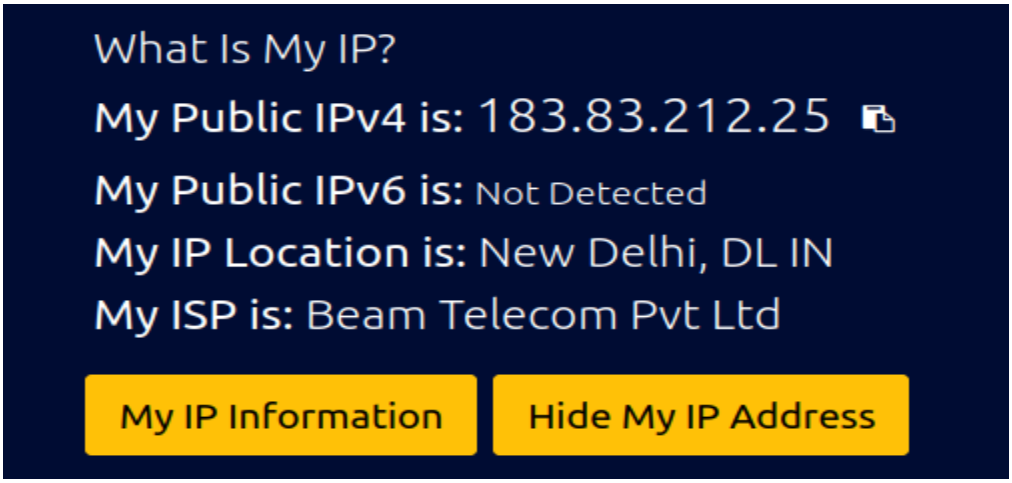
Assignment-1

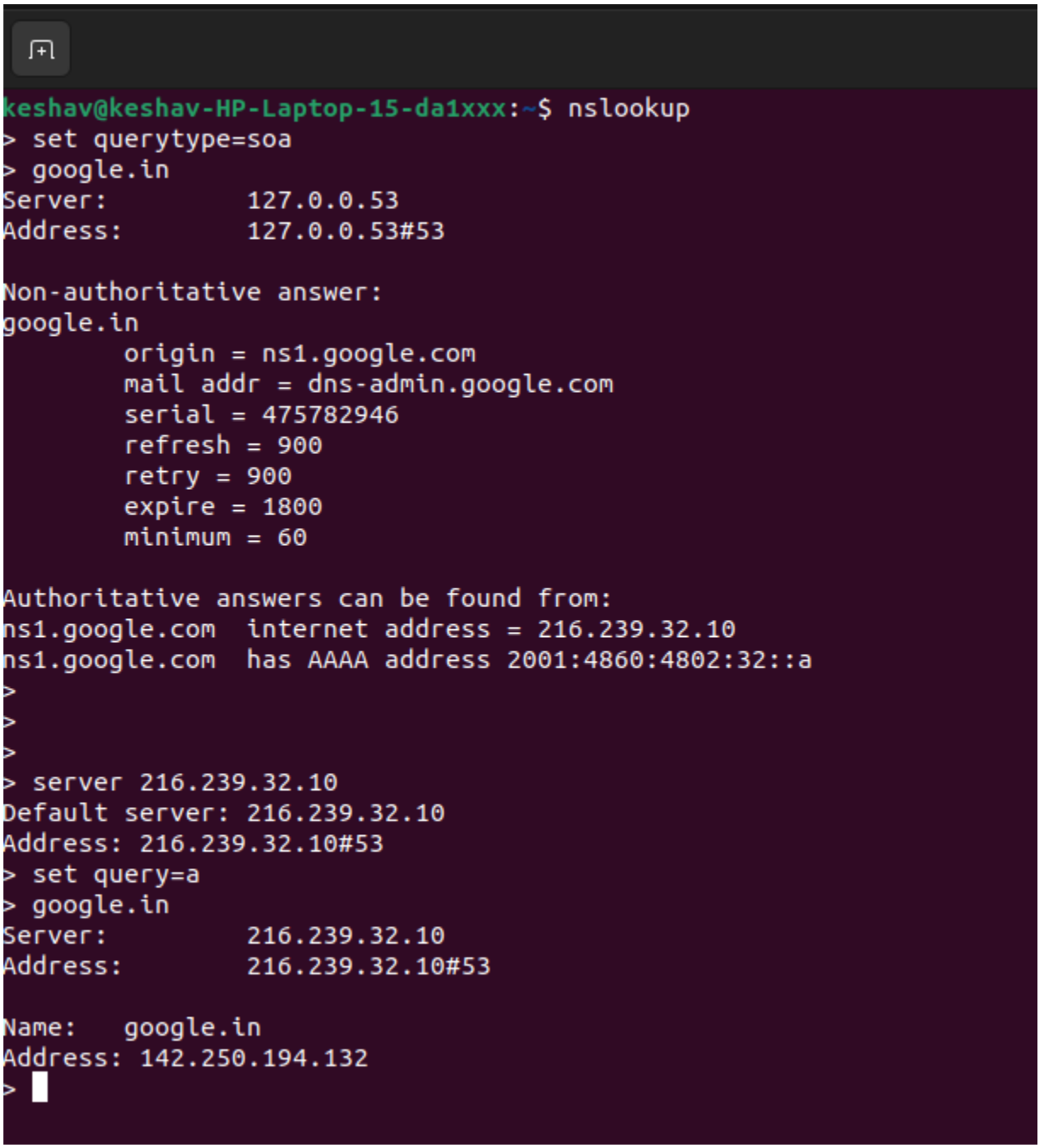
Question-1

```
keshav@keshav-HP-Laptop-15-da1xxx:~$ ifconfig
eno1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether f8:b4:6a:d1:30:0b  txqueuelen 1000  (Ethernet)
        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

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 95367  bytes 8879463 (8.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 95367  bytes 8879463 (8.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.114  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::73b0:e38f:1ce0:119e  prefixlen 64  scopeid 0x20<link>
        ether b0:68:e6:2a:fc:65  txqueuelen 1000  (Ethernet)
        RX packets 2705634  bytes 1585747044 (1.5 GB)
        RX errors 0  dropped 11  overruns 0  frame 0
        TX packets 463416  bytes 85205048 (85.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

keshav@keshav-HP-Laptop-15-da1xxx:~$
```

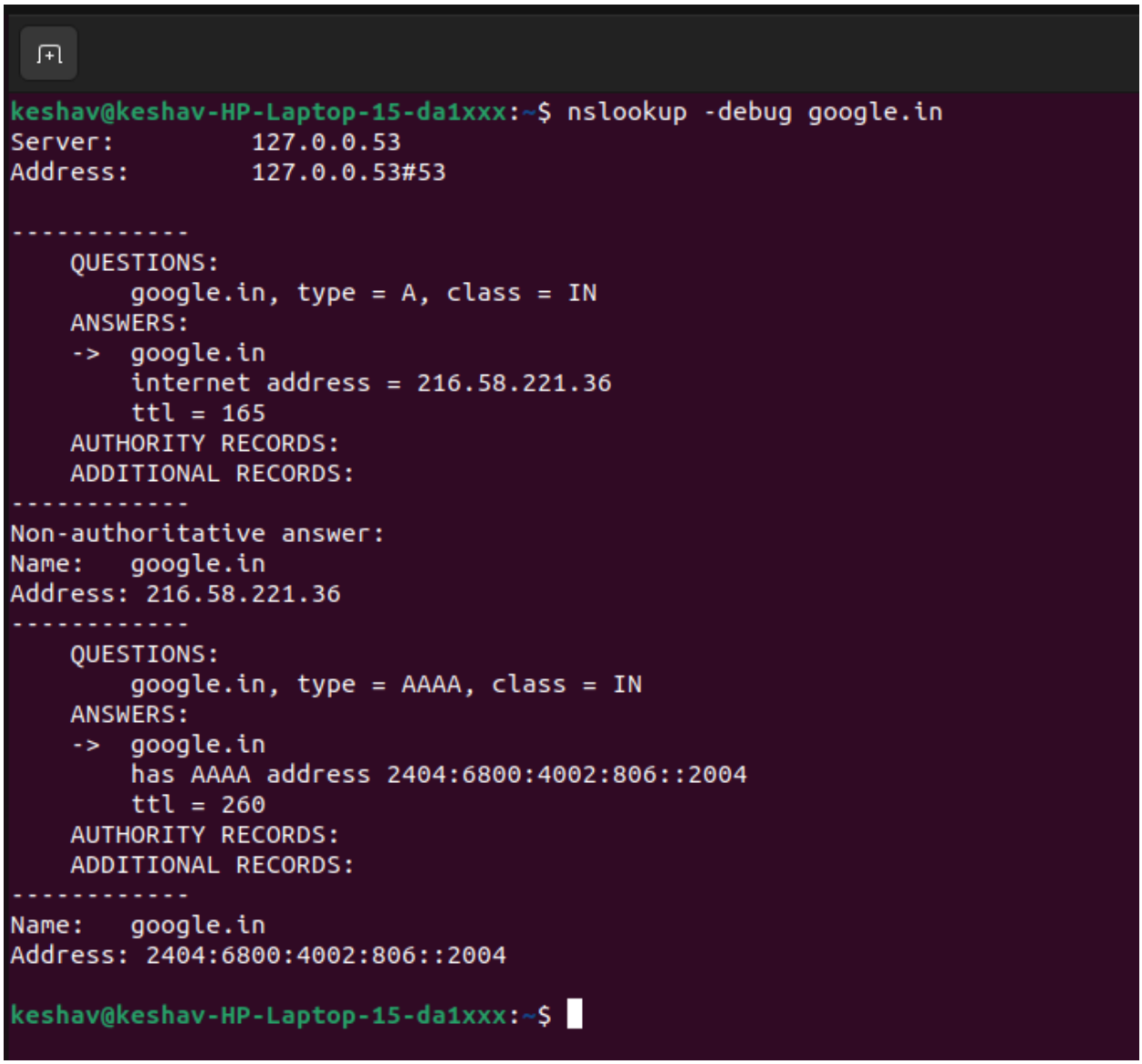


The IP address assigned to my system using ifconfig is **192.168.0.114** while the ip address found out using https://www.whatismyip.com/ is **183.83.212.25**. The 2 IPs don't match with each other. This is so because the ip address found using ifconfig command is the local ip address assigned by the router to my pc while the other ip address found using the website is the global ip address assigned to the router by the ISP. So the packet first reaches the router(global ip) and then it is forwarded to my machine by the router using the MAC address of my machine.

Question-2



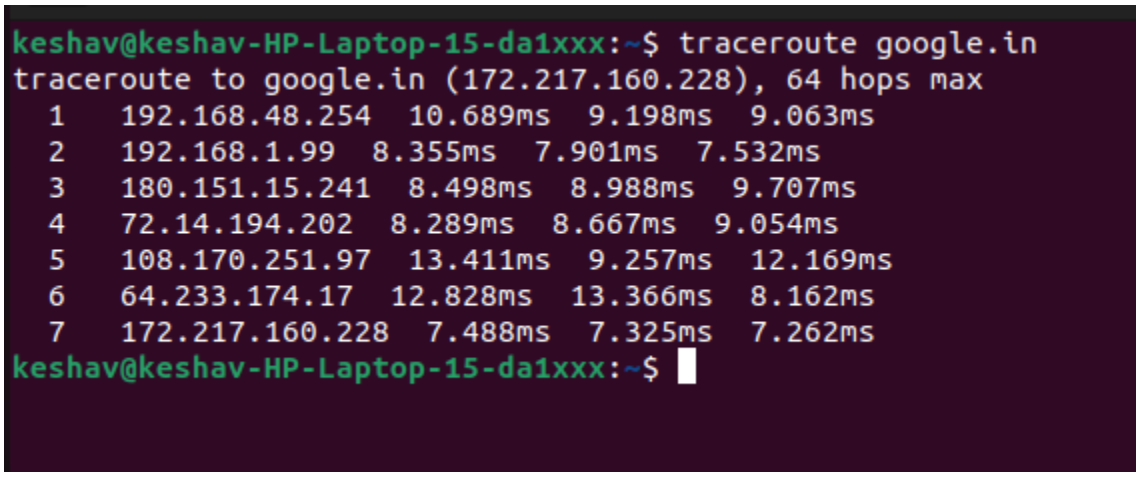
First we set the querytype to soa to get the name server for getting the ip address for authoritative answer. In this the google name server is at the **ip address 216.239.32.10**. Then I set up the server to the found nameserver. Finally I set query=a to get the authoritative answer and then again looked up nslookup.



Time to live on local DNS = 260
The entry would expire after 260 sec. TTL is measured in seconds and defines after how much time will the packet die.

Question-3

a.



Hop	Hop IP	Time1 (ms)	Time2 (ms)	Time3 (ms)	Average RTT (ms)	Average Latency
1	192.168.48.254	10.689	9.198	9.063	9.65	4.825
2	192.168.1.99	8.355	7.901	7.532	7.929333333	3.964666667
3	180.151.15.241	8.498	8.988	9.707	9.064333333	4.532166667
4	72.14.194.202	8.289	8.667	9.045	8.667	4.3335
5	108.170.251.97	13.411	9.257	12.169	11.61233333	5.806166667
6	64.233.174.17	12.828	13.366	8.162	11.452	5.726
7	172.217.160.228	7.488	7.325	7.262	7.358333333	3.679166667

Sum of average latencies of all intermediate host is: 32.86666667 ms

Maximum latency between all intermediate hosts are: 5.806166667 ms

b.

```
keshav@keshav-HP-Laptop-15-da1xxx:~$ ping -c 100 google.in
PING google.in (172.217.160.228) 56(84) bytes of data.
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=1 ttl=118 time=8.82 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=2 ttl=118 time=7.76 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=3 ttl=118 time=12.0 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=4 ttl=118 time=12.7 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=5 ttl=118 time=7.25 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=6 ttl=118 time=7.84 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=7 ttl=118 time=7.15 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=8 ttl=118 time=12.5 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=9 ttl=118 time=27.2 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=10 ttl=118 time=5.17 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=11 ttl=118 time=7.21 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=12 ttl=118 time=7.28 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=13 ttl=118 time=11.8 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=14 ttl=118 time=8.70 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=15 ttl=118 time=7.94 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=16 ttl=118 time=4.24 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=17 ttl=118 time=5.26 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=18 ttl=118 time=23.4 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=19 ttl=118 time=8.44 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=20 ttl=118 time=6.54 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=21 ttl=118 time=15.1 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=22 ttl=118 time=11.2 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=23 ttl=118 time=8.62 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=24 ttl=118 time=6.70 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=25 ttl=118 time=9.71 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=26 ttl=118 time=9.72 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=27 ttl=118 time=14.3 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=28 ttl=118 time=8.06 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=29 ttl=118 time=6.79 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=30 ttl=118 time=8.47 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=31 ttl=118 time=7.48 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=32 ttl=118 time=8.92 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=33 ttl=118 time=7.36 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=34 ttl=118 time=28.2 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=35 ttl=118 time=6.76 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=36 ttl=118 time=21.3 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=37 ttl=118 time=9.45 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=38 ttl=118 time=8.51 ms
```

```
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=86 ttl=118 time=7.05 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=87 ttl=118 time=13.5 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=88 ttl=118 time=7.92 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=89 ttl=118 time=6.66 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=90 ttl=118 time=8.01 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=91 ttl=118 time=21.9 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=92 ttl=118 time=36.4 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=93 ttl=118 time=7.31 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=94 ttl=118 time=5.89 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=95 ttl=118 time=12.4 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=96 ttl=118 time=6.27 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=97 ttl=118 time=6.83 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=98 ttl=118 time=21.6 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=99 ttl=118 time=57.0 ms
64 bytes from del03s09-in-f4.1e100.net (172.217.160.228): icmp_seq=100 ttl=118 time=7.02 ms

--- google.in ping statistics ---
100 packets transmitted, 99 received, 1% packet loss, time 99172ms
rtt min/avg/max/mdev = 3.789/15.521/191.022/25.672 ms
keshav@keshav-HP-Laptop-15-da1xxx:~$
```

Average Ping Latency = 15.521/2 = 7.7605

c.

```
keshav@keshav-HP-Laptop-15-da1xxx:~$ ping -c 100 columbia.edu
PING columbia.edu (128.59.105.24) 56(84) bytes of data.
64 bytes from columbiauniversity.net (128.59.105.24): icmp_seq=1 ttl=233 time=306 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=2 ttl=233 time=331 ms
64 bytes from childpolicy.org (128.59.105.24): icmp_seq=3 ttl=233 time=251 ms
64 bytes from columbiauniversity.org (128.59.105.24): icmp_seq=4 ttl=233 time=274 ms
64 bytes from neurotheory.columbia.edu (128.59.105.24): icmp_seq=5 ttl=233 time=296 ms
64 bytes from old.columbia.university (128.59.105.24): icmp_seq=6 ttl=233 time=320 ms
64 bytes from gutenberg-e.org (128.59.105.24): icmp_seq=7 ttl=233 time=344 ms
64 bytes from neurotheory.columbia.edu (128.59.105.24): icmp_seq=8 ttl=233 time=263 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=9 ttl=233 time=285 ms
64 bytes from www.neurotheory.columbia.edu (128.59.105.24): icmp_seq=10 ttl=233 time=309 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=11 ttl=233 time=331 ms
64 bytes from p-i-r.org (128.59.105.24): icmp_seq=12 ttl=233 time=252 ms
64 bytes from columbiauniversity.org (128.59.105.24): icmp_seq=13 ttl=233 time=274 ms
64 bytes from teachtechaward.org (128.59.105.24): icmp_seq=14 ttl=233 time=296 ms
64 bytes from columbiauniversity.org (128.59.105.24): icmp_seq=15 ttl=233 time=325 ms
64 bytes from teachtechaward.org (128.59.105.24): icmp_seq=16 ttl=233 time=342 ms
64 bytes from columbiauniversity.org (128.59.105.24): icmp_seq=17 ttl=233 time=263 ms
64 bytes from childpolicy.org (128.59.105.24): icmp_seq=18 ttl=233 time=285 ms
64 bytes from columbiauniversity.info (128.59.105.24): icmp_seq=19 ttl=233 time=308 ms
64 bytes from p-i-r.org (128.59.105.24): icmp_seq=20 ttl=233 time=334 ms
64 bytes from old.columbia.university (128.59.105.24): icmp_seq=21 ttl=233 time=252 ms
64 bytes from gutenberg-e.org (128.59.105.24): icmp_seq=22 ttl=233 time=274 ms
64 bytes from columbiauniversity.org (128.59.105.24): icmp_seq=23 ttl=233 time=296 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=24 ttl=233 time=241 ms
64 bytes from childpolicy.org (128.59.105.24): icmp_seq=25 ttl=233 time=245 ms
64 bytes from childpolicy.org (128.59.105.24): icmp_seq=26 ttl=233 time=241 ms
64 bytes from columbiauniversity.net (128.59.105.24): icmp_seq=27 ttl=233 time=253 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=28 ttl=233 time=241 ms
64 bytes from www.neurotheory.columbia.edu (128.59.105.24): icmp_seq=29 ttl=233 time=334 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=30 ttl=233 time=260 ms
64 bytes from childpolicy.org (128.59.105.24): icmp_seq=31 ttl=233 time=244 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=32 ttl=233 time=241 ms
64 bytes from teachtechaward.org (128.59.105.24): icmp_seq=33 ttl=233 time=243 ms
64 bytes from teachtechaward.org (128.59.105.24): icmp_seq=34 ttl=233 time=424 ms
64 bytes from columbiauniversity.us (128.59.105.24): icmp_seq=35 ttl=233 time=247 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=36 ttl=233 time=242 ms
64 bytes from neurotheory.columbia.edu (128.59.105.24): icmp_seq=37 ttl=233 time=254 ms
```

```
64 bytes from teachtechaward.org (128.59.105.24): icmp_seq=82 ttl=233 time=311 ms
64 bytes from neurotheory.columbia.edu (128.59.105.24): icmp_seq=83 ttl=233 time=334 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=84 ttl=233 time=256 ms
64 bytes from p-i-r.org (128.59.105.24): icmp_seq=85 ttl=233 time=276 ms
64 bytes from columbiauniversity.net (128.59.105.24): icmp_seq=86 ttl=233 time=243 ms
64 bytes from old.columbia.university (128.59.105.24): icmp_seq=87 ttl=233 time=240 ms
64 bytes from columbiauniversity.us (128.59.105.24): icmp_seq=88 ttl=233 time=242 ms
64 bytes from gutenberg-e.org (128.59.105.24): icmp_seq=89 ttl=233 time=242 ms
64 bytes from childpolicy.org (128.59.105.24): icmp_seq=90 ttl=233 time=241 ms
64 bytes from columbiauniversity.info (128.59.105.24): icmp_seq=92 ttl=233 time=336 ms
64 bytes from columbiauniversity.info (128.59.105.24): icmp_seq=93 ttl=233 time=252 ms
64 bytes from vii.org (128.59.105.24): icmp_seq=94 ttl=233 time=275 ms
64 bytes from columbiauniversity.info (128.59.105.24): icmp_seq=95 ttl=233 time=299 ms
64 bytes from p-i-r.org (128.59.105.24): icmp_seq=96 ttl=233 time=320 ms
64 bytes from old.columbia.university (128.59.105.24): icmp_seq=97 ttl=233 time=343 ms
64 bytes from childpolicy.org (128.59.105.24): icmp_seq=98 ttl=233 time=266 ms
64 bytes from old.columbia.university (128.59.105.24): icmp_seq=99 ttl=233 time=287 ms
64 bytes from p-i-r.org (128.59.105.24): icmp_seq=100 ttl=233 time=309 ms

--- columbia.edu ping statistics ---
100 packets transmitted, 99 received, 1% packet loss, time 99121ms
rtt min/avg/max/mdev = 240.343/273.139/424.008/37.860 ms
```

Average latency = 273.343/2 = 136.6715 ms

d. e.

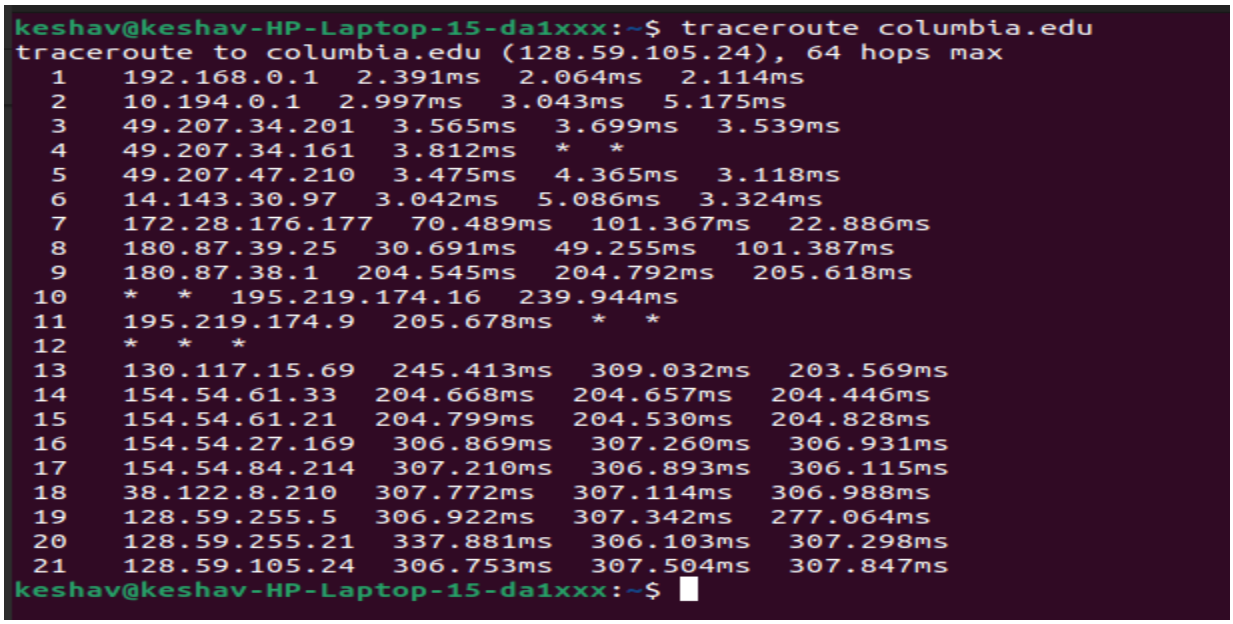
Sum of average latency of intermediate hosts of google.in ≠ average latency of 100 ping packets to google.in

Maximum latency of intermediate hosts of google.in ≈ average latency of 100 ping packets to google.in

Reason for such observations

The bottleneck latency is equal to the average latency observed by the ping. In this case bottleneck latency is around 5.8 ms and ping latency is 7.7 ms (minor difference is due to other delays). We can imagine a network as a pipe structure where the network latency is because of the bottleneck pipe.

f.



Hops for columbia.edu(21) > Hops for google.in (7) (possible bcoz routers have direct access to google.in compared to columbia where packet has to take longer path)

The reason for latency difference between the two websites are:

1. The number of intermediate hosts in columbia.edu > intermediate hosts in google.in
2. The bottleneck latency in case of columbia.edu > bottleneck latency of path of google.in
3. The traceroute for google.in is less as google.in is highly visited website so routers have smaller path access for google.in compared to columbia.edu in which packets needs to have more hops.

Answer-4

When the ping is not failing the response looks like as follows:

```
keshav@keshav-HP-Laptop-15-da1xxx:~$ ping -c 4 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.045 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.052 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.059 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.052 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3071ms
rtt min/avg/max/mdev = 0.045/0.052/0.059/0.005 ms
```

Command Run: sudo ifconfig lo down

After running the above command the ping to the localhost(127.0.0.1) fails.

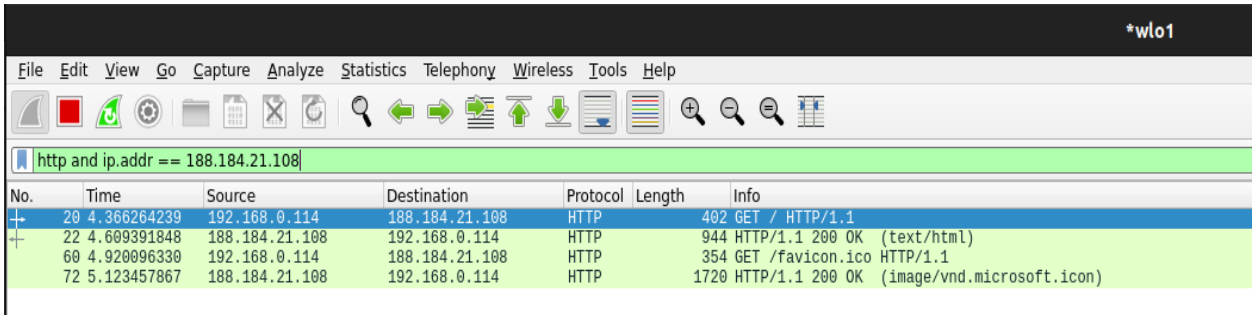
```
keshav@keshav-HP-Laptop-15-da1xxx:~$ sudo ifconfig lo down
[sudo] password for keshav:
keshav@keshav-HP-Laptop-15-da1xxx:~$
keshav@keshav-HP-Laptop-15-da1xxx:~$
keshav@keshav-HP-Laptop-15-da1xxx:~$
keshav@keshav-HP-Laptop-15-da1xxx:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
^C
--- 127.0.0.1 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7161ms

keshav@keshav-HP-Laptop-15-da1xxx:~$
```

```
keshav@keshav-HP-Laptop-15-da1xxx:~$ ifconfig
eno1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether f8:b4:6a:d1:30:0b  txqueuelen 1000  (Ethernet)
        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

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.114  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::73b0:e38f:1ce0:119e  prefixlen 64  scopeid 0x20<link>
        ether b0:68:e6:2a:fc:65  txqueuelen 1000  (Ethernet)
        RX packets 3114088  bytes 1995796153 (1.9 GB)
        RX errors 0  dropped 11  overruns 0  frame 0
        TX packets 721210  bytes 173749170 (173.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The ping command for localhost is blocked by removing the “lo” interface. Lo interface stands for loopback interface and it is a special interface that a system uses to communicate with itself. Once this is disabled then the self ping won’t happen as shown in the above images.

Answer-5

The following were the request response packets seen on wireshark



There were 2 HTTP requests and 2 HTTP responses for the 2 requests given by the browser. In the first request it asked for html content and in the second request it asked for a favicon icon.

For HTTP Request Packets:

HTTP Request type: GET

User Agent Type: Mozilla/5.0 (X11; Linux x86_64; rv:104.0) Gecko/20100101 Firefox/104.0

HTTP Request Packet URL: info.cern.ch

HTTP Request packet URI: /

For HTTP Response Packet

HTTP Response Code: 200 OK

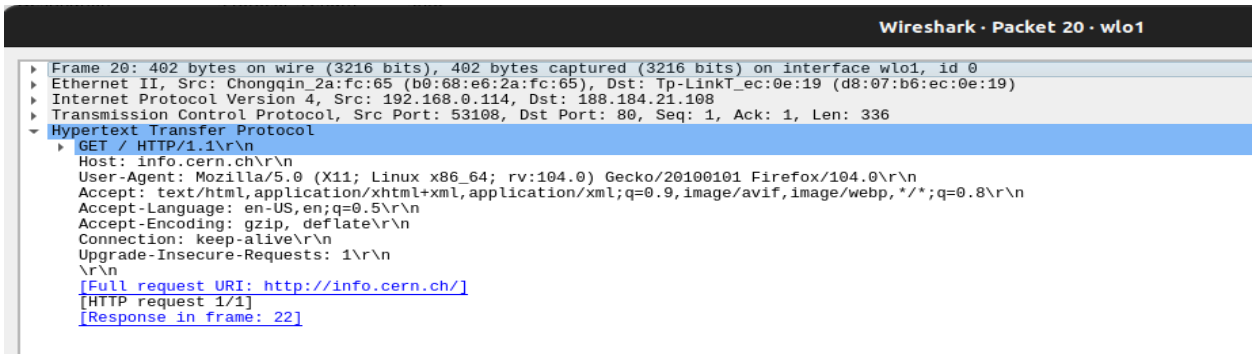
HTTP Response Description: OK

Name and version of the web server: Apache

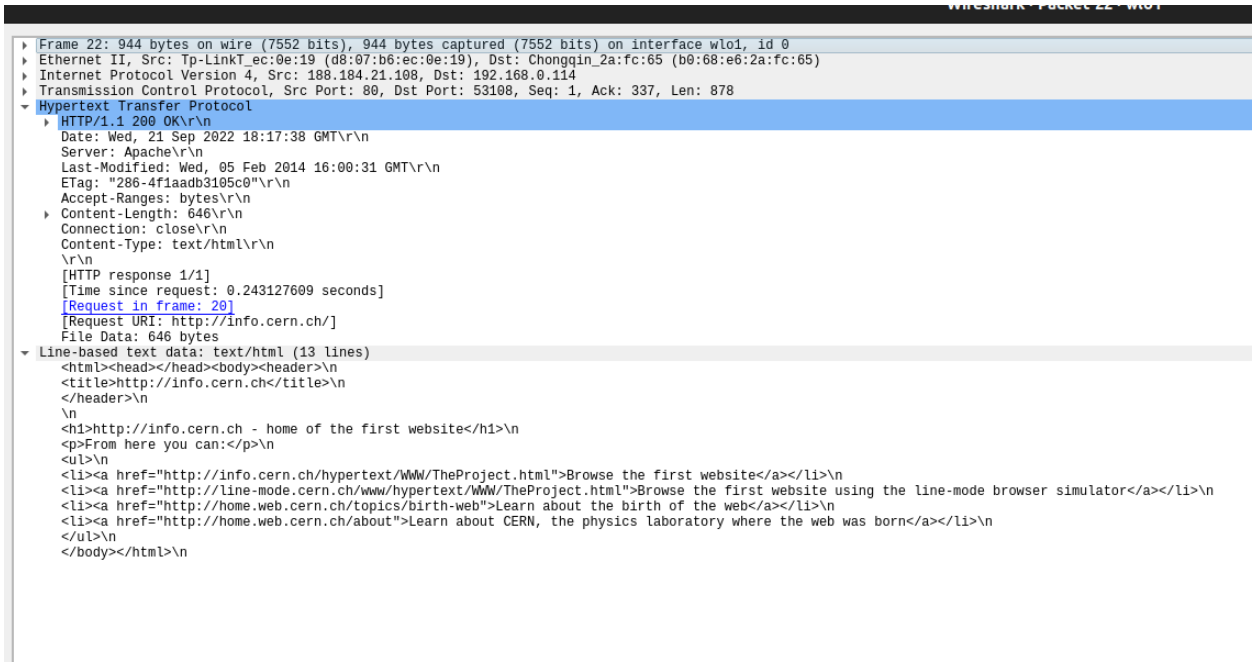
Number of objects downloaded: 2 objects were downloaded and they were not on the same tcp connection.

HTTP is not-persistent in this case.

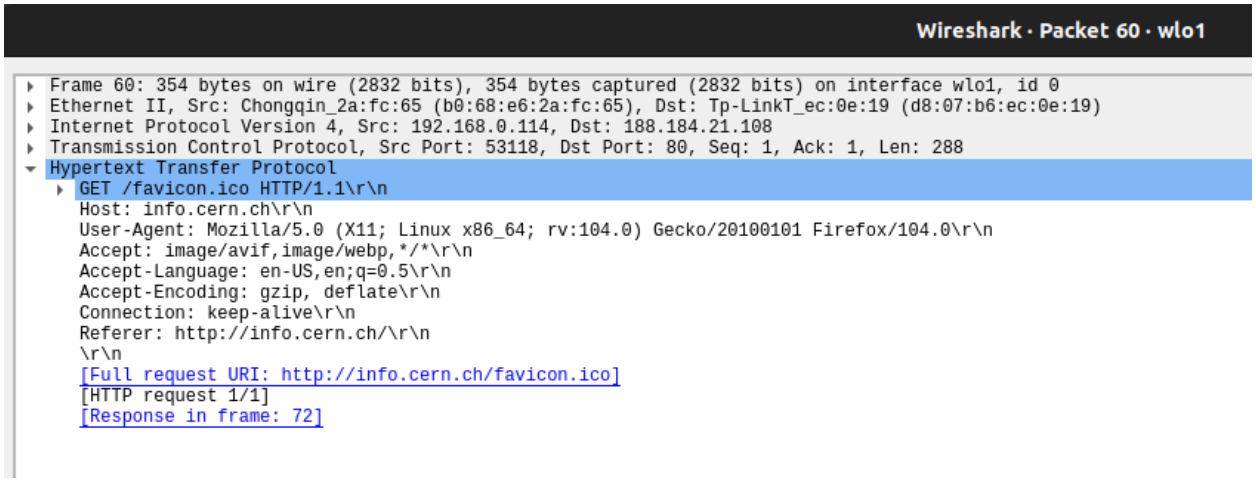
The following are the images of packets collected from the wireshark. These are http packets and there are 2 such packets. The first one requests for html while the second one requests a favicon icon. The response of the first contains html and the second one contains favicon.



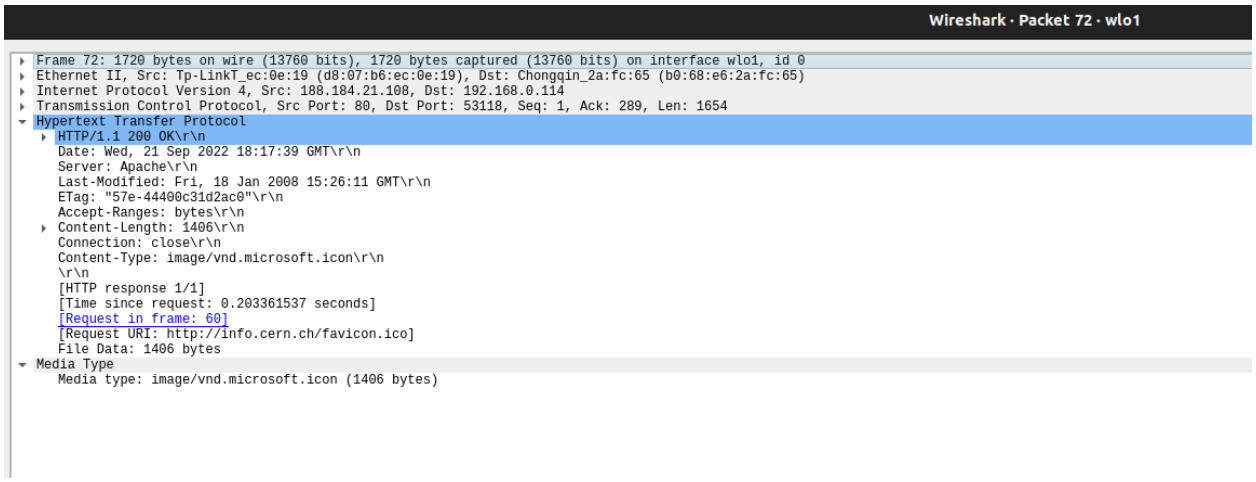
Request-1



Response-1

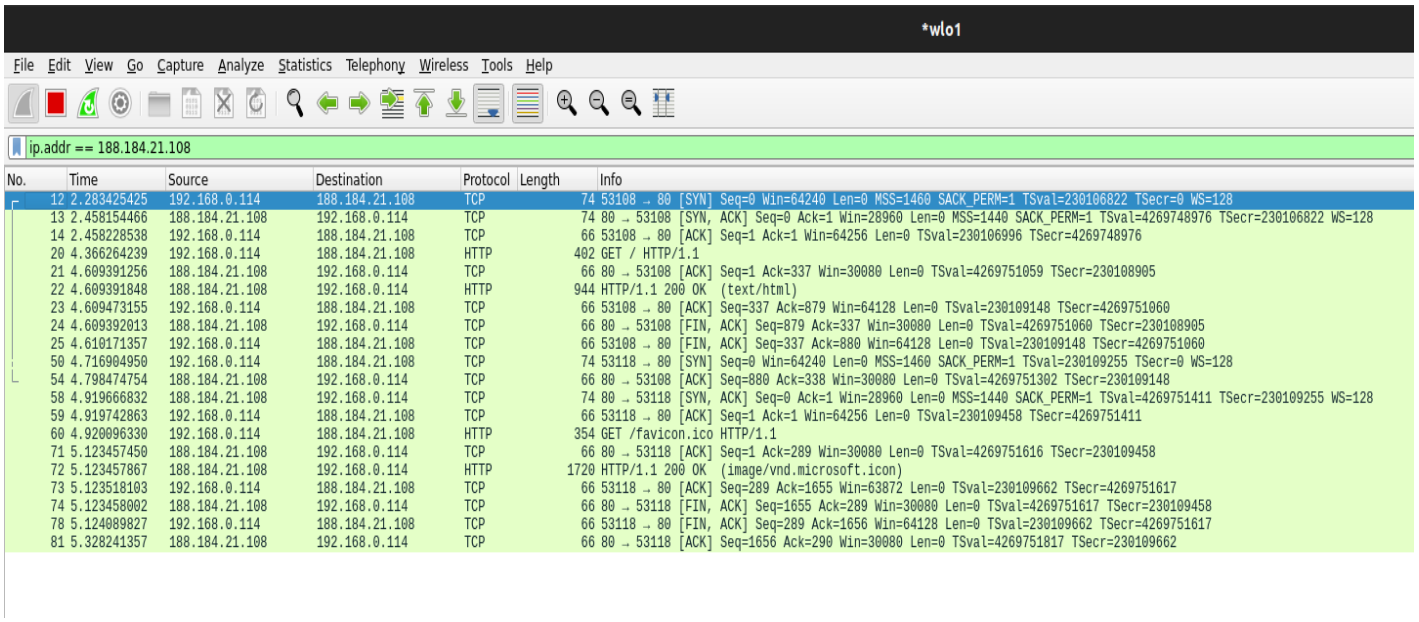


Request-2



Response-2

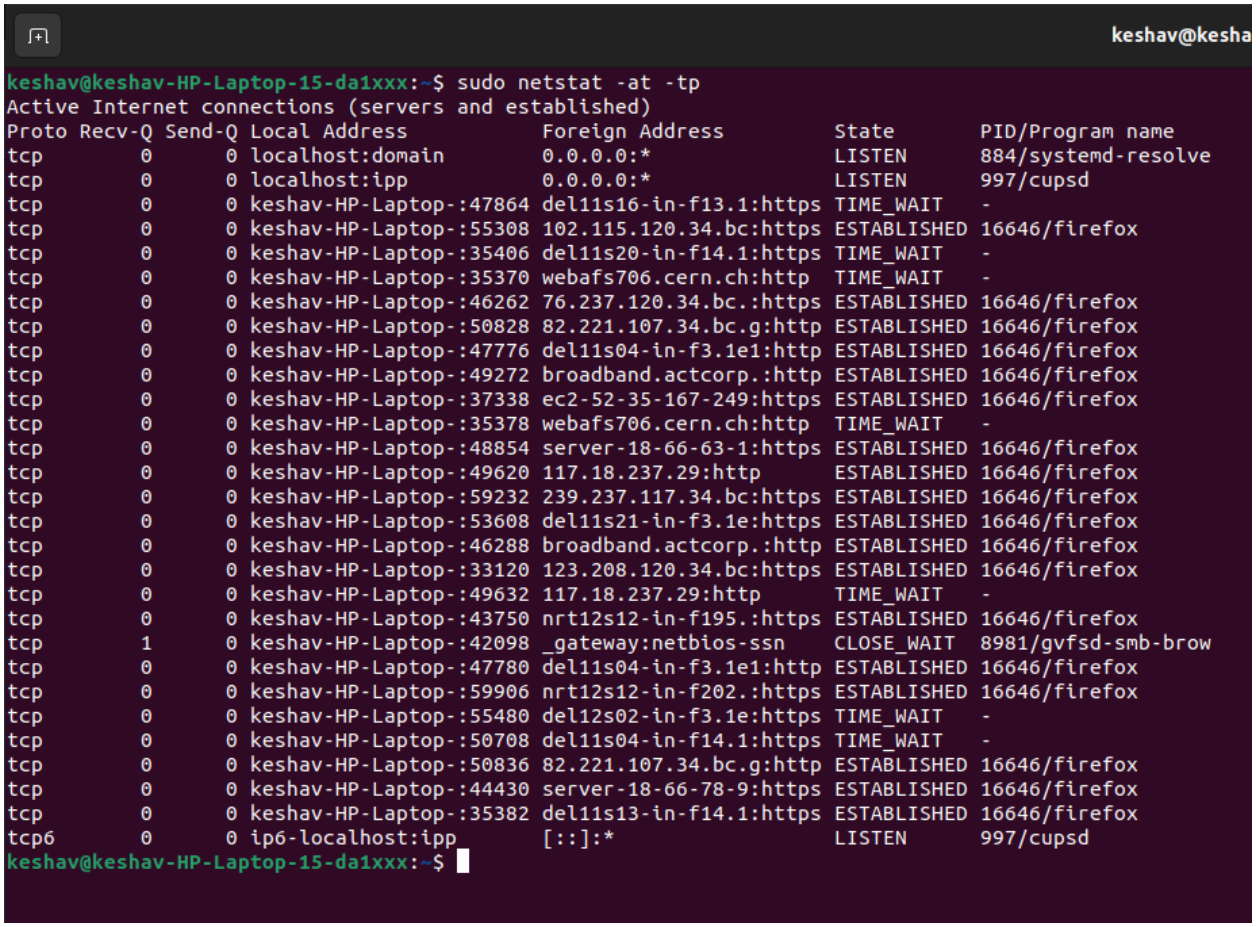
The connection is not persistent for both HTTP requests. This can be analyzed from the image below.



From the image above we can clearly see that for each HTTP request there is a separate tcp connection (from [syn] → [syn ack] →[ack] packets that is 3 way handshake) hence we can say the connection is non-persistent.

Answer-6

Command: sudo netstat -at -tp
Flags: -at: for tcp connections
-tp: to list PID/Program name



Foreign Address: webafs706.cern.ch: http
State of the connection: Time_wait