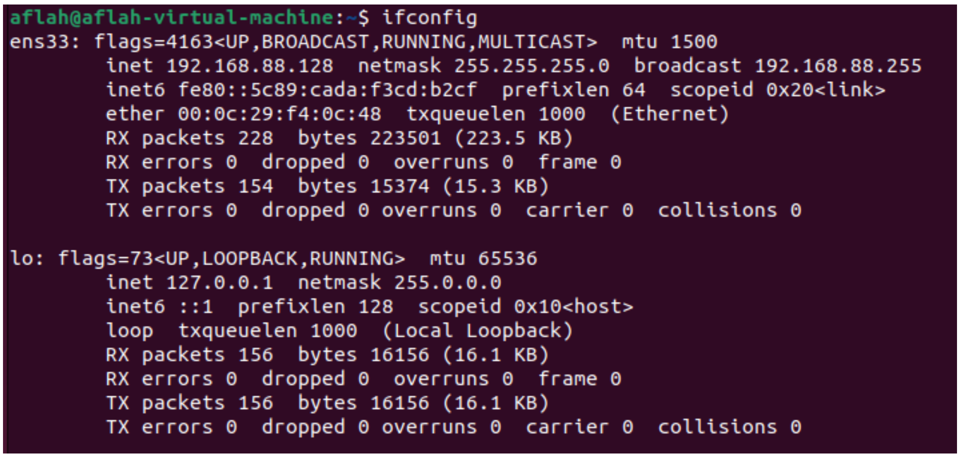
CN Assignment

Mohammad Aflah Khan, 2020082

A1)

a)



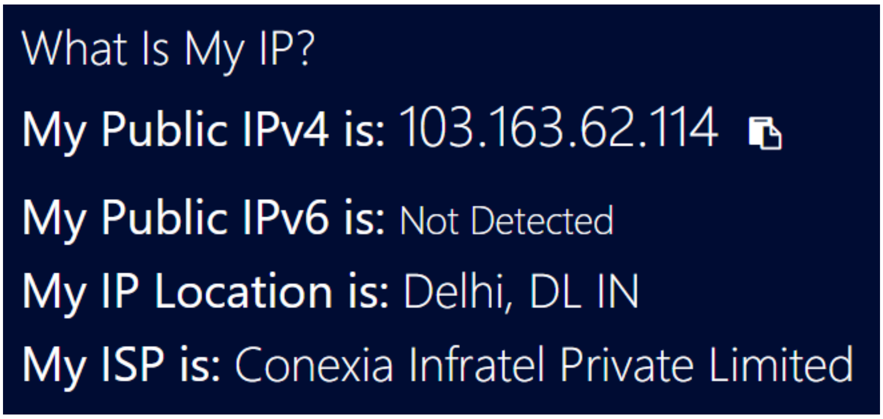
```
aflah@aflah-virtual-machine:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.88.128  netmask 255.255.255.0  broadcast 192.168.88.255
        inet6 fe80::5c89:cada:f3cd:b2cf  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:f4:0c:48  txqueuelen 1000  (Ethernet)
        RX packets 228  bytes 223501 (223.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 154  bytes 15374 (15.3 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 156  bytes 16156 (16.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 156  bytes 16156 (16.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

On Running ifconfig I see 2 outputs, here ens33 is the relevant output as ens33 as ens33 is the default network interface in Ubuntu. lo is just the loopback device which can be used to access networks locally.

Hence my IP Address according to ifconfig is 192.168.88.128

b)

If I open https://www.whatismyip.com/ I see the following –



What Is My IP?

My Public IPv4 is: 103.163.62.114

My Public IPv6 is: Not Detected

My IP Location is: Delhi, DL IN

My ISP is: Conexia Infratel Private Limited

So according to the website my IP Address is 103.163.62.114

Both these values are different as ifconfig displays the local IP address, however when someone tries to access the internet they need to pass over switches and routers in the network. The website returns the IP address which the rest of the world will see (i.e. the global IP Address) when I send requests as this is the IP address provided to me by my ISP.

A2)

a)

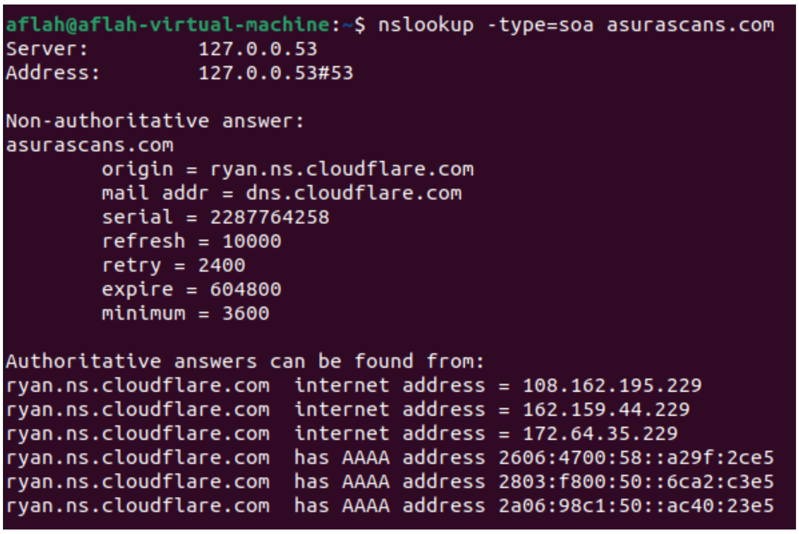
Finding the authoritative URL can be done is 2 steps:

1) First find the origin URL using a SOA (Search of Authority) query
2) Use the Origin URL for a lookup

This is because to get the authoritative answer we need to provide the authoritative name server as a part of the request. To procure the authoritative name server we can use a -type=soa flag which returns the same.

Let’s say we are interested to find details for asurascans.com which is a comic translation website.

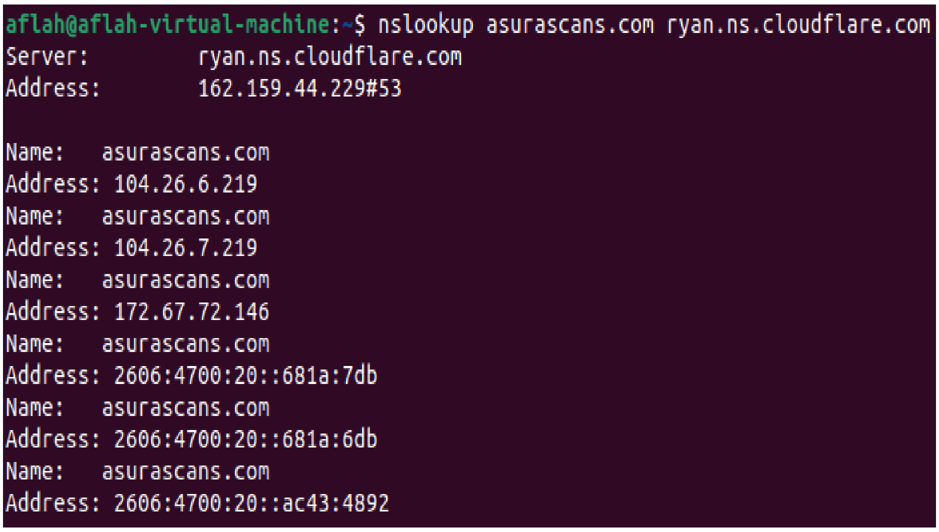
Finding the Origin URL –



```
aflah@aflah-virtual-machine:~$ nslookup -type=soa asurascans.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
asurascans.com
        origin = ryan.ns.cloudflare.com
        mail addr = dns.cloudflare.com
        serial = 2287764258
        refresh = 10000
        retry = 2400
        expire = 604800
        minimum = 3600

Authoritative answers can be found from:
ryan.ns.cloudflare.com  internet address = 108.162.195.229
ryan.ns.cloudflare.com  internet address = 162.159.44.229
ryan.ns.cloudflare.com  internet address = 172.64.35.229
ryan.ns.cloudflare.com  has AAAA address 2606:4700:58::a29f:2ce5
ryan.ns.cloudflare.com  has AAAA address 2803:f800:50::6ca2:c3e5
ryan.ns.cloudflare.com  has AAAA address 2a06:98c1:50::ac40:23e5
```

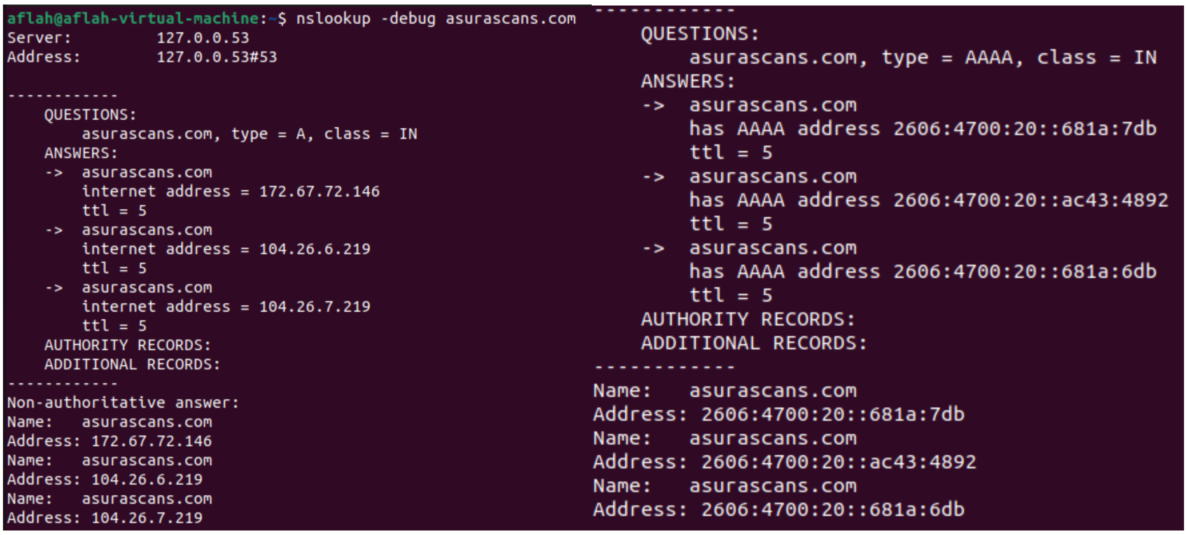
Hence our origin URL is ryan.ns.cloudflare.com

Doing lookup for this URL –



```
aflah@aflah-virtual-machine:~$ nslookup asurascans.com ryan.ns.cloudflare.com
Server:         ryan.ns.cloudflare.com
Address:        162.159.44.229#53

Name:   asurascans.com
Address: 104.26.6.219
Name:   asurascans.com
Address: 104.26.7.219
Name:   asurascans.com
Address: 172.67.72.146
Name:   asurascans.com
Address: 2606:4700:20::681a:7db
Name:   asurascans.com
Address: 2606:4700:20::681a:6db
Name:   asurascans.com
Address: 2606:4700:20::ac43:4892
```

b)



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

------------
    QUESTIONS:
        asurascans.com, type = A, class = IN
    ANSWERS:
    ->  asurascans.com
        internet address = 172.67.72.146
        ttl = 5
    ->  asurascans.com
        internet address = 104.26.6.219
        ttl = 5
    ->  asurascans.com
        internet address = 104.26.7.219
        ttl = 5
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Non-authoritative answer:
Name:   asurascans.com
Address: 172.67.72.146
Name:   asurascans.com
Address: 104.26.6.219
Name:   asurascans.com
Address: 104.26.7.219
```

```
------------
    QUESTIONS:
        asurascans.com, type = AAAA, class = IN
    ANSWERS:
    ->  asurascans.com
        has AAAA address 2606:4700:20::681a:7db
        ttl = 5
    ->  asurascans.com
        has AAAA address 2606:4700:20::ac43:4892
        ttl = 5
    ->  asurascans.com
        has AAAA address 2606:4700:20::681a:6db
        ttl = 5
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Name:   asurascans.com
Address: 2606:4700:20::681a:7db
Name:   asurascans.com
Address: 2606:4700:20::ac43:4892
Name:   asurascans.com
Address: 2606:4700:20::681a:6db
```

Time to Live (TTL)–

Command used: nslookup -debug asurascans.com

IPv4 addresses are type A

IPv6 addresses are type AAAA

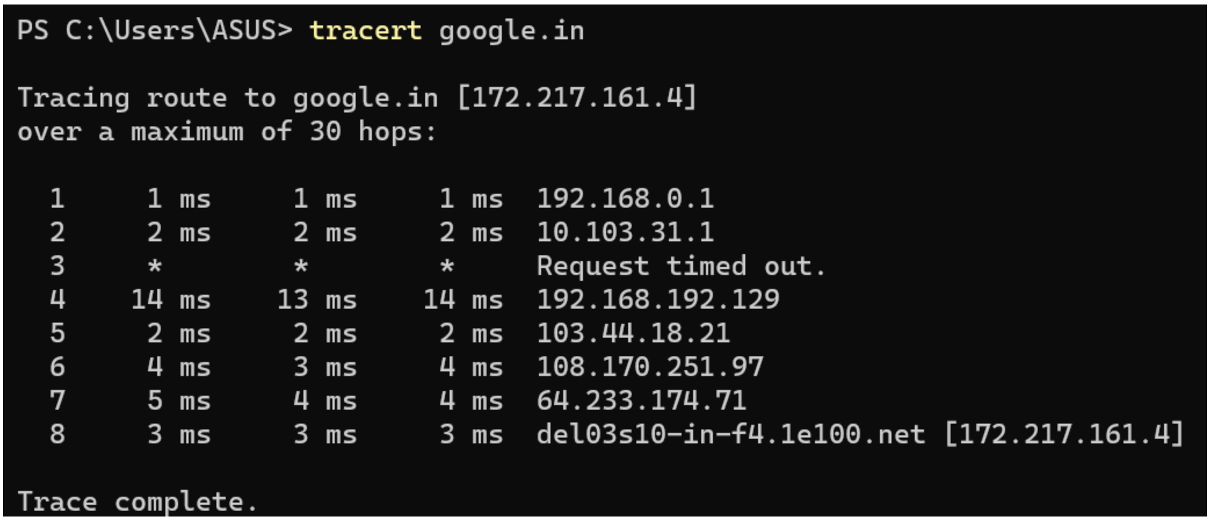
TTL for IPv4 is 5 seconds

TTL for IPv6 is 5 seconds

Hence the entries stay in the cache for 5 seconds after which they need to be refetched

A3)

Command used - tracert google.com (on my Windows Machine)



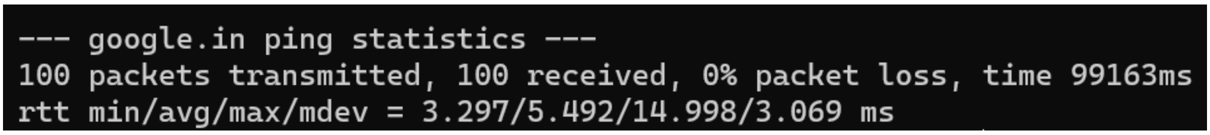
```
PS C:\Users\ASUS> tracert google.in

Tracing route to google.in [172.217.161.4]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.0.1
  2     2 ms     2 ms     2 ms  10.103.31.1
  3     *        *        *     Request timed out.
  4    14 ms    13 ms    14 ms  192.168.192.129
  5     2 ms     2 ms     2 ms  103.44.18.21
  6     4 ms     3 ms     4 ms  108.170.251.97
  7     5 ms     4 ms     4 ms  64.233.174.71
  8     3 ms     3 ms     3 ms  del03s10-in-f4.1e100.net [172.217.161.4]

Trace complete.
```

a)

As there are 8 Intermediate hosts and 1 Destination host, the average latency to each can be computed by first averaging the 3 values to get the average Round Trip Time and then then dividing by 2 gives us the average latency. Latency is approximately half the Round Trip Time assuming it's uniform and same both ways.

IP Address	Average Latency Computation	Average Latency
192.168.0.1	((1+1+1)/3)/2	0.5 ms
10.103.31.1	((2+2+2)/3)/2	1 ms
192.168.192.129	((14+13+14)/3)/2	6.833 ms
103.44.18.21	((2+2+2)/3)/2	1 ms
108.170.251.97	((4+3+4)/3)/2	1.833 ms
64.233.174.71	((5+4+4)/3)/2	2.166 ms
172.217.161.4 (Destination)	((3+3+3)/3)/2	1.5 ms

b)

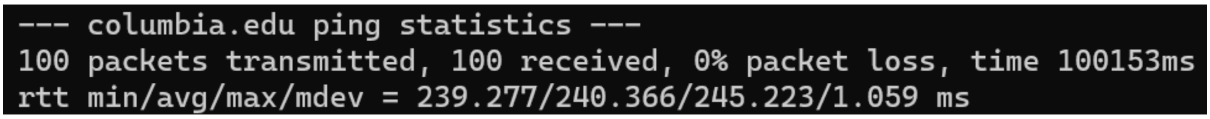


```
--- google.in ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 99163ms
rtt min/avg/max/mdev = 3.297/5.492/14.998/3.069 ms
```

Command Used - ping -c 100 google.in

Hence the Average Latency = Average RTT/2 = 5.492/2 = 2.746 ms

c)



```
--- columbia.edu ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 100153ms
rtt min/avg/max/mdev = 239.277/240.366/245.223/1.059 ms
```

Command Used - ping -c 100 columbia.edu

Hence the Average Latency = Average RTT/2 = 240.366/2 = 120.184 ms

d)

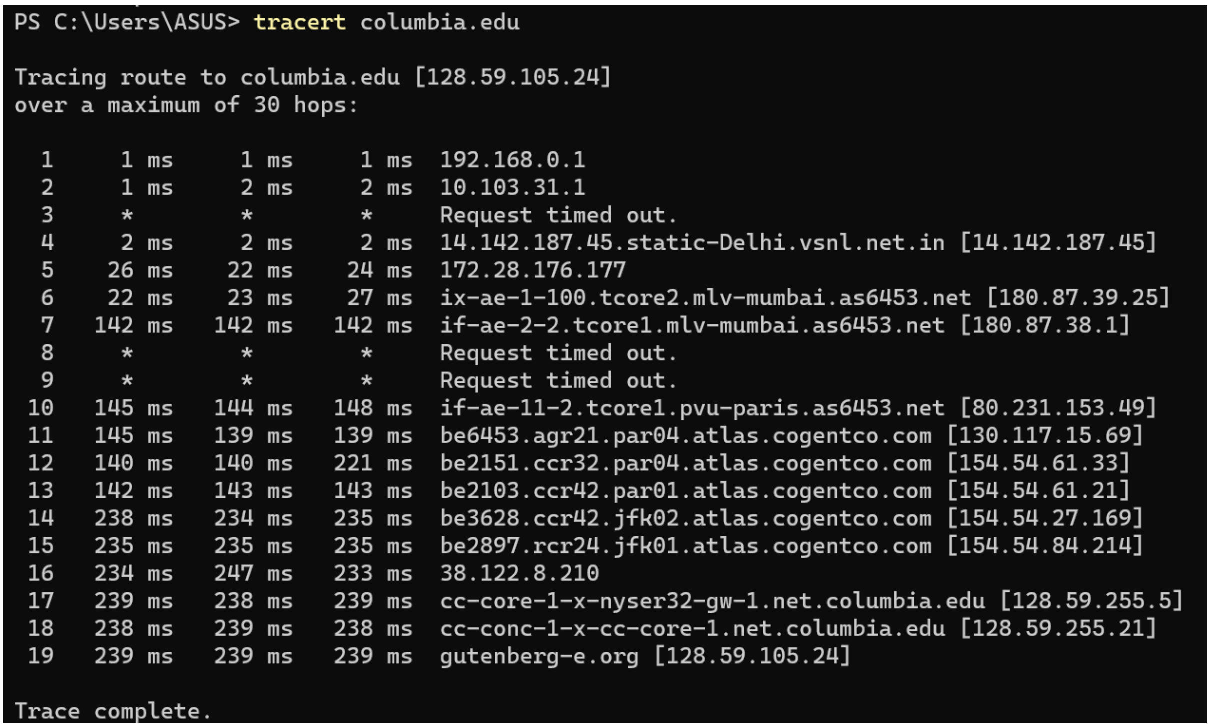
Sum of Average Latencies is 14.832 ms however actual average latency is only 2.746 ms. These are very different with the ping latency being significantly lower.

The reason for this is that tracert must wait at every intermediate host to get the response while ping simply sends packets which do not need to wait anywhere!

e)

The maximum ping latency is 6.833 ms while average latency is 2.746 ms. These values are more comparable as we are now not considering waiting at every intermediate host rather we only consider waiting at one host. So this acts similar to how ping does as it also just waits for response from destination to send back activity status and journey statistics.

f)



```
PS C:\Users\ASUS> tracert columbia.edu

Tracing route to columbia.edu [128.59.105.24]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.0.1
  2     1 ms     2 ms     2 ms  10.103.31.1
  3     *        *        *     Request timed out.
  4     2 ms     2 ms     2 ms  14.142.187.45.static-Delhi.vsnl.net.in [14.142.187.45]
  5    26 ms    22 ms    24 ms  172.28.176.177
  6    22 ms    23 ms    27 ms  ix-ae-1-100.tcore2.mlv-mumbai.as6453.net [180.87.39.25]
  7   142 ms   142 ms   142 ms  if-ae-2-2.tcore1.mlv-mumbai.as6453.net [180.87.38.1]
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10   145 ms   144 ms   148 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 11   145 ms   139 ms   139 ms  be6453.agr21.par04.atlas.cogentco.com [130.117.15.69]
 12   140 ms   140 ms   221 ms  be2151.ccr32.par04.atlas.cogentco.com [154.54.61.33]
 13   142 ms   143 ms   143 ms  be2103.ccr42.par01.atlas.cogentco.com [154.54.61.21]
 14   238 ms   234 ms   235 ms  be3628.ccr42.jfk02.atlas.cogentco.com [154.54.27.169]
 15   235 ms   235 ms   235 ms  be2897.rcr24.jfk01.atlas.cogentco.com [154.54.84.214]
 16   234 ms   247 ms   233 ms  38.122.8.210
 17   239 ms   238 ms   239 ms  cc-core-1-x-nyser32-gw-1.net.columbia.edu [128.59.255.5]
 18   238 ms   239 ms   238 ms  cc-conc-1-x-cc-core-1.net.columbia.edu [128.59.255.21]
 19   239 ms   239 ms   239 ms  gutenberg-e.org [128.59.105.24]

Trace complete.
```

Number of hops for columbia.edu = 19

Number of hops for google.in = 8

Average Latency for columbia.edu = 120.184 ms

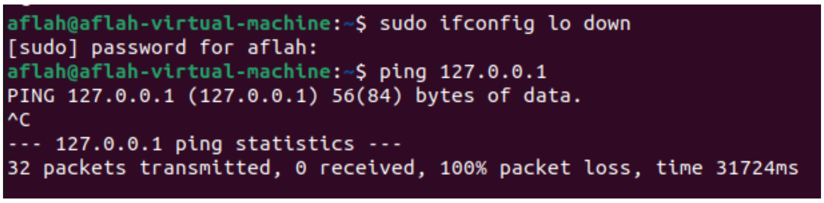
Average Latency for google.in = 2.746 ms

The latency and hops are much lower for google.in as it is a company which makes money off servicing users. If it had slower speeds people wouldn't use it and switch to competitors. To ensure that it has high speeds it also has many more data centres across the world as compared to columbia.edu which is an educational website and does not have to focus on these high requirements.

A4)

To get 100% packet loss on our local server, we can simply have the loopback interface driver shut down. The command for the same is – sudo ifconfig lo down

Now if we ping 127.0.0.1 we get 100% packet loss as there is no response since we shut down the loopback interface driver which is responsible for sending responses addressed to 127.0.0.1

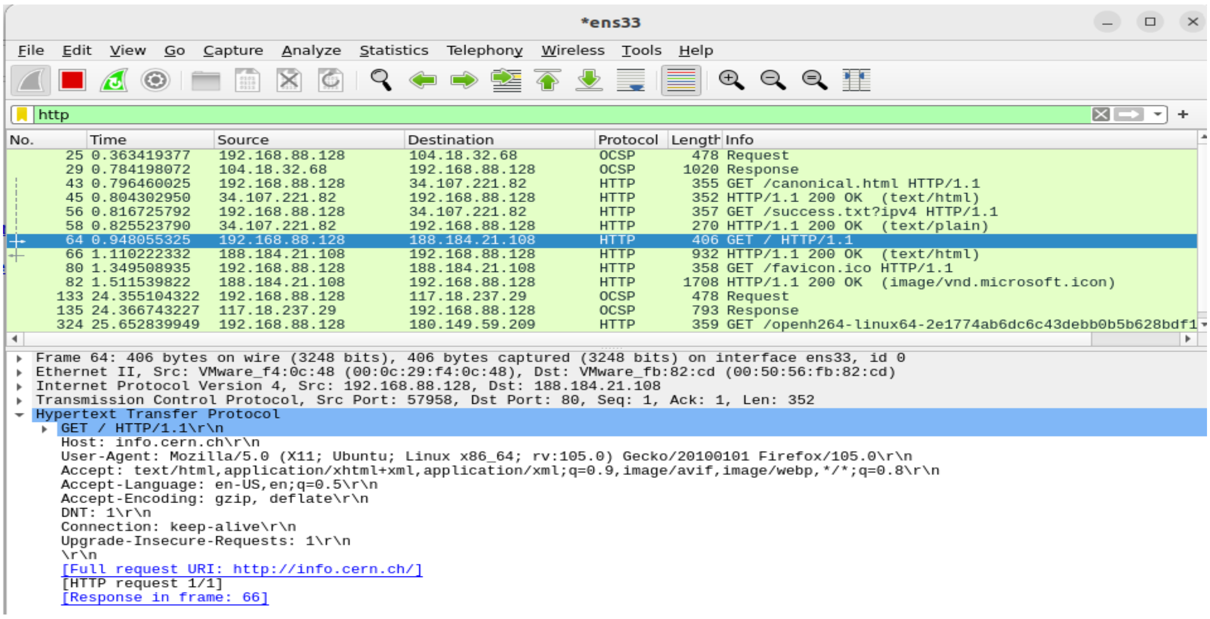


```
aflah@aflah-virtual-machine:~$ sudo ifconfig lo down
[sudo] password for aflah:
aflah@aflah-virtual-machine:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
^C
--- 127.0.0.1 ping statistics ---
32 packets transmitted, 0 received, 100% packet loss, time 31724ms
```

A5)

The capture logs are also present in the zip

- For HTTP Request Packages
    - HTTP Request Type: GET / HTTP/1.1\r\n
    - User Agent Type: User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:105.0) Gecko/20100101 Firefox/105.0\r\n
    - HTTP Request Packet URL: [Full request URI: http://info.cern.ch/]

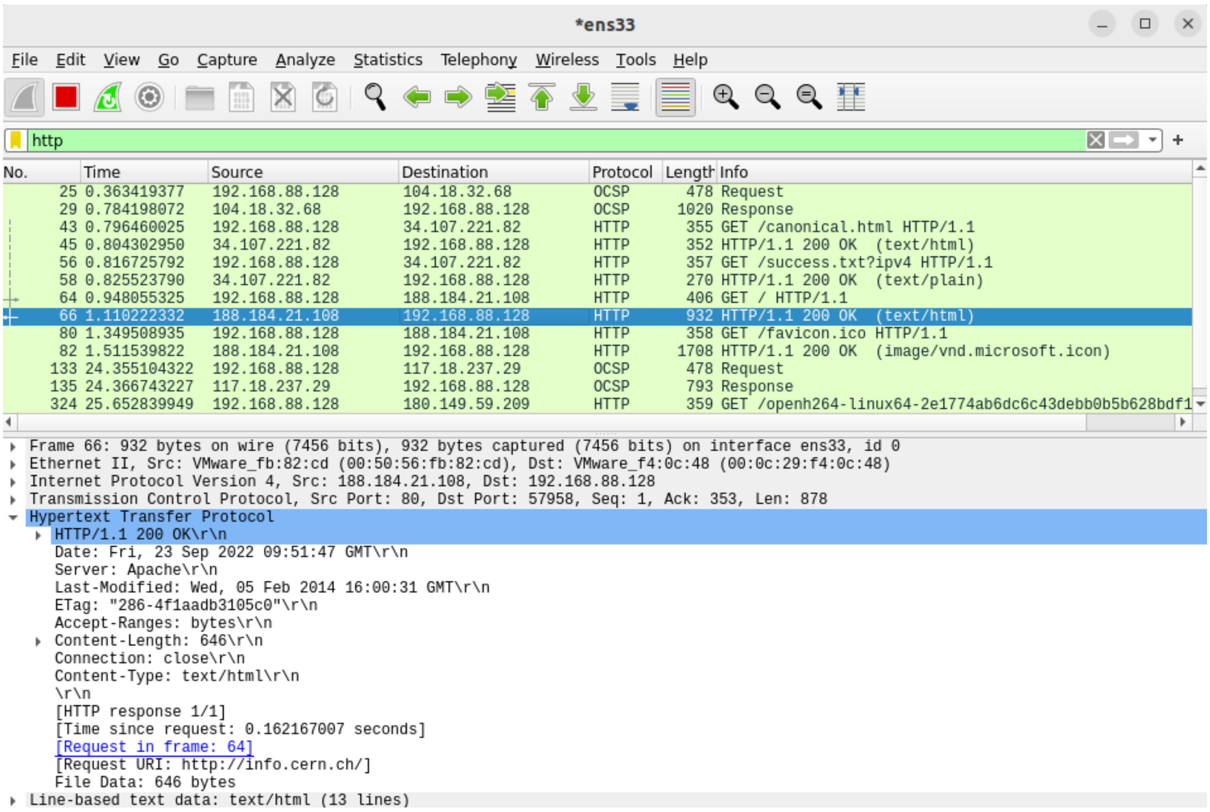


http

```
No.    Time          Source           Destination      Protocol Length Info
    25 0.363419377   192.168.88.128   104.18.32.68     OCSP      478 Request
    29 0.784198072   104.18.32.68     192.168.88.128   OCSP     1020 Response
    43 0.796460025   192.168.88.128   34.107.221.82    HTTP      355 GET /canonical.html HTTP/1.1
    45 0.804302950   34.107.221.82    192.168.88.128   HTTP      352 HTTP/1.1 200 OK  (text/html)
    56 0.816725792   192.168.88.128   34.107.221.82    HTTP      357 GET /success.txt?ipv4 HTTP/1.1
    58 0.825523790   34.107.221.82    192.168.88.128   HTTP      270 HTTP/1.1 200 OK  (text/plain)
    64 0.948055325   192.168.88.128   188.184.21.108   HTTP      406 GET / HTTP/1.1
    66 1.110222332   188.184.21.108   192.168.88.128   HTTP      932 HTTP/1.1 200 OK  (text/html)
    80 1.349508935   192.168.88.128   188.184.21.108   HTTP      358 GET /favicon.ico HTTP/1.1
    82 1.511539822   188.184.21.108   192.168.88.128   HTTP     1708 HTTP/1.1 200 OK  (image/vnd.microsoft.icon)
   133 24.355104322  192.168.88.128   117.18.237.29    OCSP      478 Request
   135 24.366743227  117.18.237.29    192.168.88.128   OCSP      793 Response
   324 25.652839949  192.168.88.128   180.149.59.209   HTTP      359 GET /openh264-linux64-2e1774ab6dc6c43debb0b5b628bdf1
```

```
▸ Frame 64: 406 bytes on wire (3248 bits), 406 bytes captured (3248 bits) on interface ens33, id 0
▸ Ethernet II, Src: VMware_f4:0c:48 (00:0c:29:f4:0c:48), Dst: VMware_fb:82:cd (00:50:56:fb:82:cd)
▸ Internet Protocol Version 4, Src: 192.168.88.128, Dst: 188.184.21.108
▸ Transmission Control Protocol, Src Port: 57958, Dst Port: 80, Seq: 1, Ack: 1, Len: 352
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Host: info.cern.ch\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:105.0) Gecko/20100101 Firefox/105.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    DNT: 1\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://info.cern.ch/]
    [HTTP request 1/1]
    [Response in frame: 66]
```

- For HTTP Response Packets
    - HTTP Response Code: 200 OK
    - HTTP response description: A 200 OK Code implies the request was successful
    - Name and version of the web server: Apache

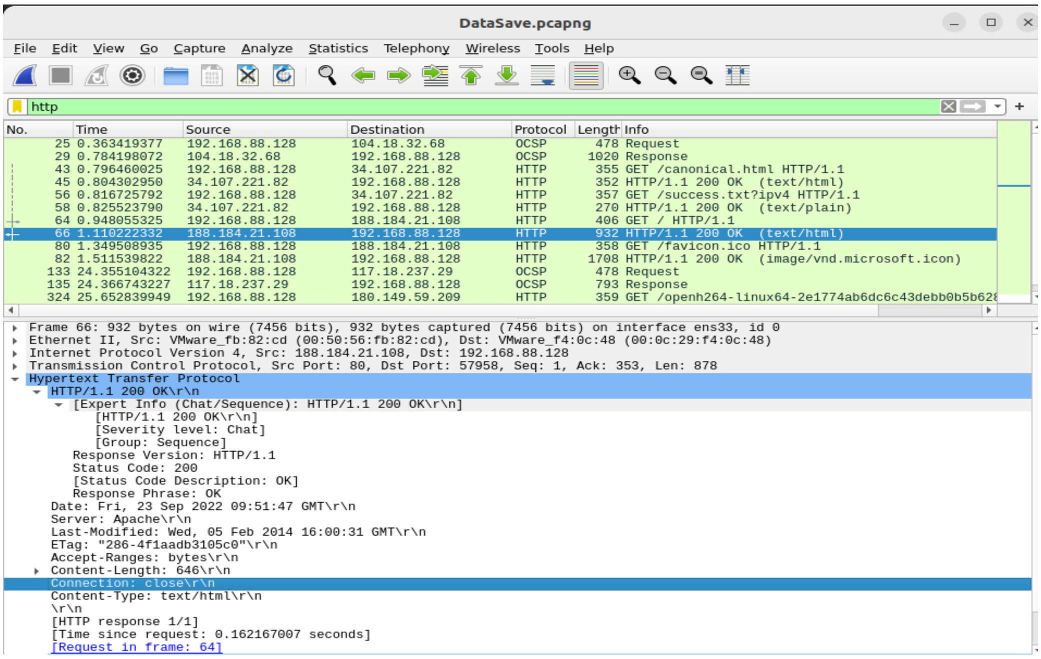


http

```
No.    Time          Source           Destination      Protocol Length Info
    25 0.363419377   192.168.88.128   104.18.32.68     OCSP      478 Request
    29 0.784198072   104.18.32.68     192.168.88.128   OCSP     1020 Response
    43 0.796460025   192.168.88.128   34.107.221.82    HTTP      355 GET /canonical.html HTTP/1.1
    45 0.804302950   34.107.221.82    192.168.88.128   HTTP      352 HTTP/1.1 200 OK  (text/html)
    56 0.816725792   192.168.88.128   34.107.221.82    HTTP      357 GET /success.txt?ipv4 HTTP/1.1
    58 0.825523790   34.107.221.82    192.168.88.128   HTTP      270 HTTP/1.1 200 OK  (text/plain)
    64 0.948055325   192.168.88.128   188.184.21.108   HTTP      406 GET / HTTP/1.1
    66 1.110222332   188.184.21.108   192.168.88.128   HTTP      932 HTTP/1.1 200 OK  (text/html)
    80 1.349508935   192.168.88.128   188.184.21.108   HTTP      358 GET /favicon.ico HTTP/1.1
    82 1.511539822   188.184.21.108   192.168.88.128   HTTP     1708 HTTP/1.1 200 OK  (image/vnd.microsoft.icon)
   133 24.355104322  192.168.88.128   117.18.237.29    OCSP      478 Request
   135 24.366743227  117.18.237.29    192.168.88.128   OCSP      793 Response
   324 25.652839949  192.168.88.128   180.149.59.209   HTTP      359 GET /openh264-linux64-2e1774ab6dc6c43debb0b5b628bdf1
```

```
▸ Frame 66: 932 bytes on wire (7456 bits), 932 bytes captured (7456 bits) on interface ens33, id 0
▸ Ethernet II, Src: VMware_fb:82:cd (00:50:56:fb:82:cd), Dst: VMware_f4:0c:48 (00:0c:29:f4:0c:48)
▸ Internet Protocol Version 4, Src: 188.184.21.108, Dst: 192.168.88.128
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 57958, Seq: 1, Ack: 353, Len: 878
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Fri, 23 Sep 2022 09:51:47 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: 0.162167007 seconds]
    [Request in frame: 64]
    [Request URI: http://info.cern.ch/]
    File Data: 646 bytes
▸ Line-based text data: text/html (13 lines)
```

- 2 Web Objects are downloaded. These 2 Web Objects are procured via 2 GET Requests as visible in the Screenshot above.
  The 2 Web Objects that are downloaded are a HTML Page and a Favicon
  They are downloaded over different TCP Connections
  We observe 2 different Source Ports used for requesting the 2 different Web Objects. For the first request we see that source port 57598 is used while for the second request source port 57962 is used.
- The HTTP Connection is Non-Persistent as we use 2 different ports to request for 2 different objects and the Connection attribute in the Response Packet is 'Close'



DataSave.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

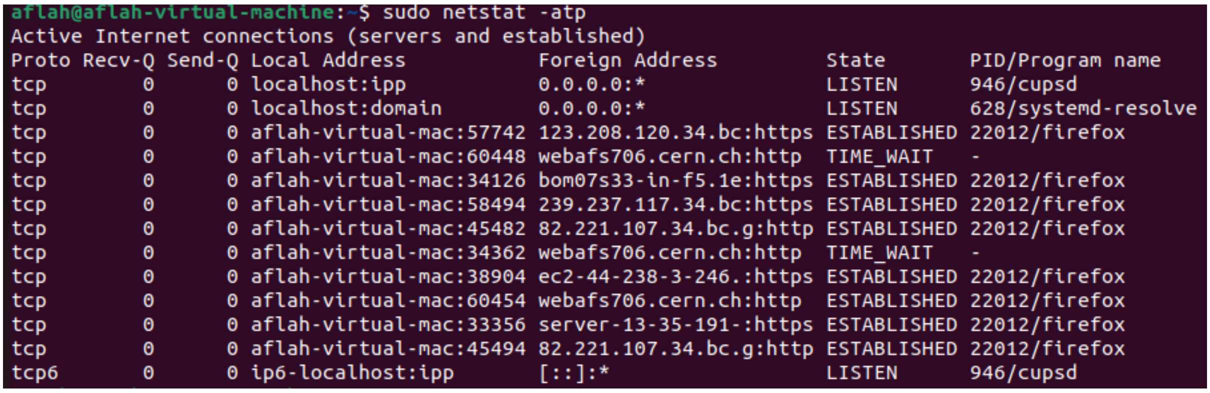
http

```
No.   Time          Source           Destination      Protocol Length Info
   25 0.363419377   192.168.88.128   104.18.32.68     OCSP      478 Request
   29 0.784198072   104.18.32.68     192.168.88.128   OCSP     1020 Response
   43 0.796460025   192.168.88.128   34.107.221.82    HTTP      355 GET /canonical.html HTTP/1.1
   45 0.804302950   34.107.221.82    192.168.88.128   HTTP      352 HTTP/1.1 200 OK  (text/html)
   56 0.816725792   192.168.88.128   34.107.221.82    HTTP      357 GET /success.txt?ipv4 HTTP/1.1
   58 0.825523790   34.107.221.82    192.168.88.128   HTTP      270 HTTP/1.1 200 OK  (text/plain)
   64 0.948055325   192.168.88.128   188.184.21.108   HTTP      406 GET / HTTP/1.1
   66 1.110222332   188.184.21.108   192.168.88.128   HTTP      932 HTTP/1.1 200 OK  (text/html)
   80 1.349508935   192.168.88.128   188.184.21.108   HTTP      358 GET /favicon.ico HTTP/1.1
   82 1.511539822   188.184.21.108   192.168.88.128   HTTP     1708 HTTP/1.1 200 OK  (image/vnd.microsoft.icon)
  133 24.355104322  192.168.88.128   117.18.237.29    OCSP      478 Request
  135 24.366743227  117.18.237.29    192.168.88.128   OCSP      793 Response
  324 25.652839949  192.168.88.128   180.149.59.209   HTTP      359 GET /openh264-linux64-2e1774ab6dc6c43debb0b5b62
```

```
Frame 66: 932 bytes on wire (7456 bits), 932 bytes captured (7456 bits) on interface ens33, id 0
Ethernet II, Src: VMware_fb:82:cd (00:50:56:fb:82:cd), Dst: VMware_f4:0c:48 (00:0c:29:f4:0c:48)
Internet Protocol Version 4, Src: 188.184.21.108, Dst: 192.168.88.128
Transmission Control Protocol, Src Port: 80, Dst Port: 57958, Seq: 1, Ack: 353, Len: 878
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      [HTTP/1.1 200 OK\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  Date: Fri, 23 Sep 2022 09:51:47 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: 0.162167007 seconds]
  [Request in frame: 64]
```

A6)

a) Command Used: netstat -atp



```
aflah@aflah-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      946/cupsd
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      628/systemd-resolve
tcp        0      0 aflah-virtual-mac:57742 123.208.120.34.bc:https ESTABLISHED 22012/firefox
tcp        0      0 aflah-virtual-mac:60448 webafs706.cern.ch:http  TIME_WAIT   -
tcp        0      0 aflah-virtual-mac:34126 bom07s33-in-f5.1e:https ESTABLISHED 22012/firefox
tcp        0      0 aflah-virtual-mac:58494 239.237.117.34.bc:https ESTABLISHED 22012/firefox
tcp        0      0 aflah-virtual-mac:45482 82.221.107.34.bc.g:http ESTABLISHED 22012/firefox
tcp        0      0 aflah-virtual-mac:34362 webafs706.cern.ch:http  TIME_WAIT   -
tcp        0      0 aflah-virtual-mac:38904 ec2-44-238-3-246.:https ESTABLISHED 22012/firefox
tcp        0      0 aflah-virtual-mac:60454 webafs706.cern.ch:http  ESTABLISHED 22012/firefox
tcp        0      0 aflah-virtual-mac:33356 server-13-35-191-:https ESTABLISHED 22012/firefox
tcp        0      0 aflah-virtual-mac:45494 82.221.107.34.bc.g:http ESTABLISHED 22012/firefox
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN      946/cupsd
```

This command lists all the active TCP Connections

b) The connection status is ESTABILISHED as seen in the terminal screenshot