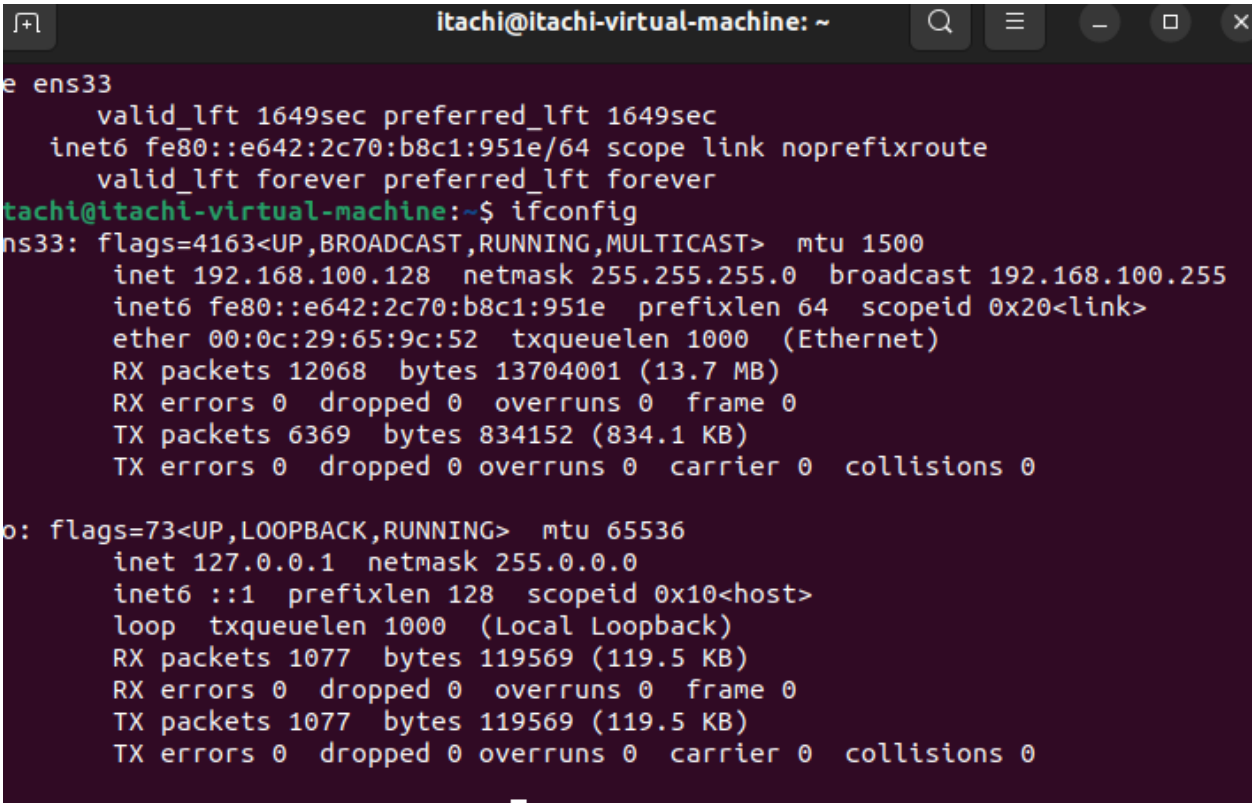
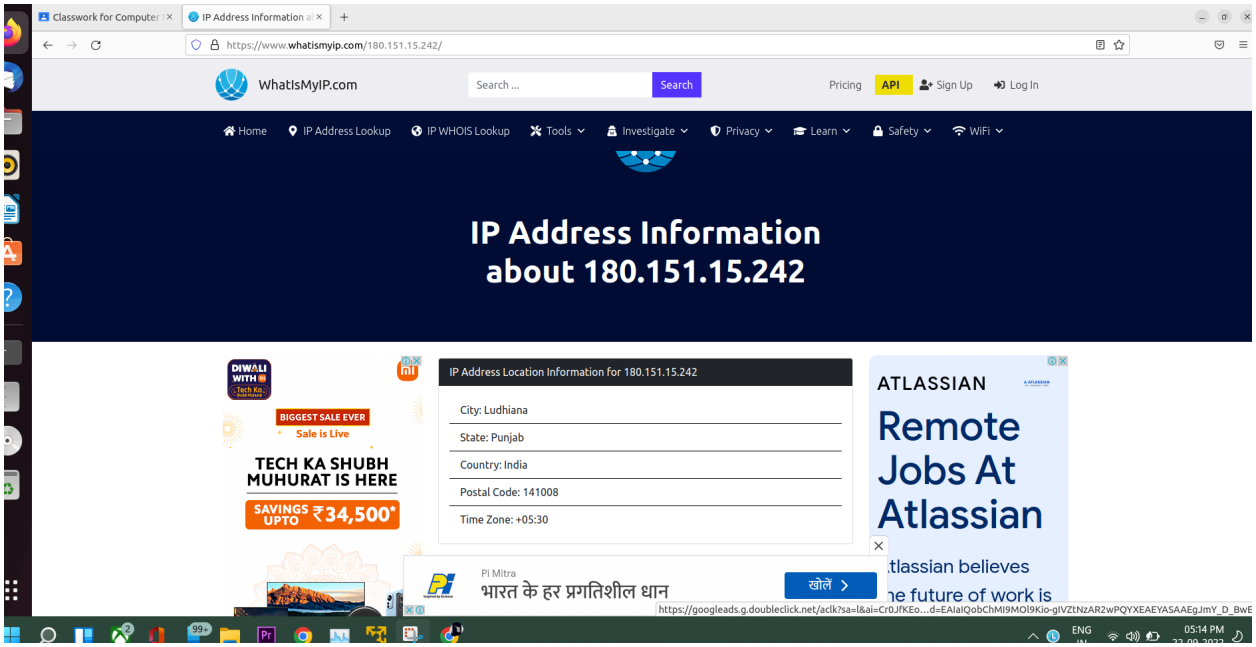
Name :Dheeraj, Roll_no: 2020194, Assignment-1



Q1) a) My network Ip address is 192.168.198.100.128 for Ubuntu



Q1)B)

whatismyip.org is showing the address that our ISP has provided to us, and config is showing us our local Ip

Q2)

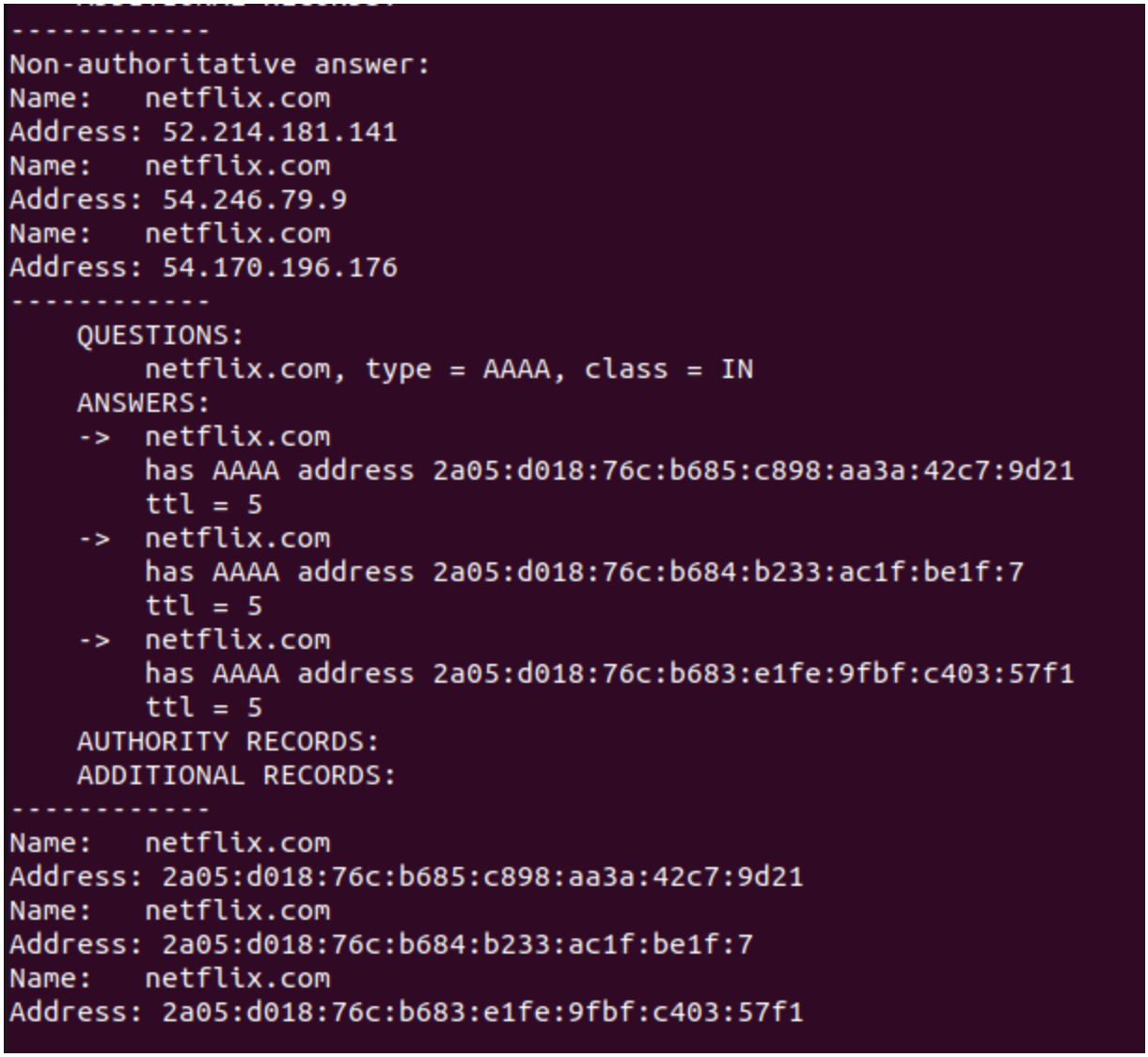
```
itachi@itachi-virtual-machine:~$ sudo nslookup -type=soa netflix.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
netflix.com
        origin = ns-81.awsdns-10.com
        mail addr = awsdns-hostmaster.amazon.com
        serial = 1
        refresh = 7200
        retry = 900
        expire = 1209600
        minimum = 1800

Authoritative answers can be found from:
ns-81.awsdns-10.com     internet address = 205.251.192.81
ns-81.awsdns-10.com     has AAAA address 2600:9000:5300:5100::1
```

```
itachi@itachi-virtual-machine:~$ sudo nslookup netflix.com ns-81.awsdns-10.com
Server:         ns-81.awsdns-10.com
Address:        205.251.192.81#53

Name:   netflix.com
Address: 54.155.178.5
Name:   netflix.com
Address: 3.251.50.149
Name:   netflix.com
Address: 54.74.73.31
Name:   netflix.com
Address: 2a05:d018:76c:b683:f711:f0cf:5cc7:b815
Name:   netflix.com
Address: 2a05:d018:76c:b685:3b38:679d:2640:1ced
Name:   netflix.com
Address: 2a05:d018:76c:b684:8e48:47c9:84aa:b34d
```

A)When we use command ” sudo nslookup -type=soa” we get the actual server name, and then we use that actual server name to get the authorial address which is”ns-81.awsdns-10.com”
Command “sudo nslookup netflix.com ns-81.awsdns-10.com ”

Q2)B)

```
itachi@itachi-virtual-machine:~$ nslookup -debug netflix.com
Server:         127.0.0.53
Address:        127.0.0.53#53

------------
    QUESTIONS:
        netflix.com, type = A, class = IN
    ANSWERS:
    ->  netflix.com
        internet address = 52.214.181.141
        ttl = 5
    ->  netflix.com
        internet address = 54.246.79.9
        ttl = 5
    ->  netflix.com
        internet address = 54.170.196.176
        ttl = 5
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
```



command:”nslookup -debug netflix.com”
Time to live for Ipv4 address(type = A): 5 sec
Time to live for Ipv6 address(type =AAAA): 5sec
The Ipv4 and Ipv6 expire in 5 secons, packets are loaded into the cache and expired after time to live

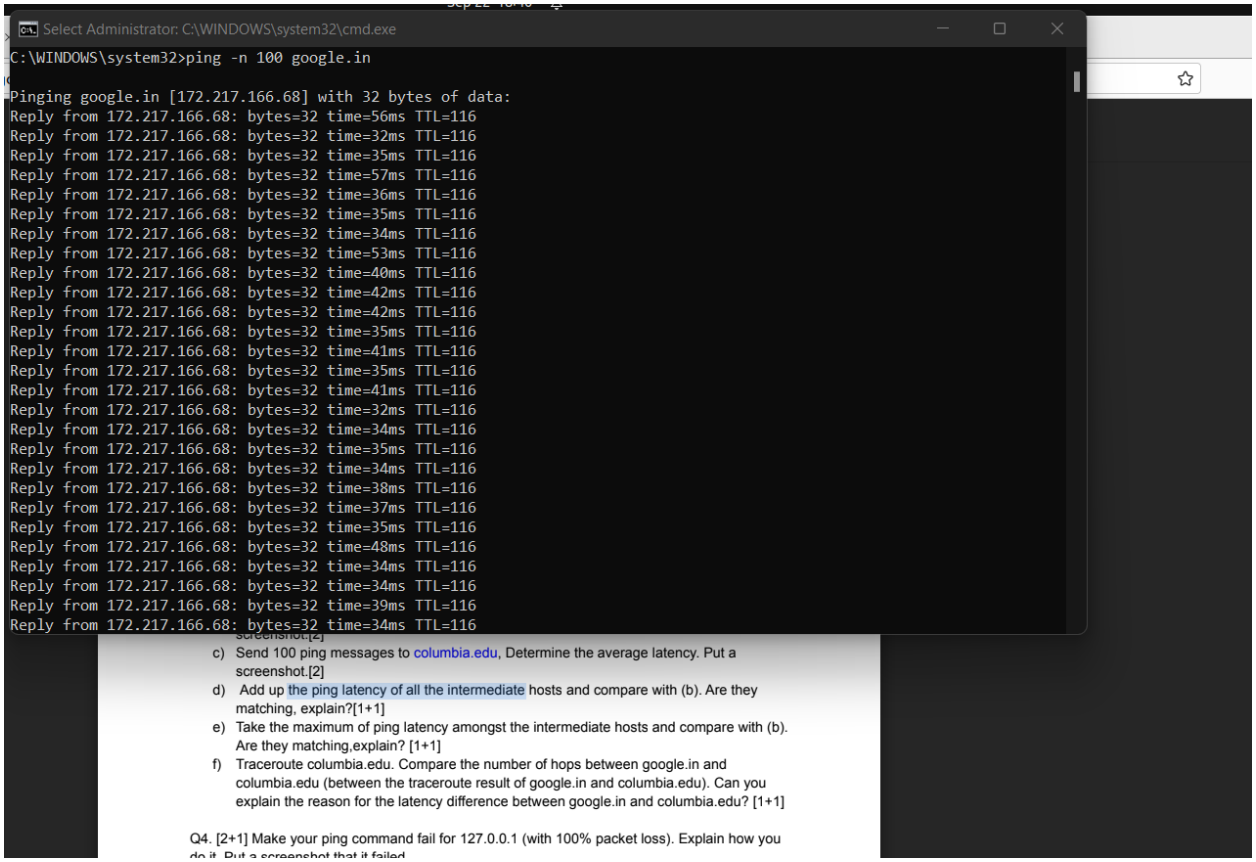
Q3

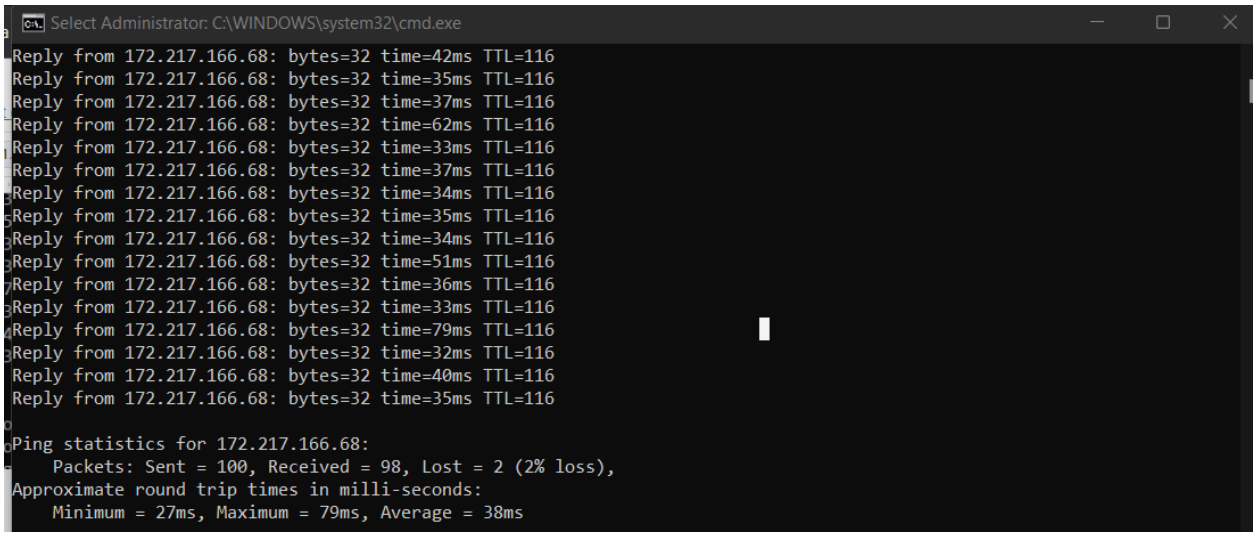
```
C:\Users\DHEERAJ> tracert google.in

Tracing route to google.in [216.58.221.36]
over a maximum of 30 hops:

  1     5 ms    10 ms     5 ms  192.168.48.254
  2    52 ms    44 ms    10 ms  auth.iiitd.edu.in [192.168.1.99]
  3    37 ms    22 ms     6 ms  180.151.15.241.reverse.spectranet.in [180.151.15.241]
  4    18 ms     5 ms     6 ms  72.14.194.202
  5     7 ms     6 ms    10 ms  108.170.251.97
  6    19 ms    12 ms     6 ms  216.239.57.33
  7    13 ms     6 ms    17 ms  del03s07-in-f4.1e100.net [216.58.221.36]

Trace complete.
```

After putting tracert google.in we get all the path router's ip address which connect us to the google.com

S.no	Latency	avg(ms)	path
1	5ms+10ms+5ms	16.7	192.168.48.254
2	52ms+44ms+10ms	35.3	auth.iiitd.edu.in
3	37ms+22ms+6ms	21.6	180.151.15.241.reverse.spectranet.in
4	18ms+5ms+6ms	9.6	72.14.194.202
5	7ms+6ms+10ms	7.6	108.170.251.97
6	19ms+12ms+6ms	12.3	216.239.57.33
7	13ms+6ms+17ms	12	del03s07-in-f4.1e100.net

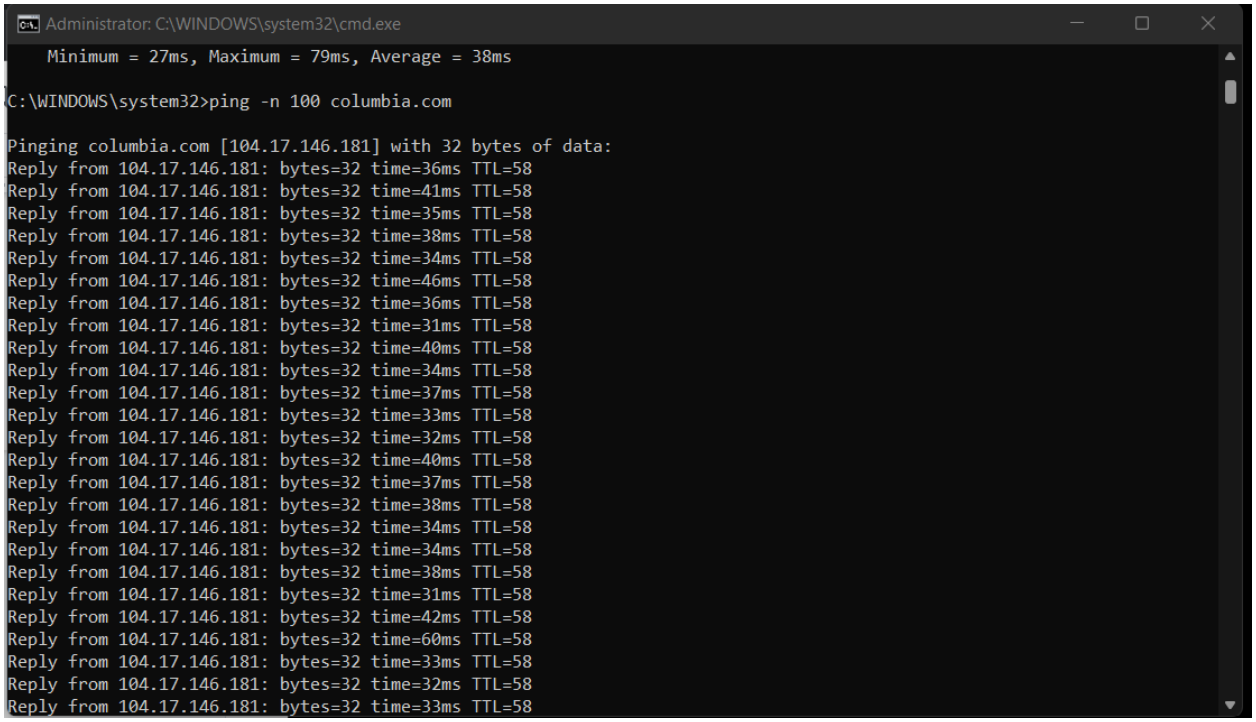
B)

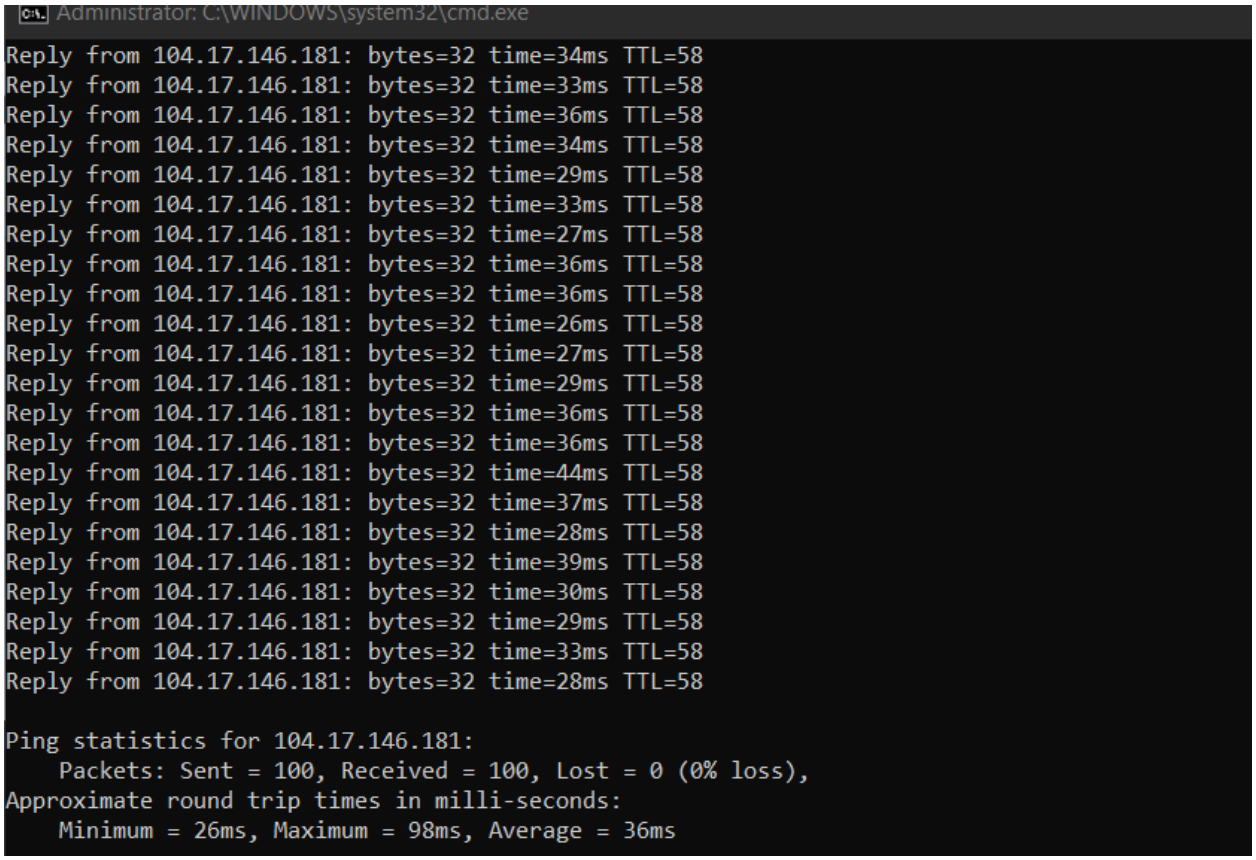




Avg latency: 38ms

C)





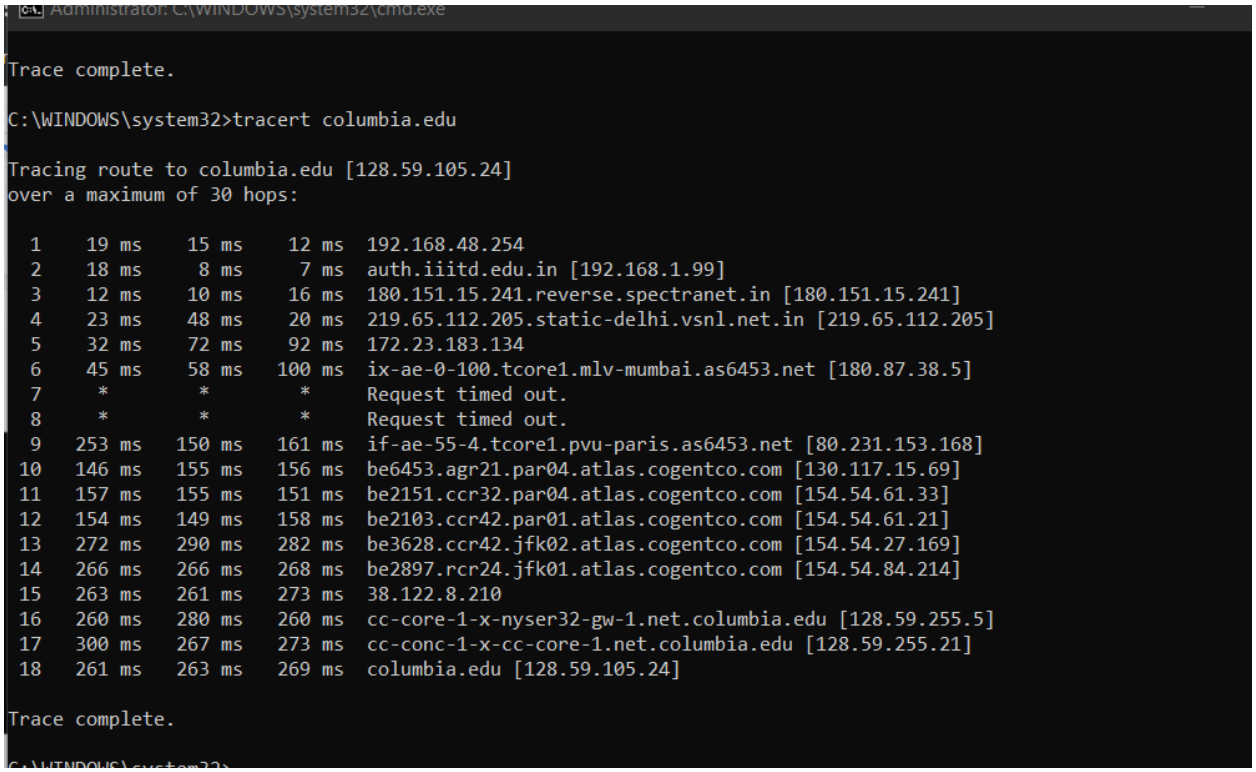
Avg = 36ms

d) sum = 115.1

No, they don't match because traceroute involves sending UDP packets to each node along the way and waiting for its timeout response (then moving on to the next node), whereas a ping is just given the time taken from the computer to that particular router

E) max =35.3 and avg latency (ping) 38ms
Yes they are nearly equal because ping command given the time taken to the destination, on the other hand, Traceroute give time taken for the packet to travel till the individual routers on the way so avg time of ping and max time of traceroute always will be nearly equal

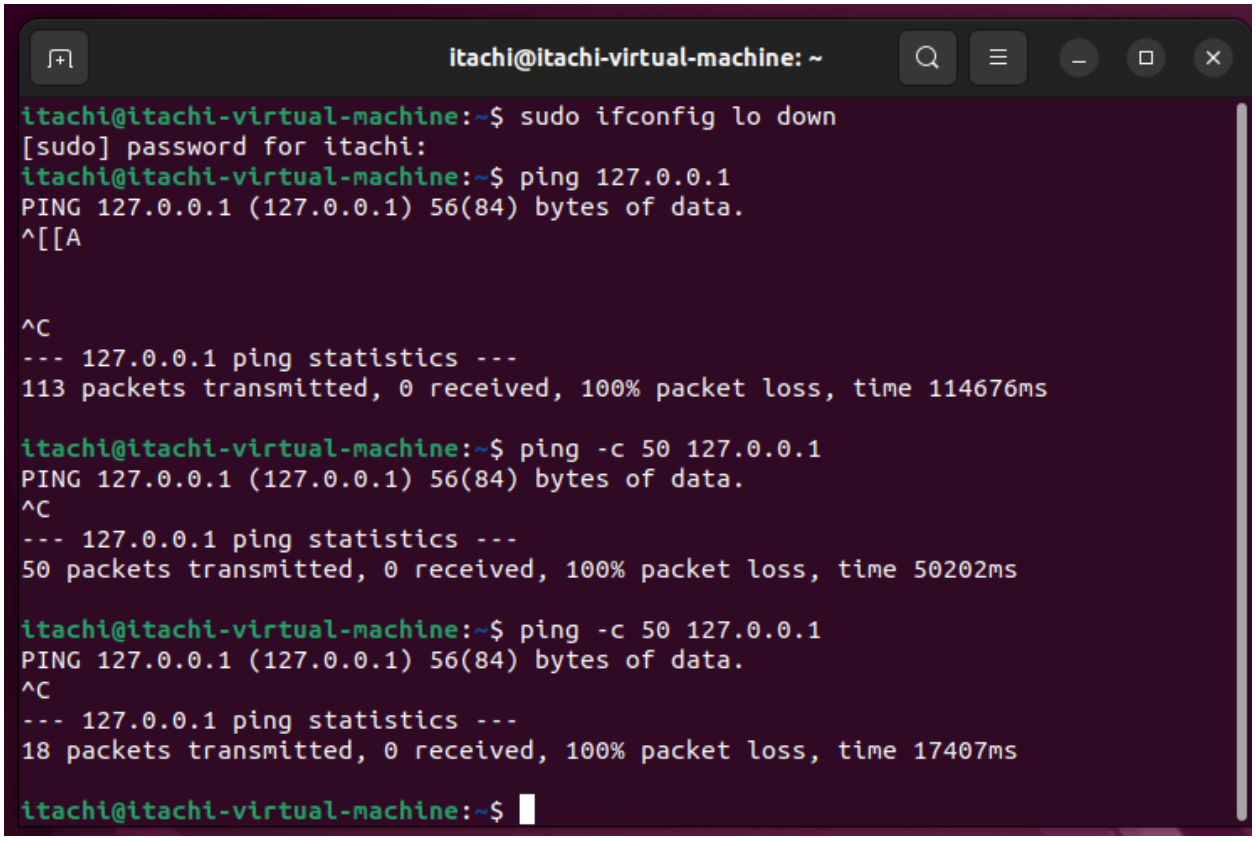
F)



```
C:\WINDOWS\system32>tracert google.in

Tracing route to google.in [142.250.67.196]
over a maximum of 30 hops:

  1    10 ms    10 ms    18 ms  192.168.48.254
  2    12 ms     9 ms     5 ms  auth.iiitd.edu.in [192.168.1.99]
  3    10 ms     6 ms     8 ms  180.151.15.241.reverse.spectranet.in [180.151.15.241]
  4    21 ms    14 ms    11 ms  72.14.194.202
  5    20 ms    10 ms    13 ms  108.170.251.108
  6    29 ms     5 ms    39 ms  72.14.233.107
  7    41 ms    29 ms    37 ms  72.14.232.138
  8    27 ms    26 ms    41 ms  108.170.248.177
  9    60 ms    36 ms    26 ms  142.250.235.11
 10    42 ms    40 ms    30 ms  bom12s08-in-f4.1e100.net [142.250.67.196]

Trace complete.
```

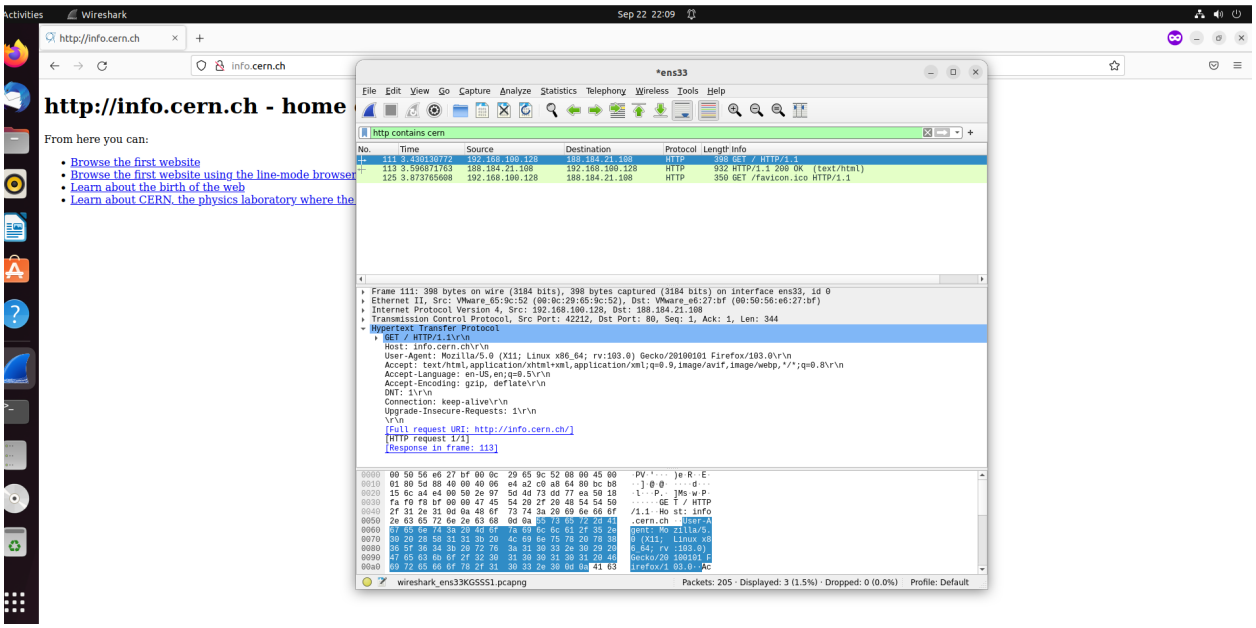
No. of hope for google: 10
No. of hope for Columbia:18
Latency difference between google and Columbia because Google is a large service provider and have many servers set up around the world, so path taken to google.in must always be smaller than Columbia.edu, which has fewer servers around the world; hence the latency of google. in is smaller than Columbia.edu

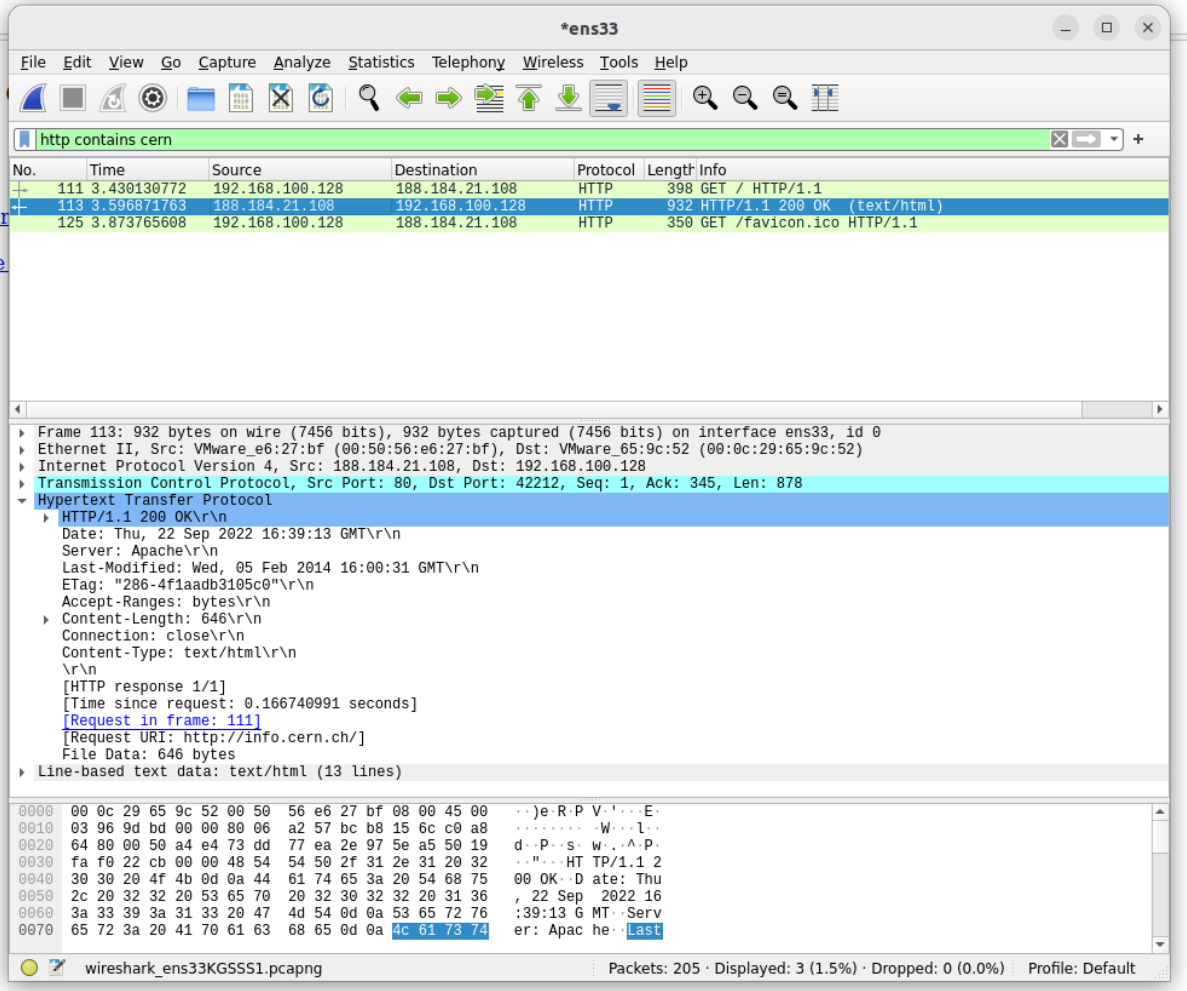
Q4)

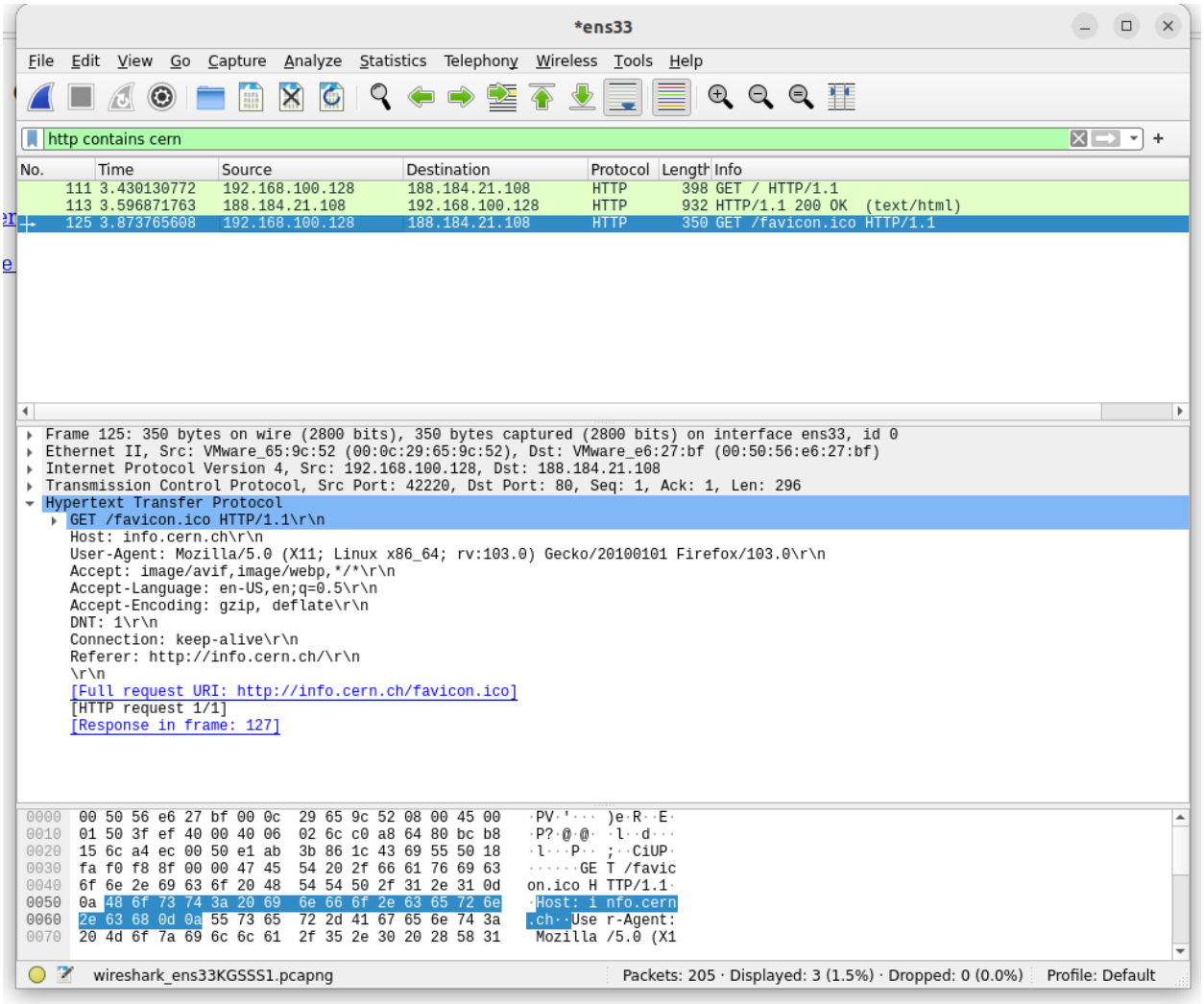


If we type the command sudo ifconfig lo down it will make localhost(127.0.01) down(that is causes the driver for the loopback interface to be shut down). When the ping command is run on 127.0.01 we don't get any response and ping command fails with 100% packet loss.

Q5)




*ens33
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http contains cern
No. Time Source Destination Protocol Length Info
111 3.430130772 192.168.100.128 188.184.21.108 HTTP 398 GET / HTTP/1.1
113 3.596871763 188.184.21.108 192.168.100.128 HTTP 932 HTTP/1.1 200 OK (text/html)
125 3.873765608 192.168.100.128 188.184.21.108 HTTP 350 GET /favicon.ico HTTP/1.1
Frame 113: 932 bytes on wire (7456 bits), 932 bytes captured (7456 bits) on interface ens33, id 0
Ethernet II, Src: VMware_e6:27:bf (00:50:56:e6:27:bf), Dst: VMware_65:9c:52 (00:0c:29:65:9c:52)
Internet Protocol Version 4, Src: 188.184.21.108, Dst: 192.168.100.128
Transmission Control Protocol, Src Port: 80, Dst Port: 42212, Seq: 1, Ack: 345, Len: 878
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Thu, 22 Sep 2022 16:39:13 GMT\r\n
Server: Apache\r\n
Last-Modified: Wed, 05 Feb 2014 16:00:31 GMT\r\n
ETag: "286-4f1aadb3105c0"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 646\r\n
Connection: close\r\n
Content-Type: text/html\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.166740991 seconds]
[Request in frame: 111]
[Request URI: http://info.cern.ch/]
File Data: 646 bytes
Line-based text data: text/html (13 lines)
0000 00 0c 29 65 9c 52 00 50 56 e6 27 bf 08 00 45 00
0010 03 96 9d bd 00 00 80 06 a2 57 bc b8 15 6c c0 a8
0020 64 80 00 50 a4 e4 73 dd 77 ea 2e 97 5e a5 50 19
0030 fa f0 22 cb 00 00 48 54 54 50 2f 31 2e 31 20 32
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 68 75
0050 2c 20 32 32 20 53 65 70 20 32 30 32 32 20 31 36
0060 3a 33 39 3a 31 33 20 47 4d 54 0d 0a 53 65 72 76
0070 65 72 3a 20 41 70 61 63 68 65 0d 0a 4c 61 73 74
wireshark_ens33KGSSS1.pcapng
Packets: 205 · Displayed: 3 (1.5%) · Dropped: 0 (0.0%)
Profile: Default



- **For HTTP request packets**

1) HTTP request type: HTTP/1.1
2) User agent type: Mozilla firefox
3) HTTP request packet's URL:http://info.cern.ch/

- **For HTTP response packets**

1) HTTP response code: 200 OK
2) HTTP response description: 200 OK which tell us successfully done
3)Name and version of the web server: Apache

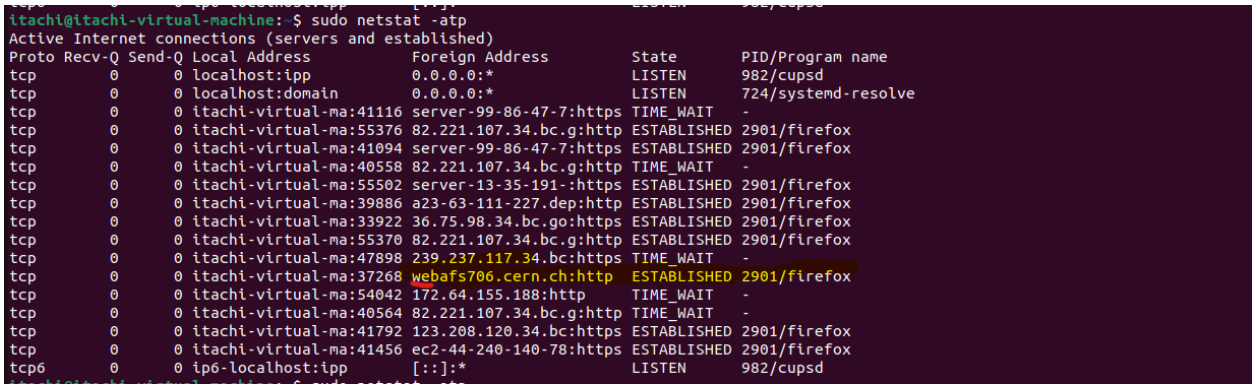
- There are 2 web objects downloaded which is the result of 2 GET requests(one which contains Html files/object, Second is image objects/files)
- AS we can see that the both have different destination port for the response of web objects and over the same TCP connection destination port can not be different hence both are on different TCP connection

- Hence this network is non-persistent

Q6) command to display all active tcp connections with pids:

a) Command : sudo netstat -atp
   PID for tcp connection is :2091/firefox

B) The state of the TCP connection to server is established



```
itachi@itachi-virtual-machine:~$ sudo netstat -atp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      982/cupsd
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      724/systemd-resolve
tcp        0      0 itachi-virtual-ma:41116 server-99-86-47-7:https TIME_WAIT   -
tcp        0      0 itachi-virtual-ma:55376 82.221.107.34.bc.g:http ESTABLISHED 2901/firefox
tcp        0      0 itachi-virtual-ma:41094 server-99-86-47-7:https ESTABLISHED 2901/firefox
tcp        0      0 itachi-virtual-ma:40558 82.221.107.34.bc.g:http TIME_WAIT   -
tcp        0      0 itachi-virtual-ma:55502 server-13-35-191-:https ESTABLISHED 2901/firefox
tcp        0      0 itachi-virtual-ma:39886 a23-63-111-227.dep:http ESTABLISHED 2901/firefox
tcp        0      0 itachi-virtual-ma:33922 36.75.98.34.bc.go:https ESTABLISHED 2901/firefox
tcp        0      0 itachi-virtual-ma:55370 82.221.107.34.bc.g:http ESTABLISHED 2901/firefox
tcp        0      0 itachi-virtual-ma:47898 239.237.117.34.bc:https TIME_WAIT   -
tcp        0      0 itachi-virtual-ma:37268 webafs706.cern.ch:http  ESTABLISHED 2901/firefox
tcp        0      0 itachi-virtual-ma:54042 172.64.155.188:http     TIME_WAIT   -
tcp        0      0 itachi-virtual-ma:40564 82.221.107.34.bc.g:http TIME_WAIT   -
tcp        0      0 itachi-virtual-ma:41792 123.208.120.34.bc:https ESTABLISHED 2901/firefox
tcp        0      0 itachi-virtual-ma:41456 ec2-44-240-140-78:https ESTABLISHED 2901/firefox
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN      982/cupsd
```