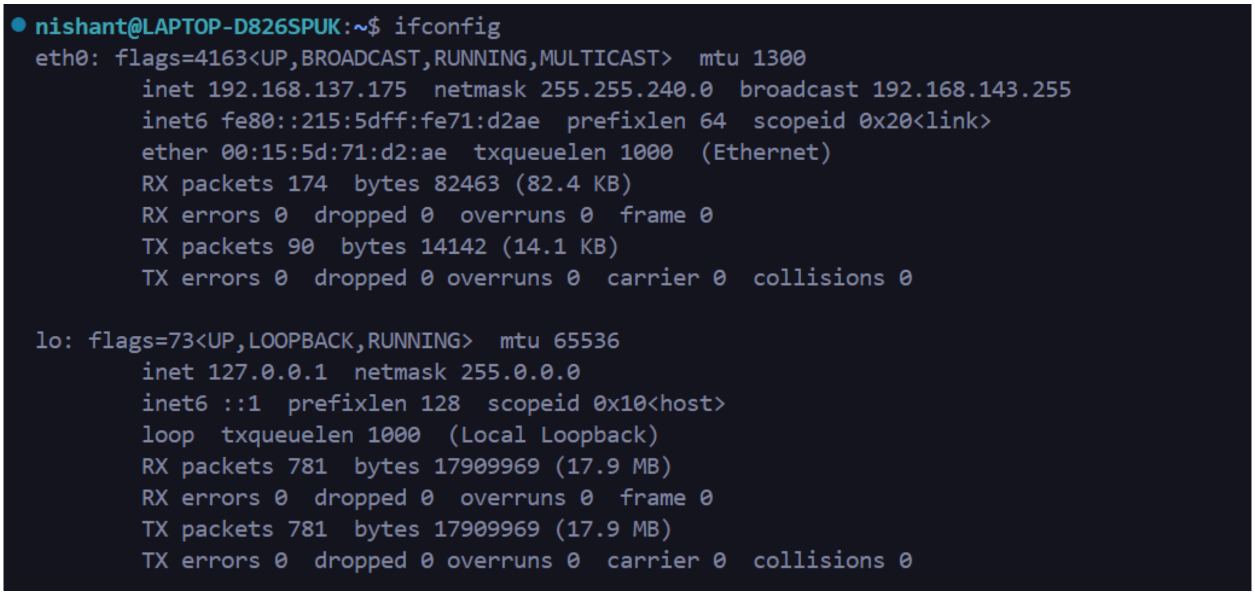
CSE 232: Programming Assignment 1

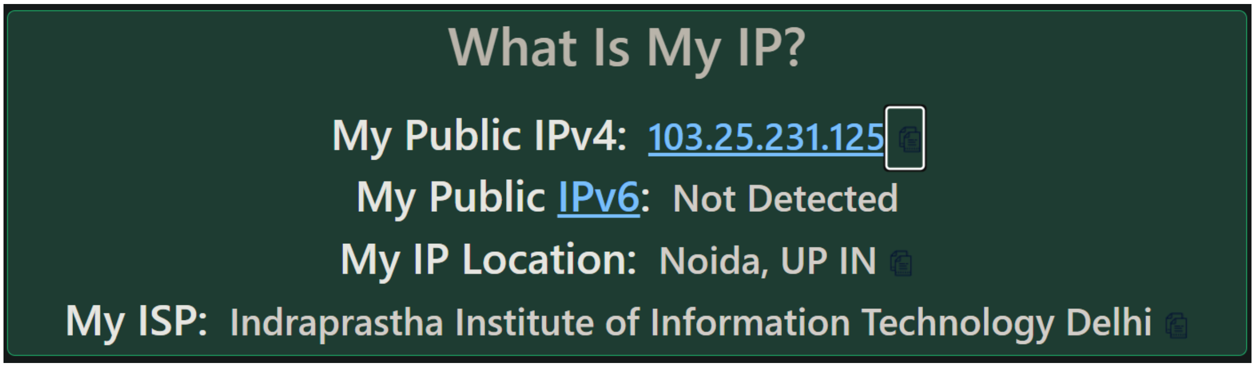
Name - Nishant Yadav
Roll No - 2022329

1. (a) The interface associated with the active network connection is eth0, and the IP Address is in the inet entry: 192.168.137.175



```
nishant@LAPTOP-D826SPUK:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1300
        inet 192.168.137.175  netmask 255.255.240.0  broadcast 192.168.143.255
        inet6 fe80::215:5dff:fe71:d2ae  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:71:d2:ae  txqueuelen 1000  (Ethernet)
        RX packets 174  bytes 82463 (82.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 90  bytes 14142 (14.1 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 781  bytes 17909969 (17.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 781  bytes 17909969 (17.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

(b) The IP Address on www.whatismyip.com is different because the IP Address we got after using ifconfig is a private or local IP that is assigned by the router. Whereas the IP on the website i.e. 103.25.231.125 is a public IP address that is provided by the ISP. Other devices see this address when we are connected over the internet. When we connect to the internet, the router translates local IP address into public IP address, this is known as Network Address Translation (NAT), that is why websites see the public IP address instead of the local one.



What Is My IP?

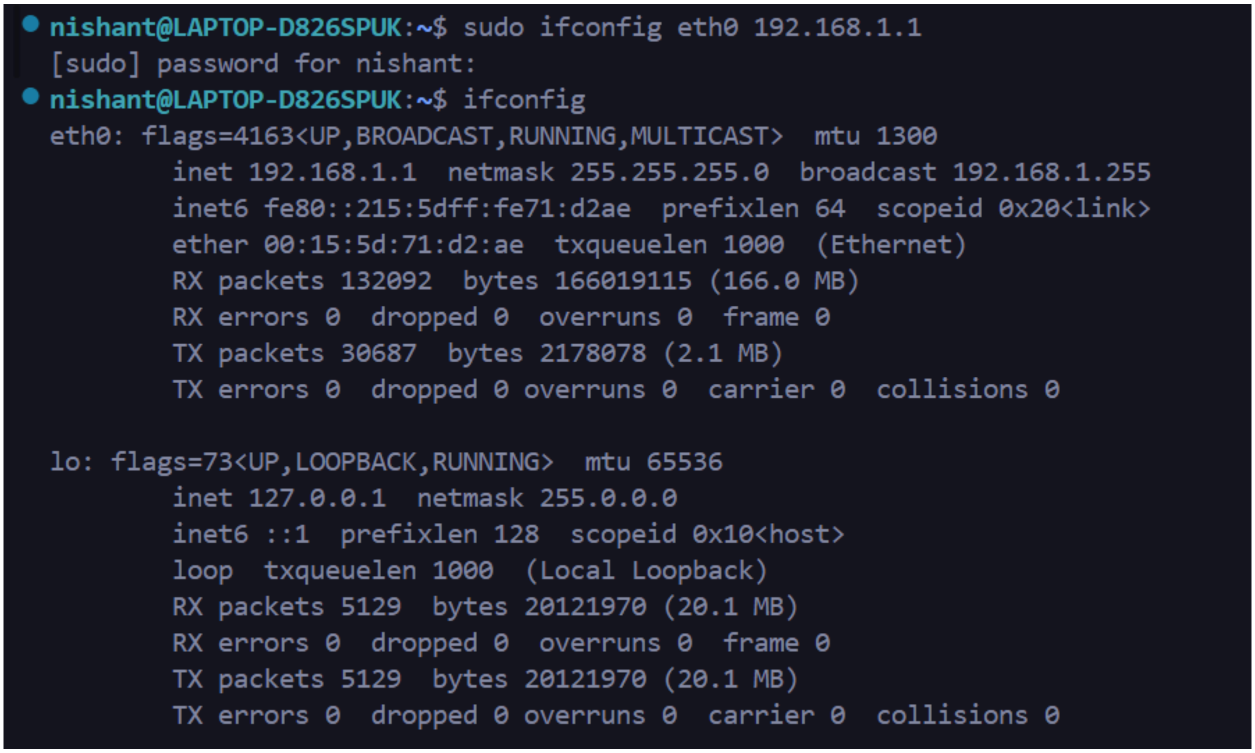
My Public IPv4: 103.25.231.125

My Public IPv6: Not Detected

My IP Location: Noida, UP IN

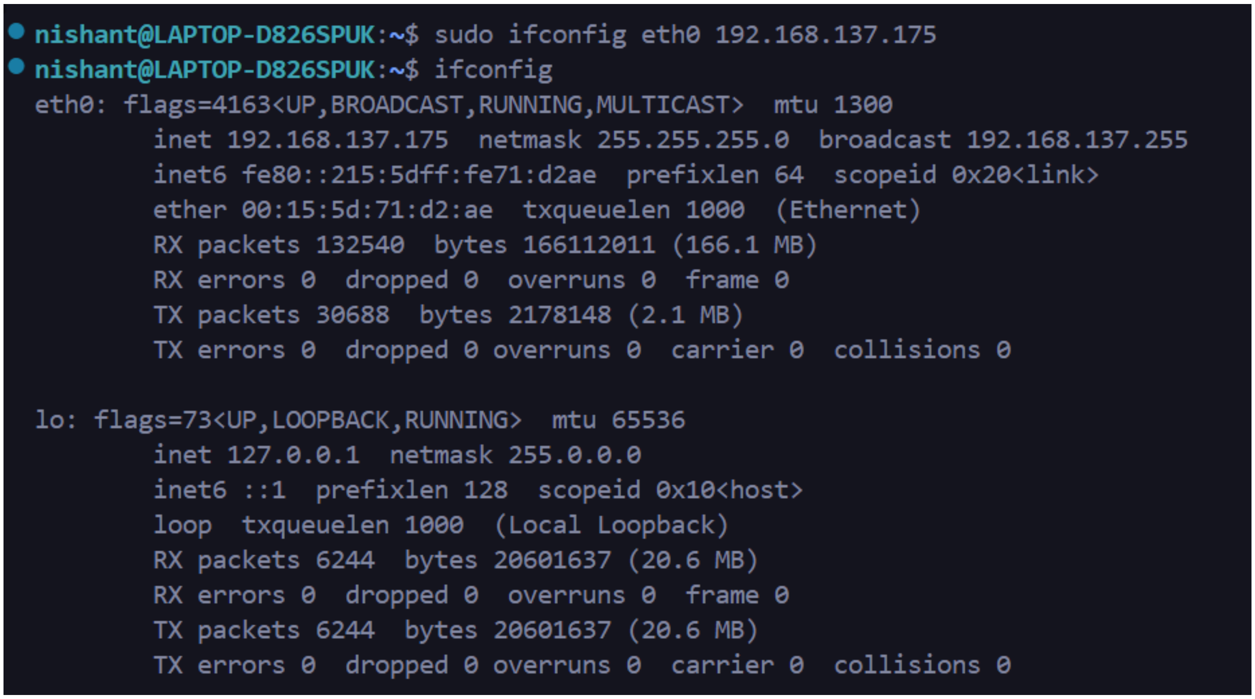
My ISP: Indraprastha Institute of Information Technology Delhi

2. I changed the IP address of eth0 to 192.168.1.1



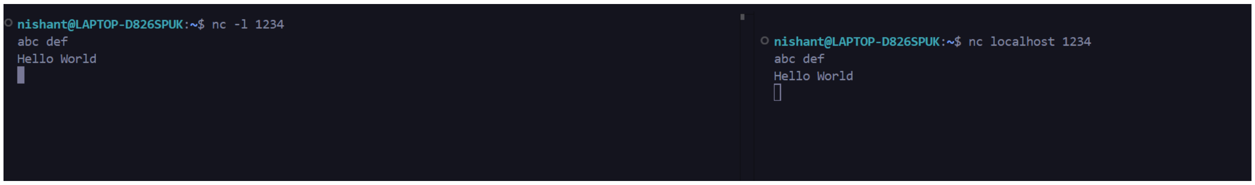
```
nishant@LAPTOP-D826SPUK:~$ sudo ifconfig eth0 192.168.1.1
[sudo] password for nishant:
nishant@LAPTOP-D826SPUK:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1300
        inet 192.168.1.1  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::215:5dff:fe71:d2ae  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:71:d2:ae  txqueuelen 1000  (Ethernet)
        RX packets 132092  bytes 166019115 (166.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30687  bytes 2178078 (2.1 MB)
        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 5129  bytes 20121970 (20.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5129  bytes 20121970 (20.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

I reverted it to the original address using the same command



```
nishant@LAPTOP-D826SPUK:~$ sudo ifconfig eth0 192.168.137.175
nishant@LAPTOP-D826SPUK:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1300
        inet 192.168.137.175  netmask 255.255.255.0  broadcast 192.168.137.255
        inet6 fe80::215:5dff:fe71:d2ae  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:71:d2:ae  txqueuelen 1000  (Ethernet)
        RX packets 132540  bytes 166112011 (166.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30688  bytes 2178148 (2.1 MB)
        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 6244  bytes 20601637 (20.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6244  bytes 20601637 (20.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

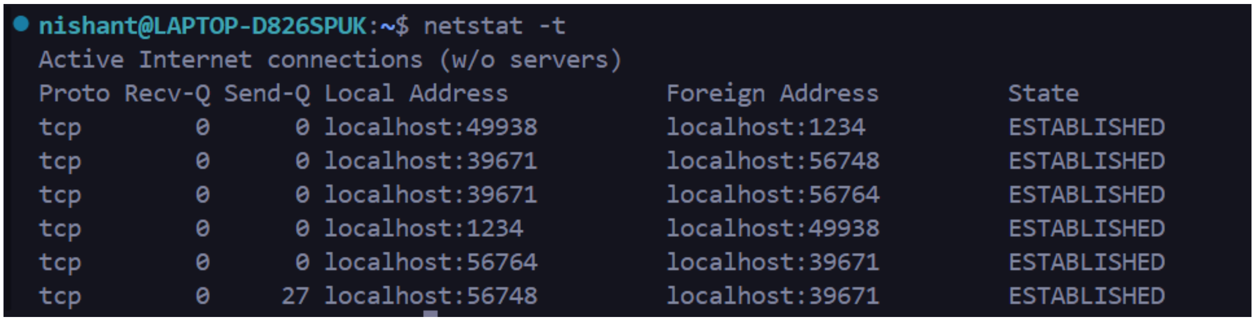
3. (a) I set up a TCP server with port number ‘1234’



```
nishant@LAPTOP-D826SPUK:~$ nc -l 1234
abc def
Hello World
```

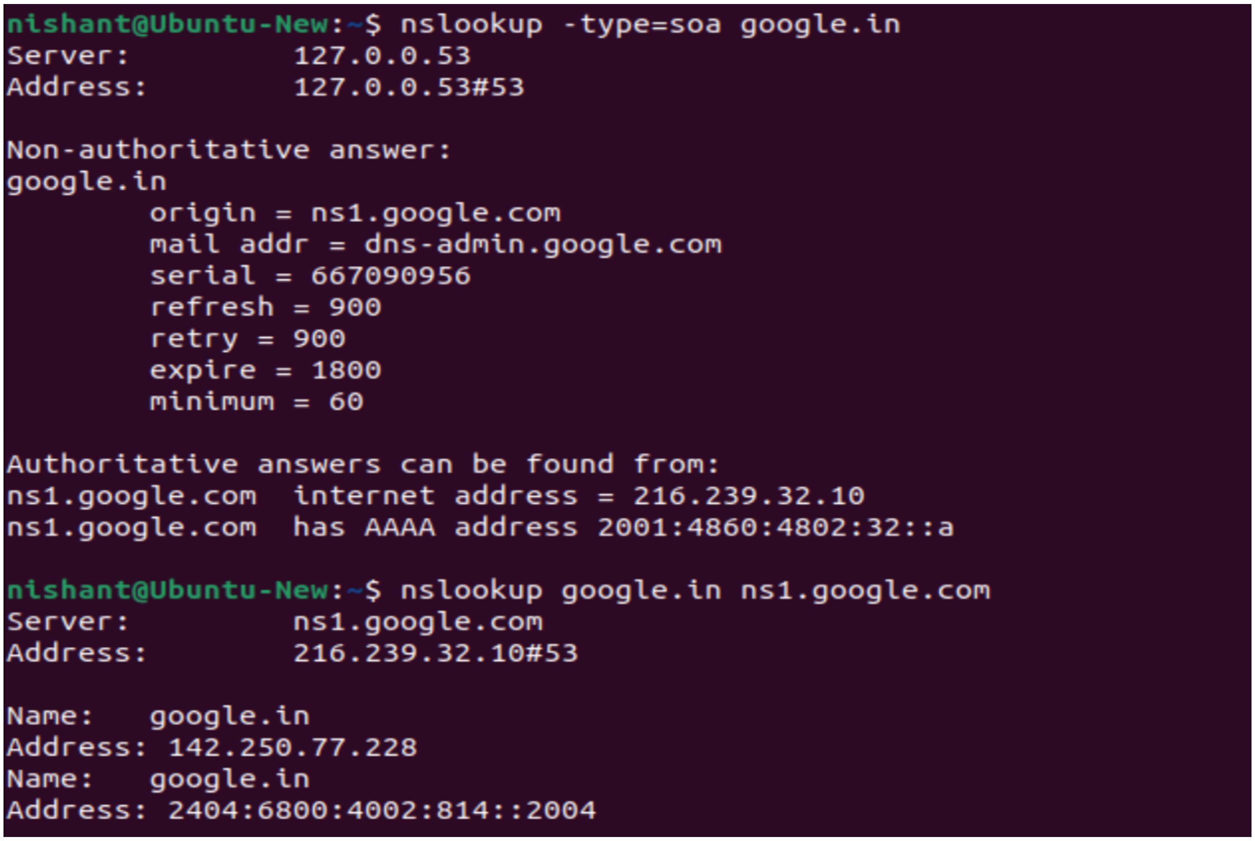
```
nishant@LAPTOP-D826SPUK:~$ nc localhost 1234
abc def
Hello World
```

(b) The state of this connection is ‘ESTABLISHED’



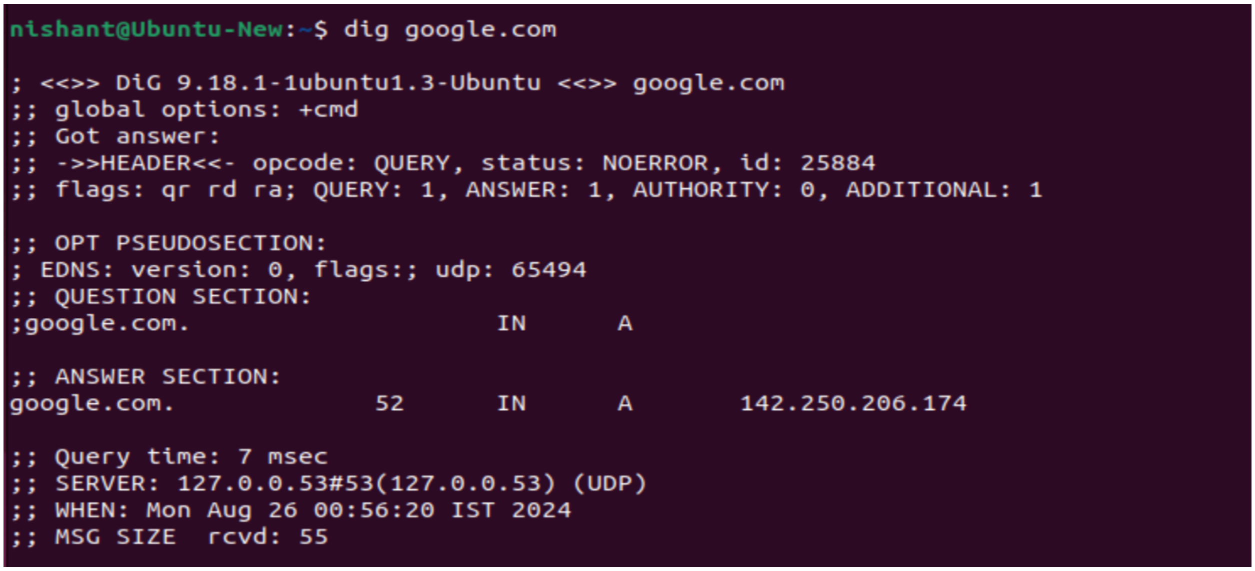
```
nishant@LAPTOP-D826SPUK:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:49938         localhost:1234          ESTABLISHED
tcp        0      0 localhost:39671         localhost:56748         ESTABLISHED
tcp        0      0 localhost:39671         localhost:56764         ESTABLISHED
tcp        0      0 localhost:1234          localhost:49938         ESTABLISHED
tcp        0      0 localhost:56764         localhost:39671         ESTABLISHED
tcp        0     27 localhost:56748         localhost:39671         ESTABLISHED
```

4. (a) I first ran the nslookup command with option -type=soa option to get the authoritative information which includes the primary name server of google.in
I then ran the nslookup command with the primary name



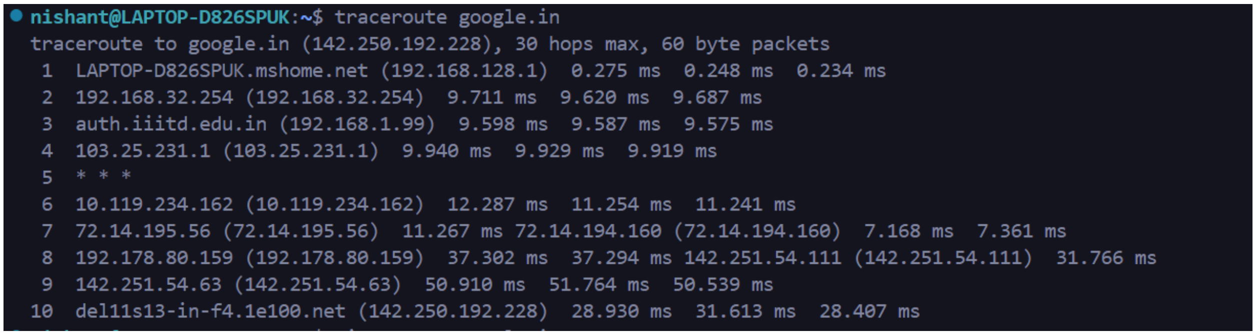
```
nishant@Ubuntu-New:~$ nslookup -type=soa google.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.in
        origin = ns1.google.com
        mail addr = dns-admin.google.com
        serial = 667090956
        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

nishant@Ubuntu-New:~$ nslookup google.in ns1.google.com
Server:         ns1.google.com
Address:        216.239.32.10#53

Name:   google.in
Address: 142.250.77.228
Name:   google.in
Address: 2404:6800:4002:814::2004
```

(b) It would take 52 seconds before this entry expires from the local DNS.



```
nishant@Ubuntu-New:~$ dig google.com

; <<>> DiG 9.18.1-1ubuntu1.3-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25884
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
google.com.             52      IN      A       142.250.206.174

;; Query time: 7 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Aug 26 00:56:20 IST 2024
;; MSG SIZE  rcvd: 55
```

5. (a) There are 10 intermediate hosts



```
nishant@LAPTOP-D826SPUK:~$ traceroute google.in
traceroute to google.in (142.250.192.228), 30 hops max, 60 byte packets
 1  LAPTOP-D826SPUK.mshome.net (192.168.128.1)  0.275 ms  0.248 ms  0.234 ms
 2  192.168.32.254 (192.168.32.254)  9.711 ms  9.620 ms  9.687 ms
 3  auth.iiitd.edu.in (192.168.1.99)  9.598 ms  9.587 ms  9.575 ms
 4  103.25.231.1 (103.25.231.1)  9.940 ms  9.929 ms  9.919 ms
 5  * * *
 6  10.119.234.162 (10.119.234.162)  12.287 ms  11.254 ms  11.241 ms
 7  72.14.195.56 (72.14.195.56)  11.267 ms 72.14.194.160 (72.14.194.160)  7.168 ms  7.361 ms
 8  192.178.80.159 (192.178.80.159)  37.302 ms  37.294 ms 142.251.54.111 (142.251.54.111)  31.766 ms
 9  142.251.54.63 (142.251.54.63)  50.910 ms  51.764 ms  50.539 ms
10  del11s13-in-f4.1e100.net (142.250.192.228)  28.930 ms  31.613 ms  28.407 ms
```

1) LAPTOP-D826SPUK.mshome.net (192.168.128.1)

   Average Latency: (0.275 + 0.248 + 0.234) / 3 = 0.252 ms

2) 192.168.32.254 (192.168.32.254)

   Average Latency: (9.711 + 9.620 + 9.687) / 3 = 9.673 ms

3) auth.iiitd.edu.in (192.168.1.99)

   Average Latency: (9.598 + 9.587 + 9.575) / 3 = 9.587 ms

4) 103.25.231.1 (103.25.231.1)

   Average Latency: (9.940 + 9.929 + 9.919) / 3 = 9.929 ms

5) 10.119.234.162 (10.119.234.162)

   Average Latency: (12.287 + 11.254 + 11.241) / 3 = 11.594 ms

6) 72.14.195.56 (72.14.195.56)

   Average Latency: 11.267 ms

7) 72.14.194.160 (72.14.194.160)

   Average Latency: (7.168 + 7.361) / 2 = 7.265 ms

8) 192.178.80.159 (192.178.80.159)

   Average Latency: 37.302 ms

9) 142.251.54.111 (142.251.54.111)

   Average Latency: 31.766 ms

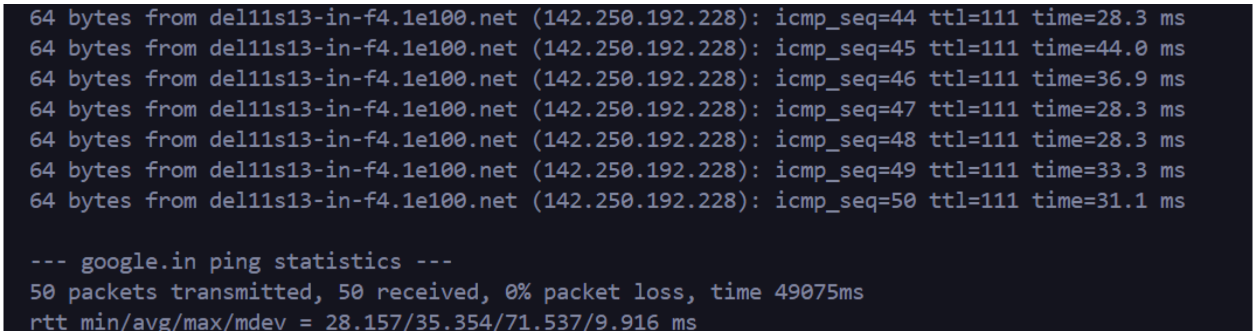
10) 142.251.54.63 (142.251.54.63)

   Average Latency: (50.910 + 51.764 + 50.539) / 3 = 51.071 ms

Destination - del11s13-in-f4.1e100.net (142.250.192.228) (Google server)

- Latencies: 28.930 ms, 31.613 ms, 28.407 ms
- Average Latency: (28.930 + 31.613 + 28.407) / 3 = 29.650 ms

(b) I used the command ‘ping -c 50 google.in’. The average latency is 35.354 ms



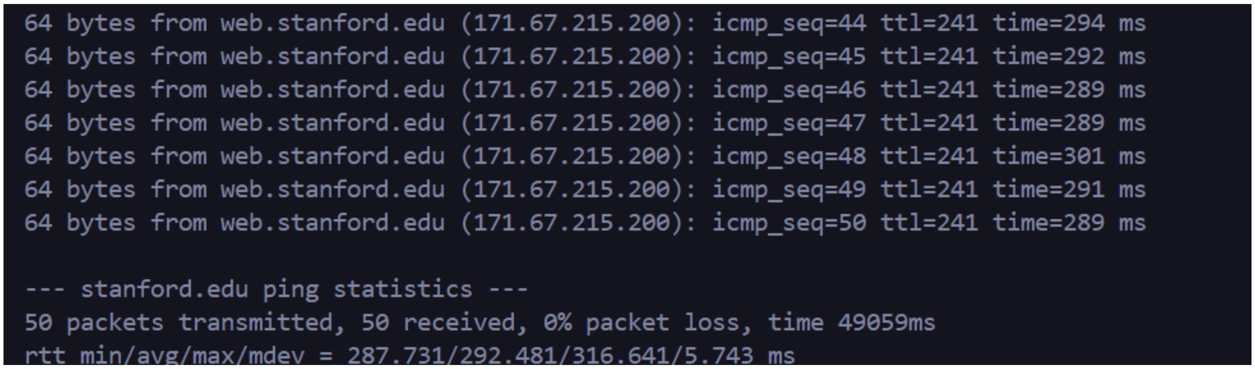
```
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=44 ttl=111 time=28.3 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=45 ttl=111 time=44.0 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=46 ttl=111 time=36.9 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=47 ttl=111 time=28.3 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=48 ttl=111 time=28.3 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=49 ttl=111 time=33.3 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=50 ttl=111 time=31.1 ms

--- google.in ping statistics ---
50 packets transmitted, 50 received, 0% packet loss, time 49075ms
rtt min/avg/max/mdev = 28.157/35.354/71.537/9.916 ms
```

(c) The sum of average latency of all the intermediate hosts in (a) is 179.706 ms. This is higher than the average latency for ping because ping measures the round trip time directly to the final destination, but traceroute measures the time for each hop individually. Additionally traceroute measures multiple times for each hop, which causes delays.

(d) The maximum latency among the intermediate hosts in (a) is 51.071 ms. This is higher than the average ping latency in (b) which is 35.354 ms. This is because when we use traceroute, it gives us latency between each intermediate hosts, and there can be some congested points with a lot of traffic that can cause delays. However when we use ping, it measures the direct round-trip time to the destination.

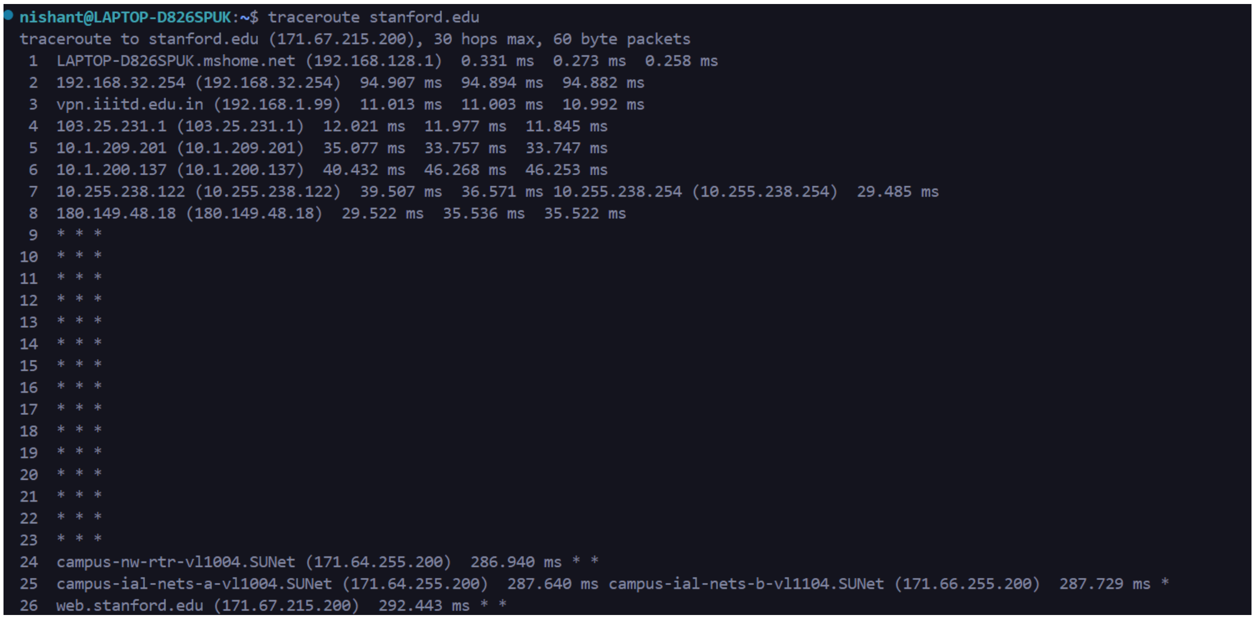
(e) Traceroute sends multiple packets to each hop. Each entry corresponds to the round-trip time it takes for an individual packet in each hop.

(f) The average latency is 292.481 ms



```
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=44 ttl=241 time=294 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=45 ttl=241 time=292 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=46 ttl=241 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=47 ttl=241 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=48 ttl=241 time=301 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=49 ttl=241 time=291 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=50 ttl=241 time=289 ms

--- stanford.edu ping statistics ---
50 packets transmitted, 50 received, 0% packet loss, time 49059ms
rtt min/avg/max/mdev = 287.731/292.481/316.641/5.743 ms
```

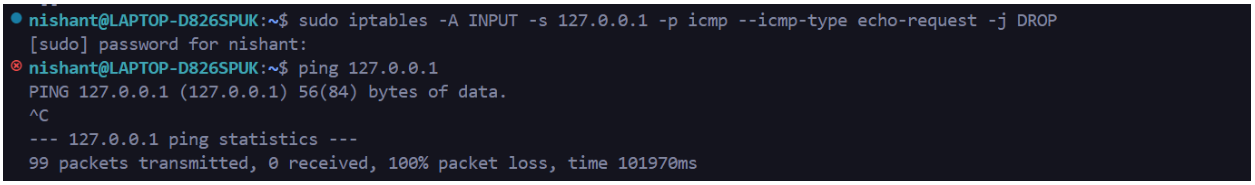
(g) The number of hops is 26 for stanford.edu as compared to 10 for google.in
This means there are more intermediate hosts for stanford.edu



```
nishant@LAPTOP-D826SPUK:~$ traceroute stanford.edu
traceroute to stanford.edu (171.67.215.200), 30 hops max, 60 byte packets
 1  LAPTOP-D826SPUK.mshome.net (192.168.128.1)  0.331 ms  0.273 ms  0.258 ms
 2  192.168.32.254 (192.168.32.254)  94.907 ms  94.894 ms  94.882 ms
 3  vpn.iiitd.edu.in (192.168.1.99)  11.013 ms  11.003 ms  10.992 ms
 4  103.25.231.1 (103.25.231.1)  12.021 ms  11.977 ms  11.845 ms
 5  10.1.209.201 (10.1.209.201)  35.077 ms  33.757 ms  33.747 ms
 6  10.1.200.137 (10.1.200.137)  40.432 ms  46.268 ms  46.253 ms
 7  10.255.238.122 (10.255.238.122)  39.507 ms  36.571 ms 10.255.238.254 (10.255.238.254)  29.485 ms
 8  180.149.48.18 (180.149.48.18)  29.522 ms  35.536 ms  35.522 ms
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  campus-nw-rtr-vl1004.SUNet (171.64.255.200)  286.940 ms * *
25  campus-ial-nets-a-vl1004.SUNet (171.64.255.200)  287.640 ms campus-ial-nets-b-vl1104.SUNet (171.66.255.200)  287.729 ms *
26  web.stanford.edu (171.67.215.200)  292.443 ms * *
```

(h) The latency for stanford.edu (292.481 ms) is more than google.in (35.354 ms) because there are more intermediate hosts for stanford.edu. The path for google.in is more optimized as there are less intermediate hosts which is not the case for stanford.edu

6. I blocked the ICMP traffic for 127.0.0.1
   This will result in 100% packet loss when we use ping



```
● nishant@LAPTOP-D826SPUK:~$ sudo iptables -A INPUT -s 127.0.0.1 -p icmp --icmp-type echo-request -j DROP
  [sudo] password for nishant:
⊗ nishant@LAPTOP-D826SPUK:~$ 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 ---
  99 packets transmitted, 0 received, 100% packet loss, time 101970ms
```