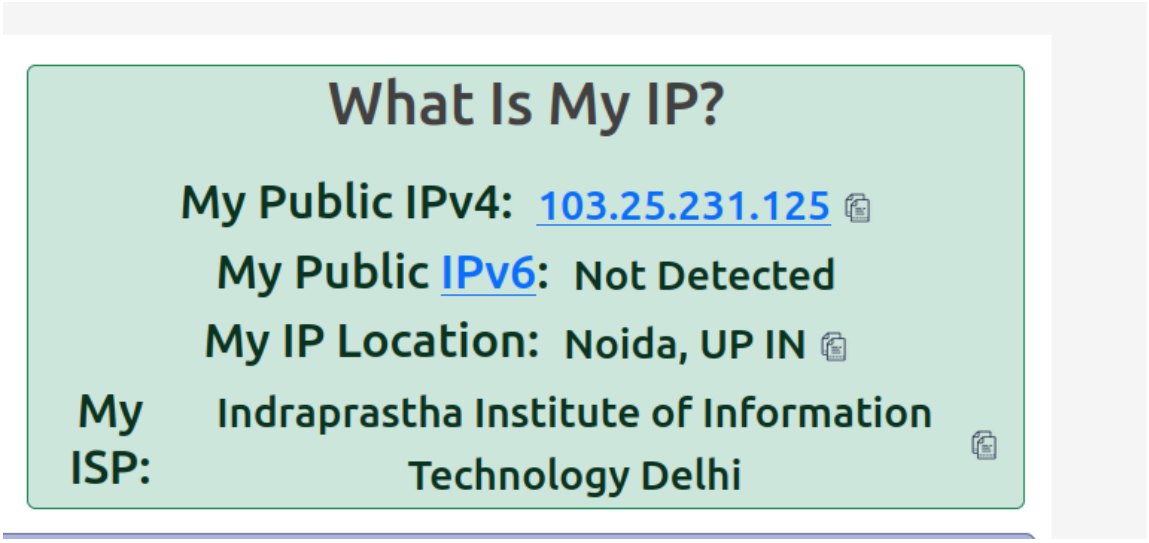
1. a)

```
shashwat@shashwat-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::5032:f071:17cf:4d94  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1e:cf:bf  txqueuelen 1000  (Ethernet)
        RX packets 12323  bytes 11225566 (11.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8427  bytes 4159872 (4.1 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 2302  bytes 230292 (230.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2302  bytes 230292 (230.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

shashwat@shashwat-VirtualBox:~$
```

IP Address: 10.0.2.15

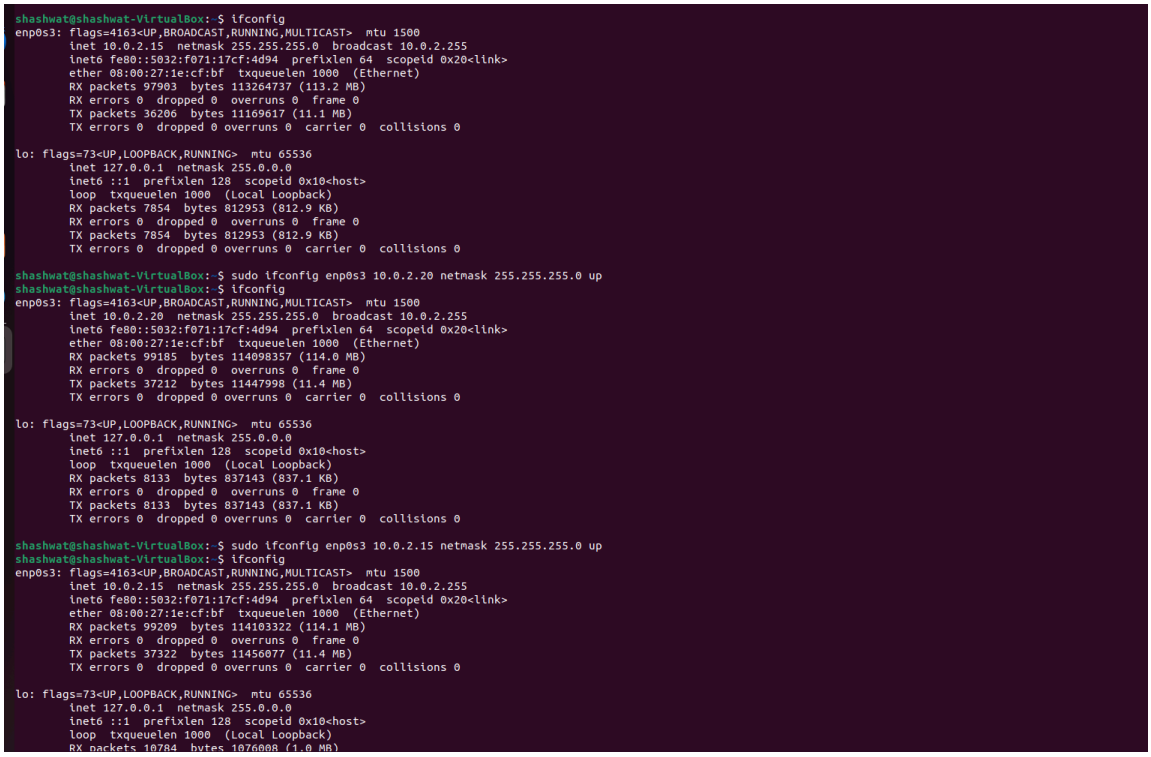
b)



The IP Addresses are different.

This is because the ip address displayed by the ifconfig command is a private IP address, which is assigned by the router to the device on the local network whereas the IP address on the website is a public IP address. The public IP address is the address of the router, which is assigned by the ISP. The router then assigns private IP addresses to the devices on the local network.

2.



First, I showed the current address using the ‘ifconfig’ command.
Then I changed the ip address from 10.0.2.15 to 10.0.2.20 using the ‘sudo ifconfig enp0s3 10.0.2.20 netmask 255.255.255.0 up’ command.
I displayed the change using the ‘ifconfig’ command and then reverted the change.

3. a)

```
C:\Users\mriga>ncat -l -p 2222
Ubuntu says hello \n
Windows says hello as well \n
```

I set up a TCP client/server connection between my VM and host machine.
I then sent messages from both the client and the server to show that the connection has been established properly.

b)

```
shashwat@shashwat-VirtualBox:~$ netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.15:51852         172.217.167.197:443     ESTABLISHED
tcp        0      0 10.0.2.15:44570         142.250.207.202:443     ESTABLISHED
tcp        0      0 10.0.2.15:36692         172.217.166.195:443     ESTABLISHED
tcp        0      0 10.0.2.15:43956         142.250.193.238:443     ESTABLISHED
tcp        0      0 10.0.2.15:53530         142.250.193.206:443     ESTABLISHED
tcp        0      0 10.0.2.15:58334         142.250.194.14:443      ESTABLISHED
tcp        0      0 10.0.2.15:53002         142.250.182.170:443     TIME_WAIT
tcp        0      0 10.0.2.15:46226         142.250.193.46:443      ESTABLISHED
tcp        0      0 10.0.2.15:48998         172.217.166.195:443     ESTABLISHED
tcp        0      0 10.0.2.15:57600         34.107.243.93:443       ESTABLISHED
tcp        0      0 10.0.2.15:50732         192.168.42.194:2222     ESTABLISHED
tcp        0      0 10.0.2.15:39924         142.250.195.10:443      ESTABLISHED
tcp6       0      0 ::1:631                 :::*                    LISTEN
shashwat@shashwat-VirtualBox:~$
```

As we can see in the third entry from the bottom, the TCP connection between the host machine and the vm is established.

4. a)

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

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

Authoritative answers can be found from:
ns4.google.com  internet address = 216.239.38.10
ns3.google.com  internet address = 216.239.36.10
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

shashwat@shashwat-VirtualBox:~$ 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

shashwat@shashwat-VirtualBox:~$
```

To get an authoritative result for ‘google.in’, I first found the DNS server and then queried that DNS server.

I first used the command ‘nslookup -type=ns google.in’ to obtain the authoritative DNS server.
I then used the ‘nslookup google.in ns1.google.com’ command to use one of the DNS servers to query the domain name and get the authoritative result.

b)

```
shashwat@shashwat-VirtualBox:~$ nslookup -debug youtube.com
Server:         127.0.0.53
Address:        127.0.0.53#53

------------
    QUESTIONS:
        youtube.com, type = A, class = IN
    ANSWERS:
    ->  youtube.com
        internet address = 142.250.194.14
        ttl = 191
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Non-authoritative answer:
Name:   youtube.com
Address: 142.250.194.14
------------
    QUESTIONS:
        youtube.com, type = AAAA, class = IN
    ANSWERS:
    ->  youtube.com
        has AAAA address 2404:6800:4002:81e::200e
        ttl = 191
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Name:   youtube.com
Address: 2404:6800:4002:81e::200e
```

This entry would expire after 191 seconds from the local DNS server.

5. a)

```
PS C:\Users\mriga> tracert google.in

Tracing route to google.in [142.250.193.4]
over a maximum of 30 hops:

  1    21 ms    17 ms   159 ms  192.168.32.254
  2     4 ms     2 ms    10 ms  vpn.iiitd.edu.in [192.168.1.99]
  3     5 ms     4 ms     3 ms  103.25.231.1
  4     *        *        *     Request timed out.
  5     6 ms     7 ms     8 ms  10.119.234.162
  6     6 ms     6 ms     6 ms  72.14.195.56
  7    32 ms    48 ms    28 ms  192.178.80.159
  8    30 ms    31 ms    29 ms  142.251.54.87
  9    45 ms    28 ms    41 ms  del11s14-in-f4.1e100.net [142.250.193.4]
```

The IP Addresses of the intermediate hosts are as follows:

1. IP Address: 192.168.32.254
   Average Latency: 65.6 ms
2. IP Address: 192.168.1.99
   Average Latency: 5.3 ms
3. IP Address: 103.25.231.1
   Average Latency: 4 ms
4. Timed out
5. IP Address: 10.119.234.162
   Average Latency: 7 ms
6. IP Address: 72.14.195.56
   Average Latency: 6 ms
7. IP Address: 192.178.80.159
   Average Latency: 36 ms
8. IP Address: 142.251.54.87
   Average Latency: 30 ms
9. IP Address: 142.250.193.4
   Average Latency: 38 ms

b)

```
PS C:\Users\mriga> ping google.in -n 50

Pinging google.in [142.250.193.4] with 32 bytes of data:
Reply from 142.250.193.4: bytes=32 time=30ms TTL=56
Reply from 142.250.193.4: bytes=32 time=45ms TTL=56
Reply from 142.250.193.4: bytes=32 time=37ms TTL=56
Reply from 142.250.193.4: bytes=32 time=39ms TTL=56
Reply from 142.250.193.4: bytes=32 time=30ms TTL=56
Reply from 142.250.193.4: bytes=32 time=29ms TTL=56
Reply from 142.250.193.4: bytes=32 time=29ms TTL=56
Reply from 142.250.193.4: bytes=32 time=29ms TTL=56
Reply from 142.250.193.4: bytes=32 time=30ms TTL=56
Reply from 142.250.193.4: bytes=32 time=31ms TTL=56
Reply from 142.250.193.4: bytes=32 time=30ms TTL=56
Reply from 142.250.193.4: bytes=32 time=30ms TTL=56
Reply from 142.250.193.4: bytes=32 time=29ms TTL=56
Reply from 142.250.193.4: bytes=32 time=63ms TTL=56
Reply from 142.250.193.4: bytes=32 time=29ms TTL=56
Reply from 142.250.193.4: bytes=32 time=40ms TTL=56
Reply from 142.250.193.4: bytes=32 time=29ms TTL=56
Reply from 142.250.193.4: bytes=32 time=32ms TTL=56
Reply from 142.250.193.4: bytes=32 time=31ms TTL=56
Reply from 142.250.193.4: bytes=32 time=41ms TTL=56
Reply from 142.250.193.4: bytes=32 time=37ms TTL=56
Reply from 142.250.193.4: bytes=32 time=56ms TTL=56
Reply from 142.250.193.4: bytes=32 time=27ms TTL=56
Reply from 142.250.193.4: bytes=32 time=31ms TTL=56
Reply from 142.250.193.4: bytes=32 time=27ms TTL=56
Reply from 142.250.193.4: bytes=32 time=59ms TTL=56
Reply from 142.250.193.4: bytes=32 time=70ms TTL=56
Reply from 142.250.193.4: bytes=32 time=68ms TTL=56
Reply from 142.250.193.4: bytes=32 time=31ms TTL=56
Reply from 142.250.193.4: bytes=32 time=28ms TTL=56
```

```
Reply from 142.250.193.4: bytes=32 time=27ms TTL=56
Reply from 142.250.193.4: bytes=32 time=31ms TTL=56
Reply from 142.250.193.4: bytes=32 time=27ms TTL=56
Reply from 142.250.193.4: bytes=32 time=59ms TTL=56
Reply from 142.250.193.4: bytes=32 time=70ms TTL=56
Reply from 142.250.193.4: bytes=32 time=68ms TTL=56
Reply from 142.250.193.4: bytes=32 time=31ms TTL=56
Reply from 142.250.193.4: bytes=32 time=28ms TTL=56
Reply from 142.250.193.4: bytes=32 time=67ms TTL=56
Reply from 142.250.193.4: bytes=32 time=76ms TTL=56
Reply from 142.250.193.4: bytes=32 time=68ms TTL=56
Reply from 142.250.193.4: bytes=32 time=30ms TTL=56
Reply from 142.250.193.4: bytes=32 time=39ms TTL=56
Reply from 142.250.193.4: bytes=32 time=31ms TTL=56
Reply from 142.250.193.4: bytes=32 time=58ms TTL=56
Reply from 142.250.193.4: bytes=32 time=73ms TTL=56
Reply from 142.250.193.4: bytes=32 time=52ms TTL=56
Reply from 142.250.193.4: bytes=32 time=27ms TTL=56
Reply from 142.250.193.4: bytes=32 time=28ms TTL=56
Reply from 142.250.193.4: bytes=32 time=42ms TTL=56
Reply from 142.250.193.4: bytes=32 time=44ms TTL=56
Reply from 142.250.193.4: bytes=32 time=30ms TTL=56
Reply from 142.250.193.4: bytes=32 time=63ms TTL=56
Reply from 142.250.193.4: bytes=32 time=28ms TTL=56
Reply from 142.250.193.4: bytes=32 time=28ms TTL=56
Reply from 142.250.193.4: bytes=32 time=29ms TTL=56
Reply from 142.250.193.4: bytes=32 time=43ms TTL=56
Reply from 142.250.193.4: bytes=32 time=30ms TTL=56

Ping statistics for 142.250.193.4:
    Packets: Sent = 50, Received = 50, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 27ms, Maximum = 76ms, Average = 40ms
```

Average Latency: 40 ms

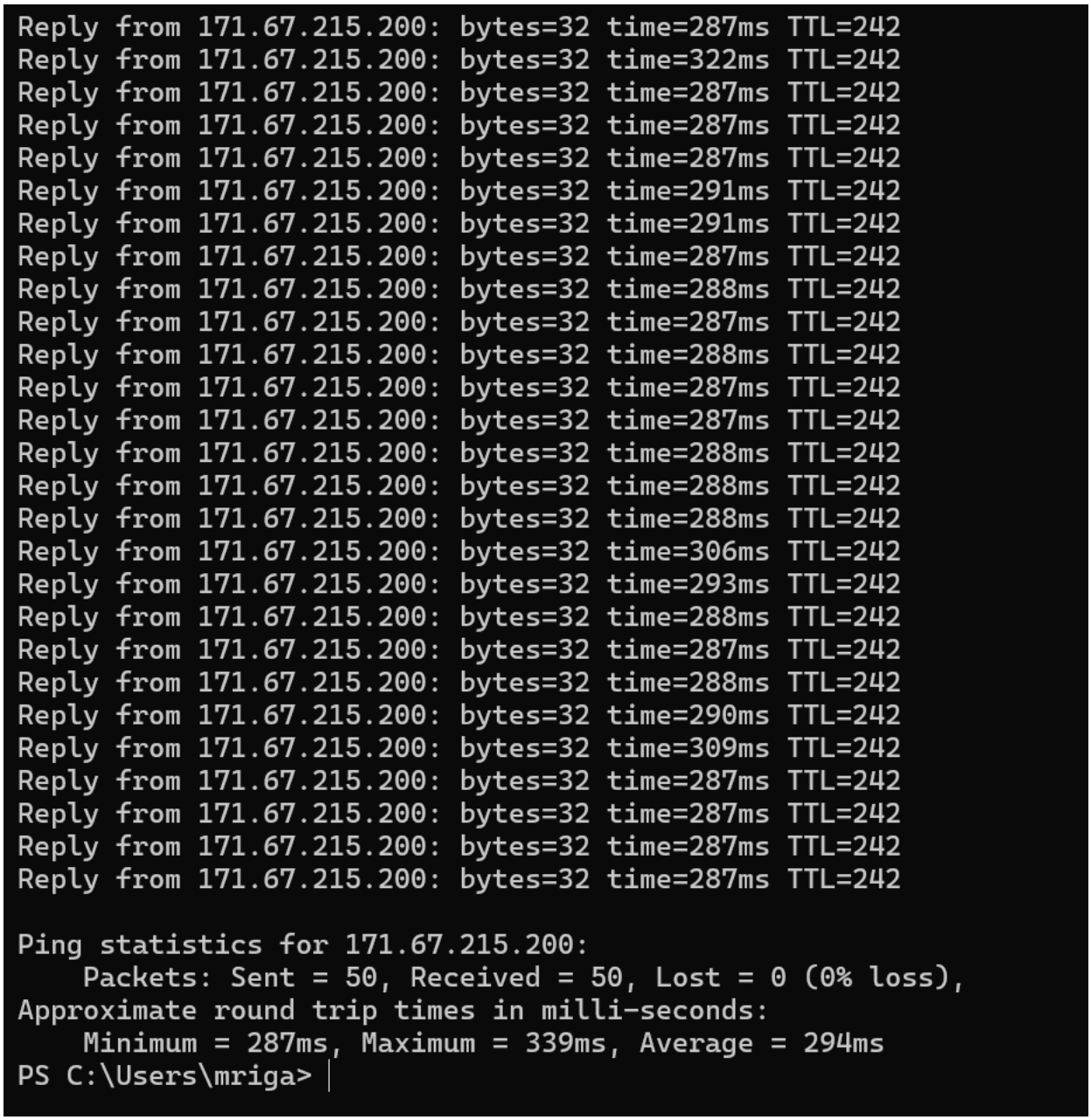
c) The total ping latency over all the intermediate hosts obtained in a) is 191.9 ms which is much higher than the average latency of 40 ms for the ping command.
In general, the latency of the ping command is lower than the traceroute (or tracert) command as the ping only measures the time from the destination and back. On the other hand, the traceroute command measures the latency to each hop separately. Each of these hops involve different routers which may induce additional latency which is not present in the ping command.

d) The maximum latency amongst the intermediate hosts was 65.6 ms which is higher than the average latency of 40 ms for the ping command. This is because the maximum latency amongst the intermediate host for the traceroute command can appear to be inflated because of congestion on a particular intermediate host whereas the average latency of the ping command is calculated over multiple packets and thus is less affected by the impact of a particularly slow hop.

e) If there are multiple entries for a single hop while using the traceroute command, it means that there are multiple paths to reach the destination host. These multiple entries imply that packets can take different routes through the network even when targeting the same hop.

f)

```
PS C:\Users\mriga> ping stanford.edu -n 50

Pinging stanford.edu [171.67.215.200] with 32 bytes of data:
Reply from 171.67.215.200: bytes=32 time=287ms TTL=242
Reply from 171.67.215.200: bytes=32 time=287ms TTL=242
Reply from 171.67.215.200: bytes=32 time=288ms TTL=242
Reply from 171.67.215.200: bytes=32 time=287ms TTL=242
Reply from 171.67.215.200: bytes=32 time=303ms TTL=242
Reply from 171.67.215.200: bytes=32 time=304ms TTL=242
Reply from 171.67.215.200: bytes=32 time=291ms TTL=242
Reply from 171.67.215.200: bytes=32 time=300ms TTL=242
Reply from 171.67.215.200: bytes=32 time=288ms TTL=242
Reply from 171.67.215.200: bytes=32 time=287ms TTL=242
Reply from 171.67.215.200: bytes=32 time=287ms TTL=242
Reply from 171.67.215.200: bytes=32 time=295ms TTL=242
Reply from 171.67.215.200: bytes=32 time=309ms TTL=242
Reply from 171.67.215.200: bytes=32 time=339ms TTL=242
Reply from 171.67.215.200: bytes=32 time=301ms TTL=242
Reply from 171.67.215.200: bytes=32 time=317ms TTL=242
Reply from 171.67.215.200: bytes=32 time=325ms TTL=242
Reply from 171.67.215.200: bytes=32 time=296ms TTL=242
Reply from 171.67.215.200: bytes=32 time=325ms TTL=242
Reply from 171.67.215.200: bytes=32 time=287ms TTL=242
Reply from 171.67.215.200: bytes=32 time=287ms TTL=242
Reply from 171.67.215.200: bytes=32 time=287ms TTL=242
Reply from 171.67.215.200: bytes=32 time=289ms TTL=242
Reply from 171.67.215.200: bytes=32 time=287ms TTL=242
Reply from 171.67.215.200: bytes=32 time=322ms TTL=242
Reply from 171.67.215.200: bytes=32 time=287ms TTL=242
Reply from 171.67.215.200: bytes=32 time=287ms TTL=242
Reply from 171.67.215.200: bytes=32 time=287ms TTL=242
Reply from 171.67.215.200: bytes=32 time=291ms TTL=242
Reply from 171.67.215.200: bytes=32 time=291ms TTL=242
```



Average Latency: 294 ms

g)

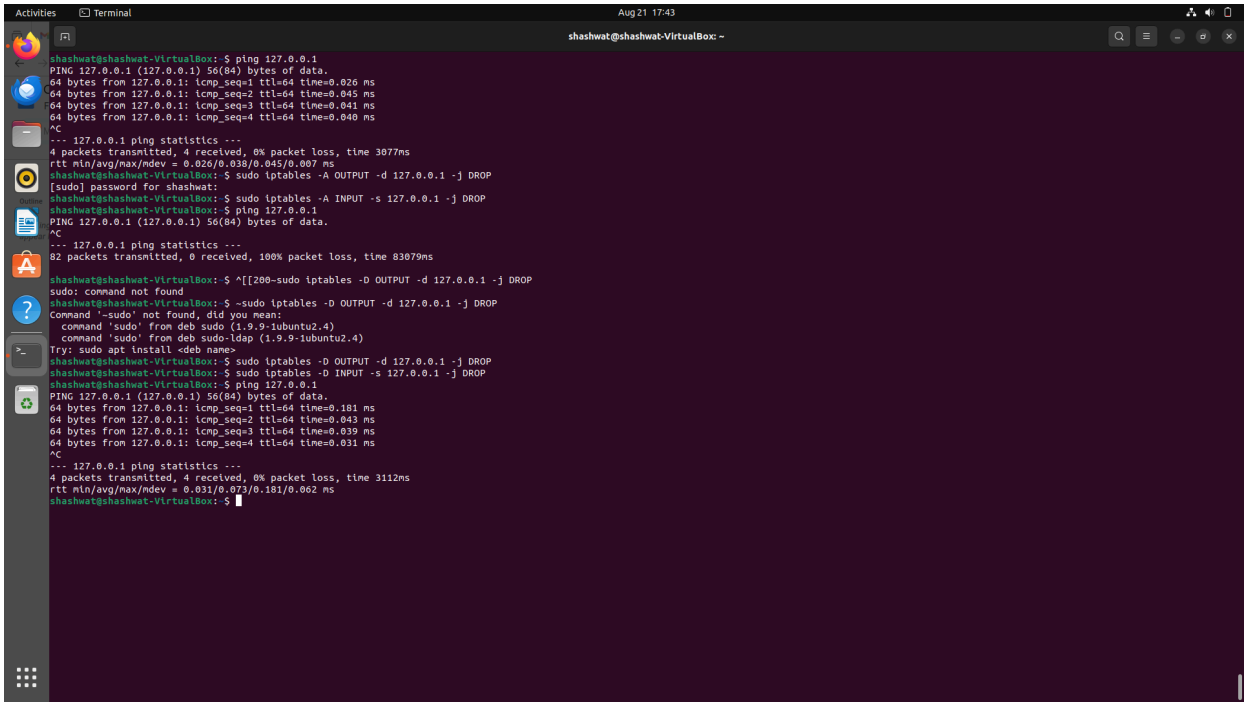
```
PS C:\Users\mriga> tracert stanford.edu

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

  1    22 ms    38 ms   102 ms  192.168.32.254
  2     2 ms     3 ms     2 ms  vpn.iiitd.edu.in [192.168.1.99]
  3     3 ms     5 ms     3 ms  103.25.231.1
  4    29 ms    29 ms    29 ms  10.1.209.201
  5    60 ms    34 ms    35 ms  10.1.200.137
  6    43 ms    47 ms    68 ms  10.255.238.254
  7    29 ms    27 ms    28 ms  180.149.48.18
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24   287 ms   286 ms   287 ms  campus-nw-rtr-vl1004.SUNet [171.64.255.200]
 25     *        *        *     Request timed out.
 26   287 ms   288 ms   287 ms  web.stanford.edu [171.67.215.200]

Trace complete.
```

The number of hops for stanford.edu is 26 which is higher than the 9 hops for google.in.

h) The average latency for stanford.edu is much higher than the average latency for google.in. This could be due to a variety of factors such as :

1) Geographical location: The physical distance between us and the google servers present in India is much lesser than the physical distance between us and the stanford servers present in USA.
2) Number of Hops: More intermediate hops generally results in a higher latency as a larger number of hops means more time for the data to be processed and forwarded.

6.



I have used ‘iptables’ to block traffic coming to and from ‘127.0.0.1’.
Firstly, I have shown that the ping command was working properly initially.
Then I used ‘sudo iptables -A OUTPUT -d 127.0.0.1 -j DROP’ and ‘sudo iptables -A INPUT -s 127.0.0.1 -j DROP’ commands to drop the outgoing and ingoing packets coming to and from 127.0.0.1.
After this, the ping command fails with 100% packet loss.
In the end, I restore the normal functionality and show that the ping command is working again.