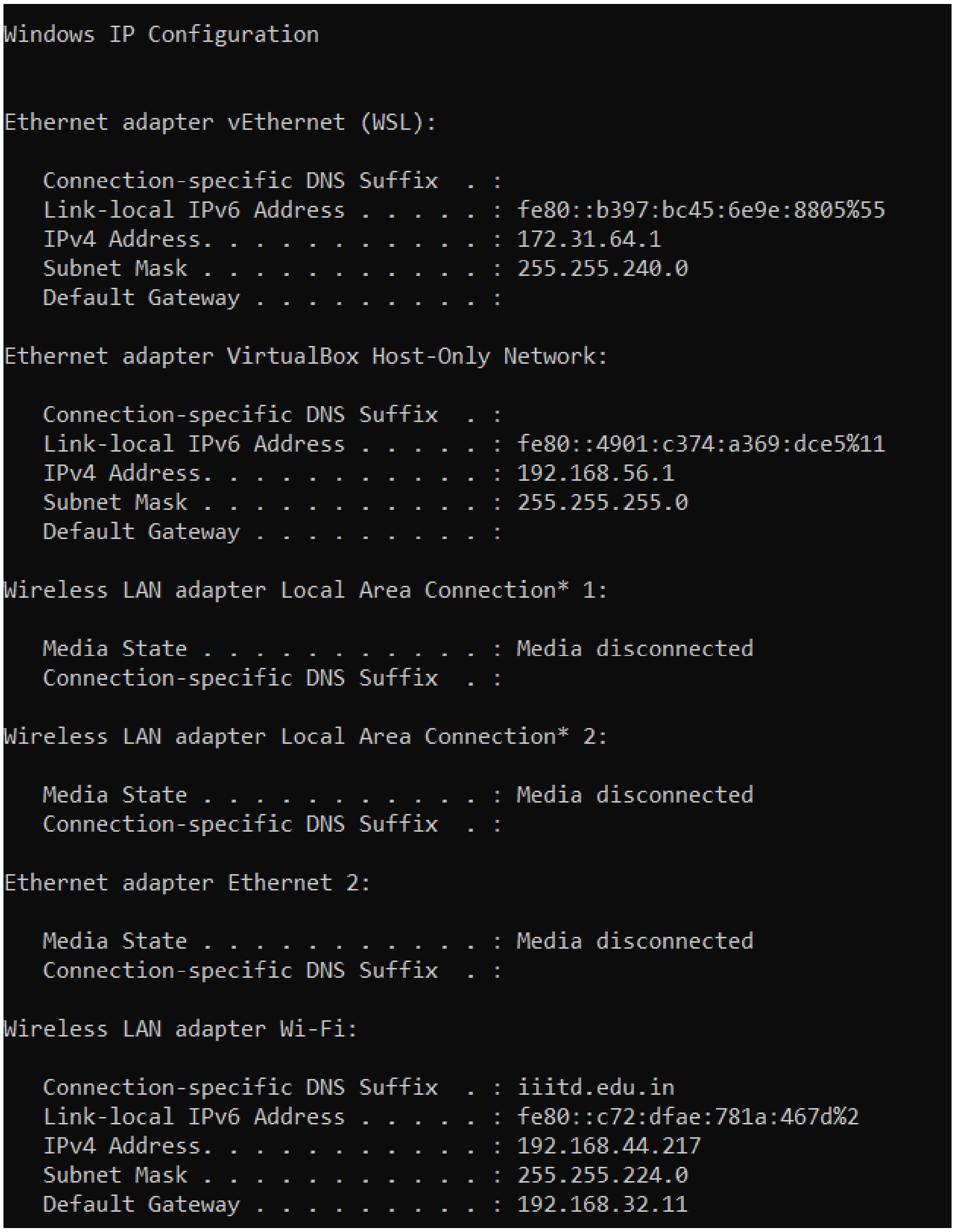
2021093-Assignment1

Assumption: Some of the screenshots are from my windows machine while some are from my Kali VM (I had Kali already set up).

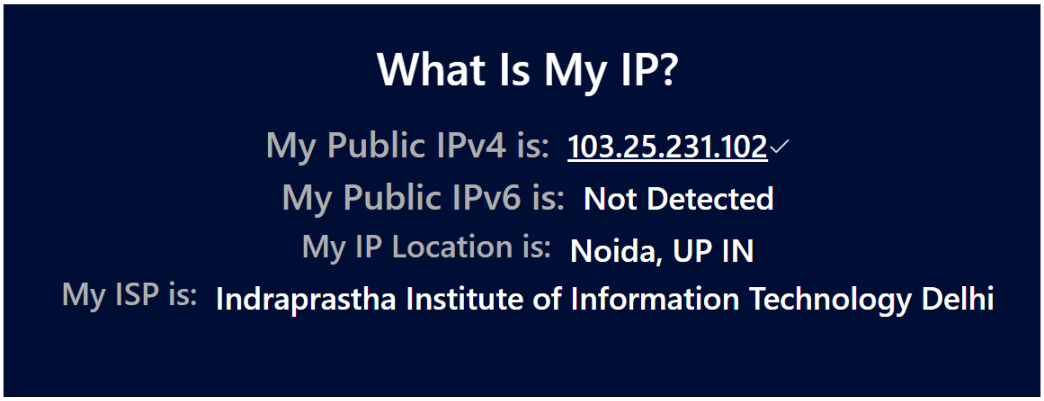
Question 1

1. Output for *Ipconfig:*
   IP Address for my local WiFi adapter: 192.168.44.217.



```
Windows IP Configuration


Ethernet adapter vEthernet (WSL):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b397:bc45:6e9e:8805%55
   IPv4 Address. . . . . . . . . . . : 172.31.64.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4901:c374:a369:dce5%11
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : iiitd.edu.in
   Link-local IPv6 Address . . . . . : fe80::c72:dfae:781a:467d%2
   IPv4 Address. . . . . . . . . . . : 192.168.44.217
   Subnet Mask . . . . . . . . . . . : 255.255.224.0
   Default Gateway . . . . . . . . . : 192.168.32.11
```

2. Output for IP at www.whatismyip.com:
   IPV4 address: 103.25.231.102



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

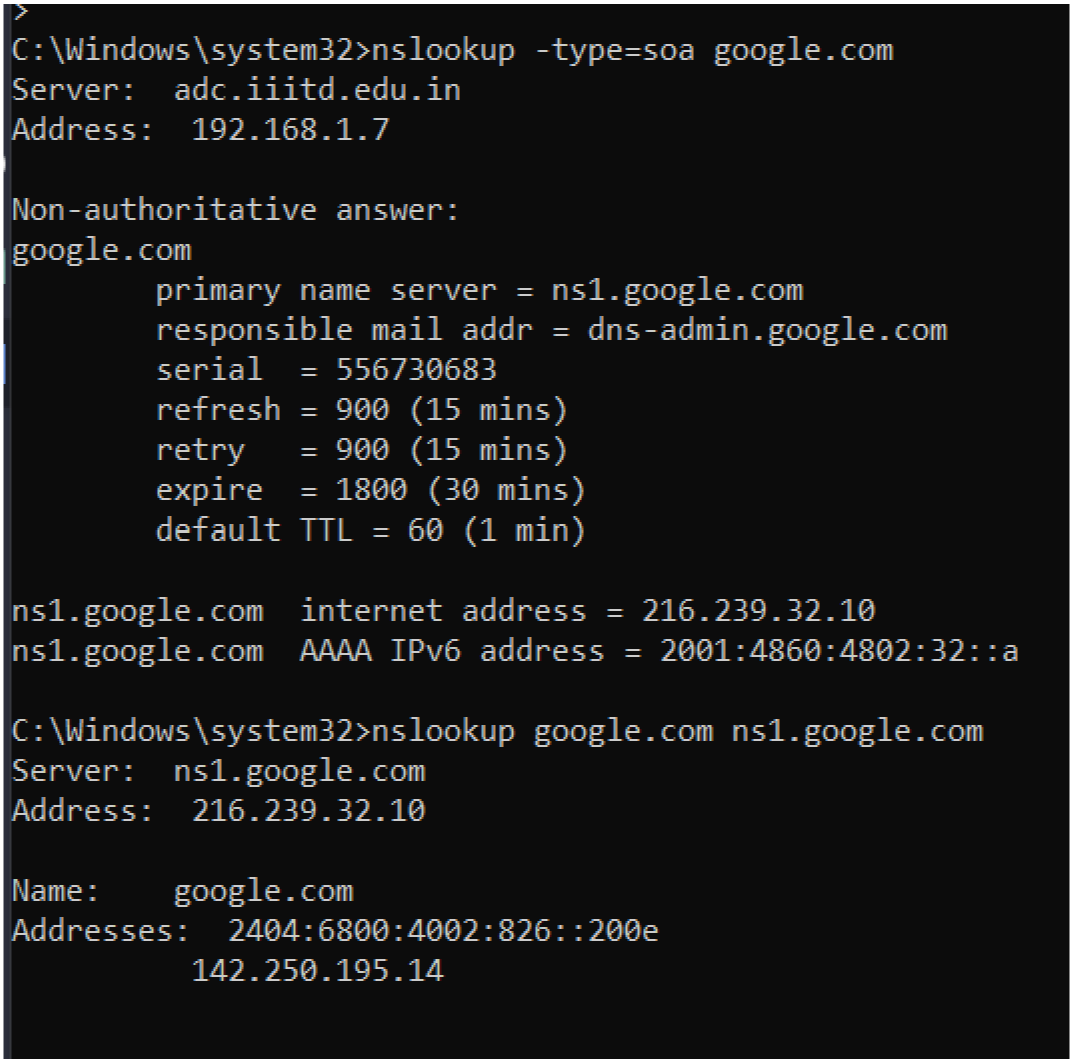
My ISP is: Indraprastha Institute of Information Technology Delhi

The two above present IP addresses are different, as in the former case it is displaying my private device IP while in the latter it is showing the public device IP.

Question 2

1. Authoritative result for ‘google.in’.
   Explaination: Upon normal nslookup, it was found that a non-authoritative answer was obtained. In order to get the authoritative, we had to look at SOA (Start of Authority), which contains the information for a zone.
   Therefore documentation of nslookup had the type flag with soa as an attribute.

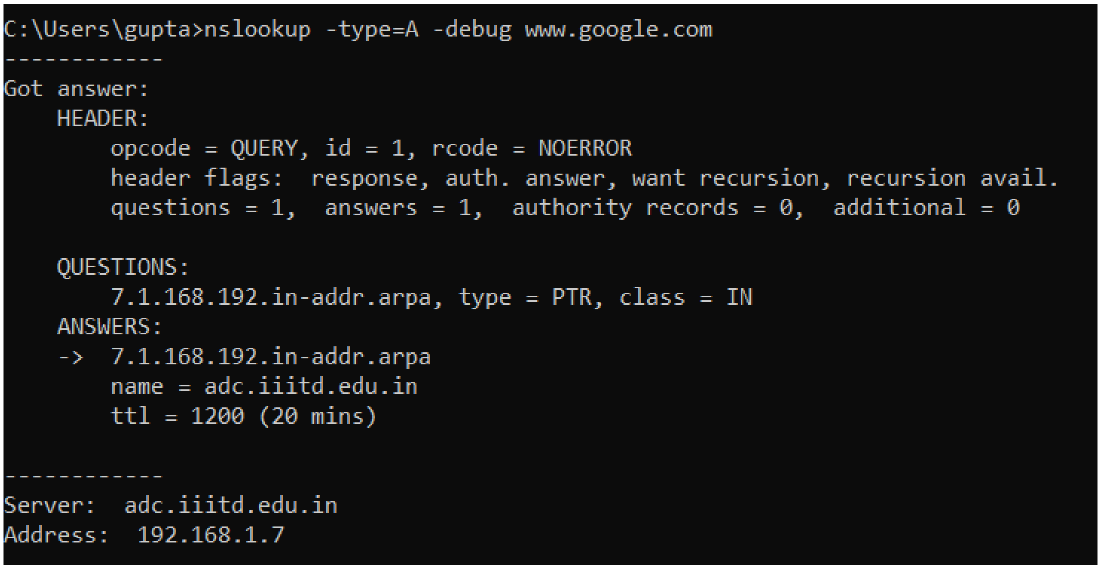
   Authoritative IPV4: 142.250.195.14
   Authoritative IPV6: 2404:6800:4002:826::200e



```
>
C:\Windows\system32>nslookup -type=soa google.com
Server:  adc.iiitd.edu.in
Address:  192.168.1.7

Non-authoritative answer:
google.com
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 556730683
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)

ns1.google.com  internet address = 216.239.32.10
ns1.google.com  AAAA IPv6 address = 2001:4860:4802:32::a

C:\Windows\system32>nslookup google.com ns1.google.com
Server:  ns1.google.com
Address:  216.239.32.10

Name:    google.com
Addresses:  2404:6800:4002:826::200e
          142.250.195.14
```

2. TTL (Time to live): It is the time that a website should exist on a local DNS before being looked up again.

   In the below mentioned TTL is 20 mins, which means that after **20 mins**, another lookup will be performed for google.com, and if this command was run repeatedly, it’s possible to see the time decrease. The *-debug* flag shows elaborate information about the domain.



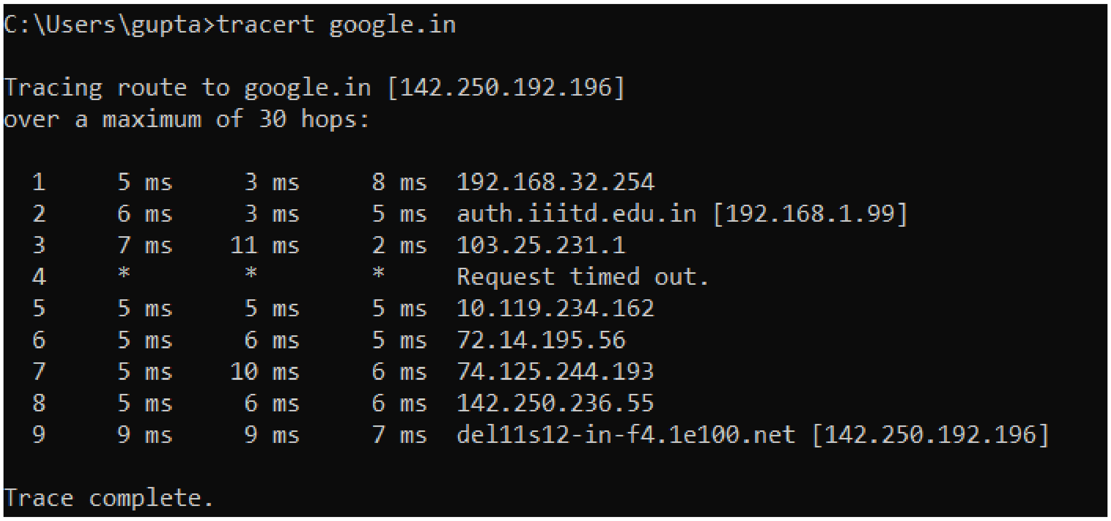
```
C:\Users\gupta>nslookup -type=A -debug www.google.com
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 1, rcode = NOERROR
        header flags:  response, auth. answer, want recursion, recursion avail.
        questions = 1,  answers = 1,  authority records = 0,  additional = 0

    QUESTIONS:
        7.1.168.192.in-addr.arpa, type = PTR, class = IN
    ANSWERS:
    ->  7.1.168.192.in-addr.arpa
        name = adc.iiitd.edu.in
        ttl = 1200 (20 mins)

------------
Server:  adc.iiitd.edu.in
Address:  192.168.1.7
```

Question 3

1. There are 6 intermediate hosts. (*Ignoring the initial, final and * hosts)*
   Their corresponding IP addresses are present in the right column.

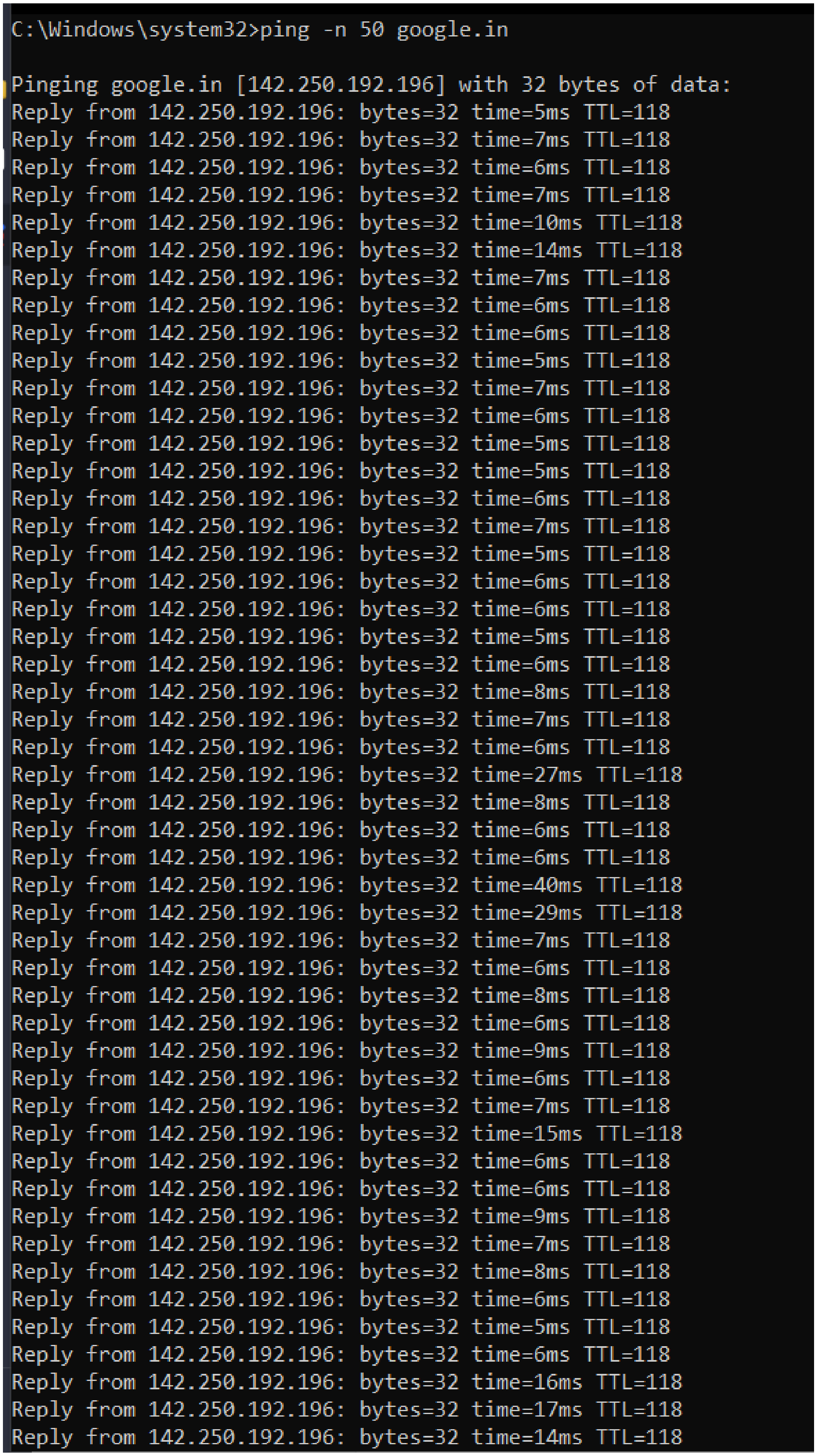
   Network Latency is how long it takes for something sent from a source host to reach a destination.
   RTT (round trip time) is how long it takes for a request sent from a source to a destination, and for it to come back (*includes processing).*

   So, assuming no processing, we will take Latency to be half of RTT.
   Therefore,
   1 → (5+ 3 + 8)/6 = **5.3333333333333/2**
   2 → 4.6666666666667/2
   3 → 6.6666666666667/2
   4 → timeout
   5 → 5/2
   6 → 5.3333333333333/2
   7 → 7/2
   8 → 5.6666666666667/2
   9 → 8.3333333333333/2

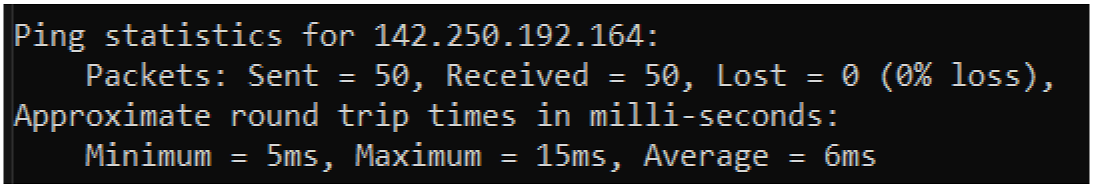


```
C:\Users\gupta>tracert google.in

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

  1     5 ms     3 ms     8 ms  192.168.32.254
  2     6 ms     3 ms     5 ms  auth.iiitd.edu.in [192.168.1.99]
  3     7 ms    11 ms     2 ms  103.25.231.1
  4     *        *        *     Request timed out.
  5     5 ms     5 ms     5 ms  10.119.234.162
  6     5 ms     6 ms     5 ms  72.14.195.56
  7     5 ms    10 ms     6 ms  74.125.244.193
  8     5 ms     6 ms     6 ms  142.250.236.55
  9     9 ms     9 ms     7 ms  del11s12-in-f4.1e100.net [142.250.192.196]

Trace complete.
```

2. 50 pings to google.in:
   Average Latency (RTT): 6ms



```
C:\Windows\system32>ping -n 50 google.in

Pinging google.in [142.250.192.196] with 32 bytes of data:
Reply from 142.250.192.196: bytes=32 time=5ms TTL=118
Reply from 142.250.192.196: bytes=32 time=7ms TTL=118
Reply from 142.250.192.196: bytes=32 time=6ms TTL=118
Reply from 142.250.192.196: bytes=32 time=7ms TTL=118
Reply from 142.250.192.196: bytes=32 time=10ms TTL=118
Reply from 142.250.192.196: bytes=32 time=14ms TTL=118
Reply from 142.250.192.196: bytes=32 time=7ms TTL=118
Reply from 142.250.192.196: bytes=32 time=6ms TTL=118
Reply from 142.250.192.196: bytes=32 time=6ms TTL=118
Reply from 142.250.192.196: bytes=32 time=5ms TTL=118
Reply from 142.250.192.196: bytes=32 time=7ms TTL=118
Reply from 142.250.192.196: bytes=32 time=6ms TTL=118
Reply from 142.250.192.196: bytes=32 time=5ms TTL=118
Reply from 142.250.192.196: bytes=32 time=5ms TTL=118
Reply from 142.250.192.196: bytes=32 time=6ms TTL=118
Reply from 142.250.192.196: bytes=32 time=7ms TTL=118
Reply from 142.250.192.196: bytes=32 time=5ms TTL=118
Reply from 142.250.192.196: bytes=32 time=6ms TTL=118
Reply from 142.250.192.196: bytes=32 time=6ms TTL=118
Reply from 142.250.192.196: bytes=32 time=5ms TTL=118
Reply from 142.250.192.196: bytes=32 time=6ms TTL=118
Reply from 142.250.192.196: bytes=32 time=8ms TTL=118
Reply from 142.250.192.196: bytes=32 time=7ms TTL=118
Reply from 142.250.192.196: bytes=32 time=6ms TTL=118
Reply from 142.250.192.196: bytes=32 time=27ms TTL=118
Reply from 142.250.192.196: bytes=32 time=8ms TTL=118
Reply from 142.250.192.196: bytes=32 time=6ms TTL=118
Reply from 142.250.192.196: bytes=32 time=6ms TTL=118
Reply from 142.250.192.196: bytes=32 time=40ms TTL=118
Reply from 142.250.192.196: bytes=32 time=29ms TTL=118
Reply from 142.250.192.196: bytes=32 time=7ms TTL=118
Reply from 142.250.192.196: bytes=32 time=6ms TTL=118
Reply from 142.250.192.196: bytes=32 time=8ms TTL=118
Reply from 142.250.192.196: bytes=32 time=6ms TTL=118
Reply from 142.250.192.196: bytes=32 time=9ms TTL=118
Reply from 142.250.192.196: bytes=32 time=6ms TTL=118
Reply from 142.250.192.196: bytes=32 time=7ms TTL=118
Reply from 142.250.192.196: bytes=32 time=15ms TTL=118
Reply from 142.250.192.196: bytes=32 time=6ms TTL=118
Reply from 142.250.192.196: bytes=32 time=6ms TTL=118
Reply from 142.250.192.196: bytes=32 time=9ms TTL=118
Reply from 142.250.192.196: bytes=32 time=7ms TTL=118
Reply from 142.250.192.196: bytes=32 time=8ms TTL=118
Reply from 142.250.192.196: bytes=32 time=6ms TTL=118
Reply from 142.250.192.196: bytes=32 time=5ms TTL=118
Reply from 142.250.192.196: bytes=32 time=6ms TTL=118
Reply from 142.250.192.196: bytes=32 time=16ms TTL=118
Reply from 142.250.192.196: bytes=32 time=17ms TTL=118
Reply from 142.250.192.196: bytes=32 time=14ms TTL=118
```

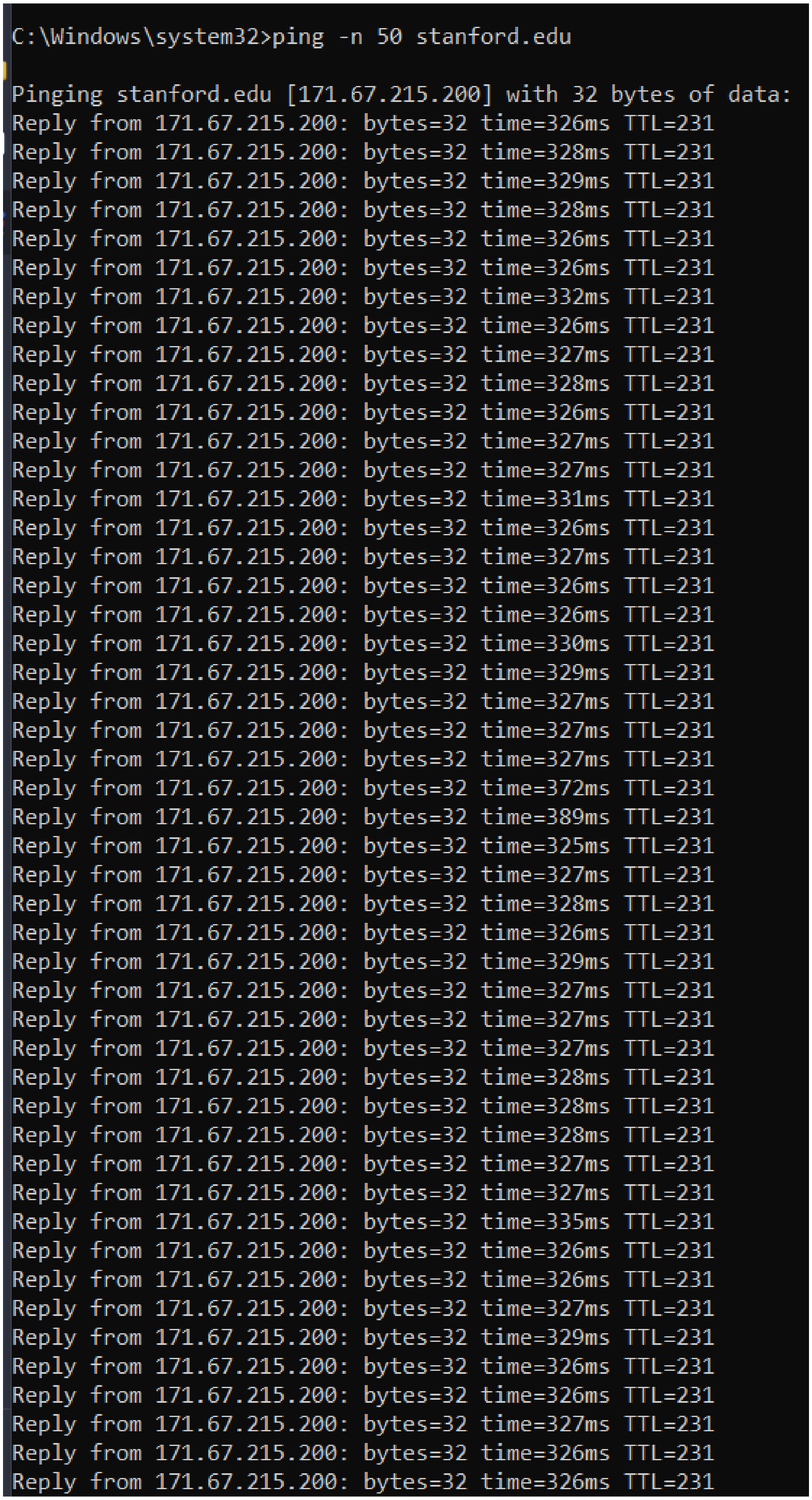


```
Ping statistics for 142.250.192.164:
    Packets: Sent = 50, Received = 50, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 15ms, Average = 6ms
```

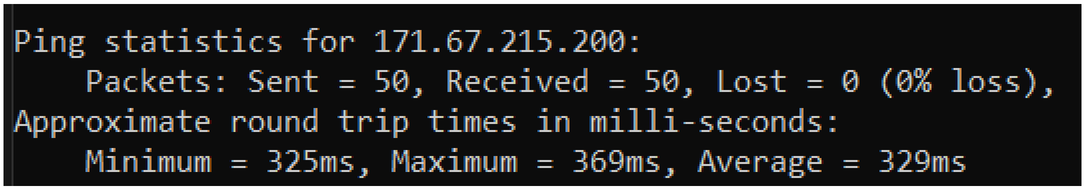
3. Average of latencies in (a) = 6.6, which is not equal to the average in part (b), this is because both of these are taking different paths for the packets.
4. Max ping latency is 10ms in (a) while in (b) it is 29ms, this is also because of that two different routes may be taken by the commands.
5. The three column entries while using tracert corresponding to the RTT (round trip time), which are counted 3 times, hence three columns.

6. 50 pings to stanford.edu:

   Average Latency: 329 ms.

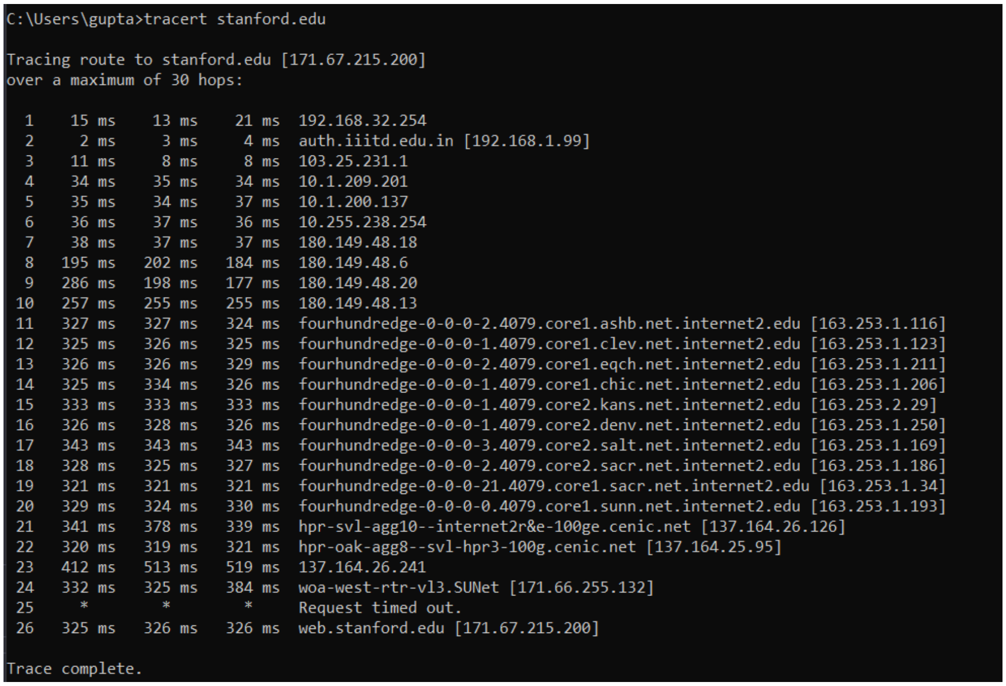


```
C:\Windows\system32>ping -n 50 stanford.edu

Pinging stanford.edu [171.67.215.200] with 32 bytes of data:
Reply from 171.67.215.200: bytes=32 time=326ms TTL=231
Reply from 171.67.215.200: bytes=32 time=328ms TTL=231
Reply from 171.67.215.200: bytes=32 time=329ms TTL=231
Reply from 171.67.215.200: bytes=32 time=328ms TTL=231
Reply from 171.67.215.200: bytes=32 time=326ms TTL=231
Reply from 171.67.215.200: bytes=32 time=326ms TTL=231
Reply from 171.67.215.200: bytes=32 time=332ms TTL=231
Reply from 171.67.215.200: bytes=32 time=326ms TTL=231
Reply from 171.67.215.200: bytes=32 time=327ms TTL=231
Reply from 171.67.215.200: bytes=32 time=328ms TTL=231
Reply from 171.67.215.200: bytes=32 time=326ms TTL=231
Reply from 171.67.215.200: bytes=32 time=327ms TTL=231
Reply from 171.67.215.200: bytes=32 time=327ms TTL=231
Reply from 171.67.215.200: bytes=32 time=331ms TTL=231
Reply from 171.67.215.200: bytes=32 time=326ms TTL=231
Reply from 171.67.215.200: bytes=32 time=327ms TTL=231
Reply from 171.67.215.200: bytes=32 time=326ms TTL=231
Reply from 171.67.215.200: bytes=32 time=326ms TTL=231
Reply from 171.67.215.200: bytes=32 time=330ms TTL=231
Reply from 171.67.215.200: bytes=32 time=329ms TTL=231
Reply from 171.67.215.200: bytes=32 time=327ms TTL=231
Reply from 171.67.215.200: bytes=32 time=327ms TTL=231
Reply from 171.67.215.200: bytes=32 time=327ms TTL=231
Reply from 171.67.215.200: bytes=32 time=372ms TTL=231
Reply from 171.67.215.200: bytes=32 time=389ms TTL=231
Reply from 171.67.215.200: bytes=32 time=325ms TTL=231
Reply from 171.67.215.200: bytes=32 time=327ms TTL=231
Reply from 171.67.215.200: bytes=32 time=328ms TTL=231
Reply from 171.67.215.200: bytes=32 time=326ms TTL=231
Reply from 171.67.215.200: bytes=32 time=329ms TTL=231
Reply from 171.67.215.200: bytes=32 time=327ms TTL=231
Reply from 171.67.215.200: bytes=32 time=327ms TTL=231
Reply from 171.67.215.200: bytes=32 time=327ms TTL=231
Reply from 171.67.215.200: bytes=32 time=328ms TTL=231
Reply from 171.67.215.200: bytes=32 time=328ms TTL=231
Reply from 171.67.215.200: bytes=32 time=328ms TTL=231
Reply from 171.67.215.200: bytes=32 time=327ms TTL=231
Reply from 171.67.215.200: bytes=32 time=327ms TTL=231
Reply from 171.67.215.200: bytes=32 time=335ms TTL=231
Reply from 171.67.215.200: bytes=32 time=326ms TTL=231
Reply from 171.67.215.200: bytes=32 time=326ms TTL=231
Reply from 171.67.215.200: bytes=32 time=327ms TTL=231
Reply from 171.67.215.200: bytes=32 time=329ms TTL=231
Reply from 171.67.215.200: bytes=32 time=326ms TTL=231
Reply from 171.67.215.200: bytes=32 time=326ms TTL=231
Reply from 171.67.215.200: bytes=32 time=327ms TTL=231
Reply from 171.67.215.200: bytes=32 time=326ms TTL=231
Reply from 171.67.215.200: bytes=32 time=326ms 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 = 325ms, Maximum = 369ms, Average = 329ms
```

7. Tracert for stanford.edu:



```
C:\Users\gupta>tracert stanford.edu

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

  1    15 ms    13 ms    21 ms  192.168.32.254
  2     2 ms     3 ms     4 ms  auth.iiitd.edu.in [192.168.1.99]
  3    11 ms     8 ms     8 ms  103.25.231.1
  4    34 ms    35 ms    34 ms  10.1.209.201
  5    35 ms    34 ms    37 ms  10.1.200.137
  6    36 ms    37 ms    36 ms  10.255.238.254
  7    38 ms    37 ms    37 ms  180.149.48.18
  8   195 ms   202 ms   184 ms  180.149.48.6
  9   286 ms   198 ms   177 ms  180.149.48.20
 10   257 ms   255 ms   255 ms  180.149.48.13
 11   327 ms   327 ms   324 ms  fourhundredge-0-0-0-2.4079.core1.ashb.net.internet2.edu [163.253.1.116]
 12   325 ms   326 ms   325 ms  fourhundredge-0-0-0-1.4079.core1.clev.net.internet2.edu [163.253.1.123]
 13   326 ms   326 ms   329 ms  fourhundredge-0-0-0-2.4079.core1.eqch.net.internet2.edu [163.253.1.211]
 14   325 ms   334 ms   326 ms  fourhundredge-0-0-0-1.4079.core1.chic.net.internet2.edu [163.253.1.206]
 15   333 ms   333 ms   333 ms  fourhundredge-0-0-0-1.4079.core2.kans.net.internet2.edu [163.253.2.29]
 16   326 ms   328 ms   326 ms  fourhundredge-0-0-0-1.4079.core2.denv.net.internet2.edu [163.253.1.250]
 17   343 ms   343 ms   343 ms  fourhundredge-0-0-0-3.4079.core2.salt.net.internet2.edu [163.253.1.169]
 18   328 ms   325 ms   327 ms  fourhundredge-0-0-0-2.4079.core2.sacr.net.internet2.edu [163.253.1.186]
 19   321 ms   321 ms   321 ms  fourhundredge-0-0-0-21.4079.core1.sacr.net.internet2.edu [163.253.1.34]
 20   329 ms   324 ms   330 ms  fourhundredge-0-0-0-0.4079.core1.sunn.net.internet2.edu [163.253.1.193]
 21   341 ms   378 ms   339 ms  hpr-svl-agg10--internet2r&e-100ge.cenic.net [137.164.26.126]
 22   320 ms   319 ms   321 ms  hpr-oak-agg8--svl-hpr3-100g.cenic.net [137.164.25.95]
 23   412 ms   513 ms   519 ms  137.164.26.241
 24   332 ms   325 ms   384 ms  woa-west-rtr-vl3.SUNet [171.66.255.132]
 25     *        *        *     Request timed out.
 26   325 ms   326 ms   326 ms  web.stanford.edu [171.67.215.200]

Trace complete.
```

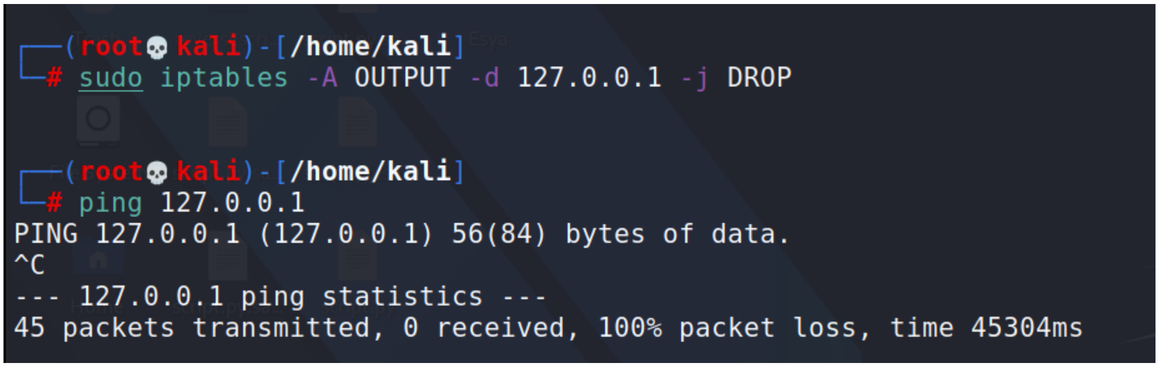
Comparing google.in and stanford.edu, the number of hops are way more in case of stanford, and the RTT is higher as well.

8. Some of the reasons for latency differences:
   - Physical Topology: google.in server may be closer than stanford.edu
   - Routing: Routing protocols may differ between the two servers.
   - Network optimisation: Google uses sophisticated CDNs (Content delivery networks) for better data delivery, unlike stanford.

Question 4

The below screenshot shows that all the packets sent to 127.0.0.1 were dropped, and therefore 100% packet loss.
This was acheived by configuring *iptables* which helps filter network traffic using policies.
The DROP, filters them out by dropping them.
Therefore a policy was created to drop all the packets that were sent to 127.0.0.1, which is the loopback address to the device.
Flags:

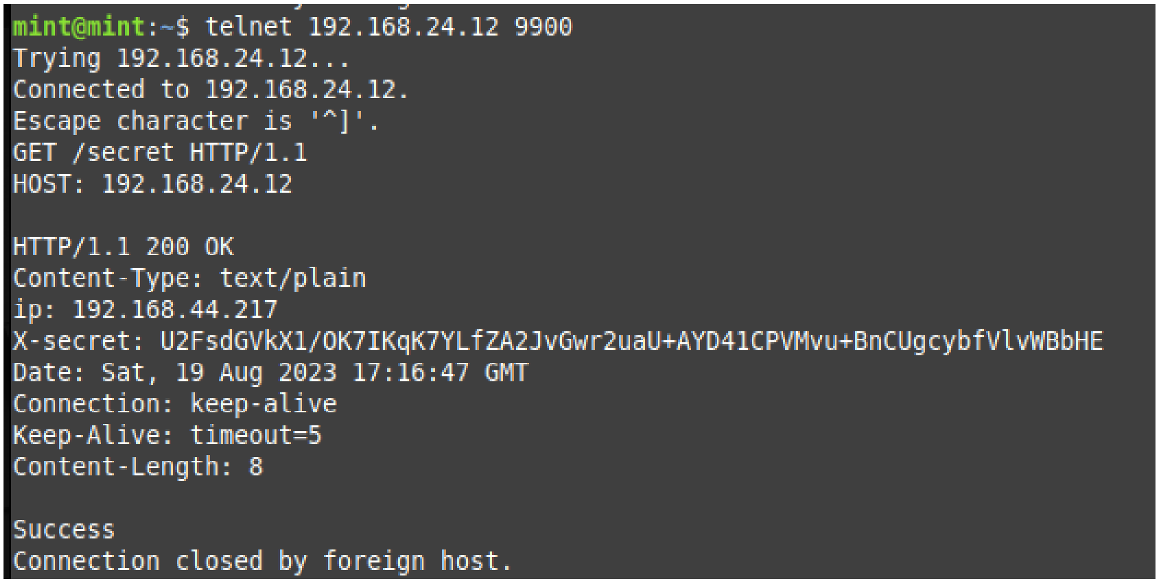
- *-A: Append rule to the selected chain.*
- *-d: destination.*
- *-j: jump.*



```
┌──(root💀kali)-[/home/kali]
└─# sudo iptables -A OUTPUT -d 127.0.0.1 -j DROP

┌──(root💀kali)-[/home/kali]
└─# 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 ---
45 packets transmitted, 0 received, 100% packet loss, time 45304ms
```

Question 5

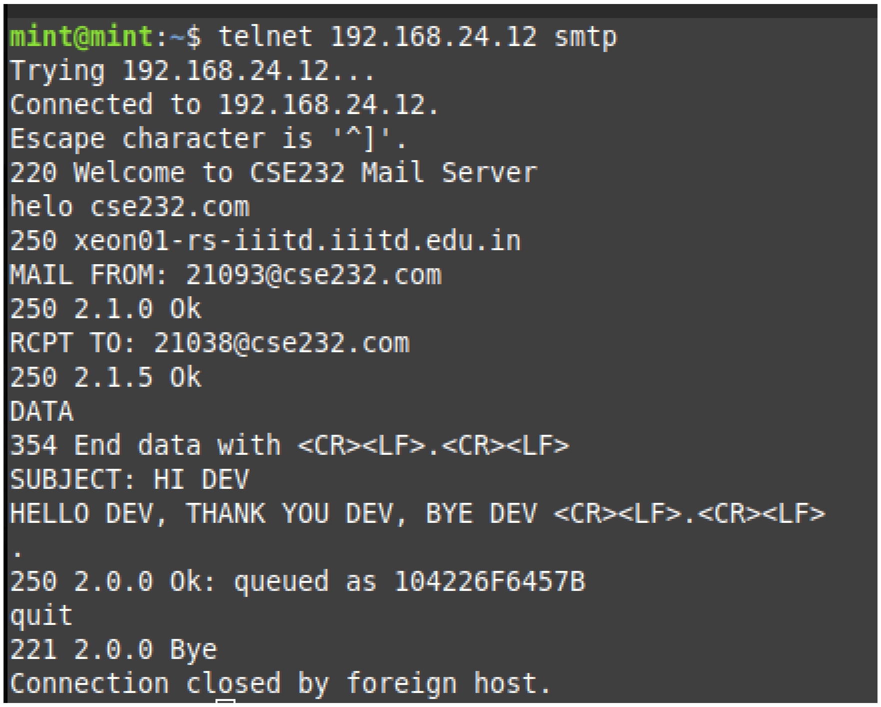
Here is the successful connection from telnet:



```
mint@mint:~$ 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: 192.168.44.217
X-secret: U2FsdGVkX1/OK7IKqK7YLfZA2JvGwr2uaU+AYD41CPVMvu+BnCUgcybfVlvWBbHE
Date: Sat, 19 Aug 2023 17:16:47 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Content-Length: 8

Success
Connection closed by foreign host.
```

Question 6

Output from the SMTP sent to my dear friend DEV MITTAL.



```
mint@mint:~$ 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: 21093@cse232.com
250 2.1.0 Ok
RCPT TO: 21038@cse232.com
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
SUBJECT: HI DEV
HELLO DEV, THANK YOU DEV, BYE DEV <CR><LF>.<CR><LF>
.
250 2.0.0 Ok: queued as 104226F6457B
quit
221 2.0.0 Bye
Connection closed by foreign host.
```