# CSE 232: Assignment 2

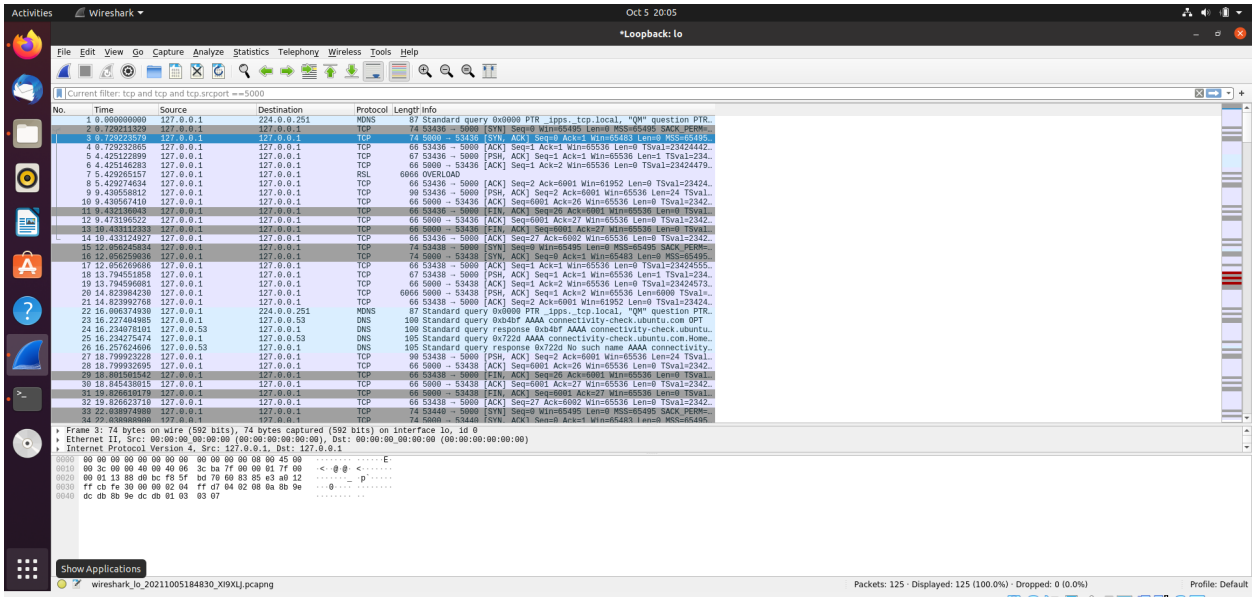
## Name - Utkarsh Dubey

## Roll no - 2019213

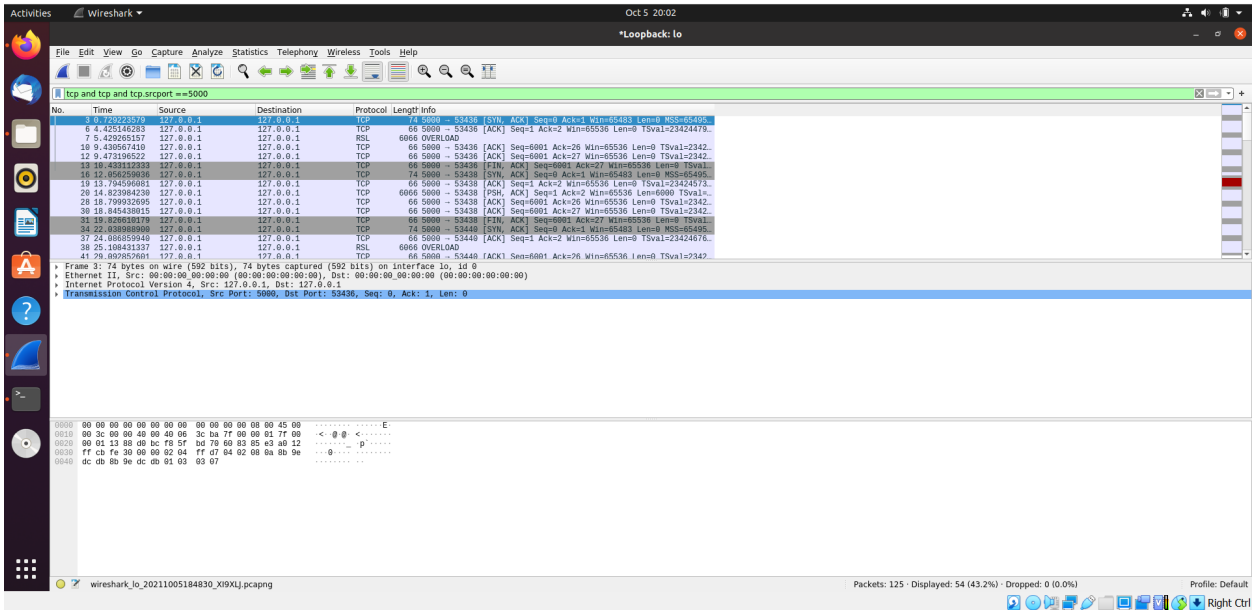
## Question 1 -

Started server and client programs for 2 mins

Wireshark packet collection




Applying filters -



Plot -

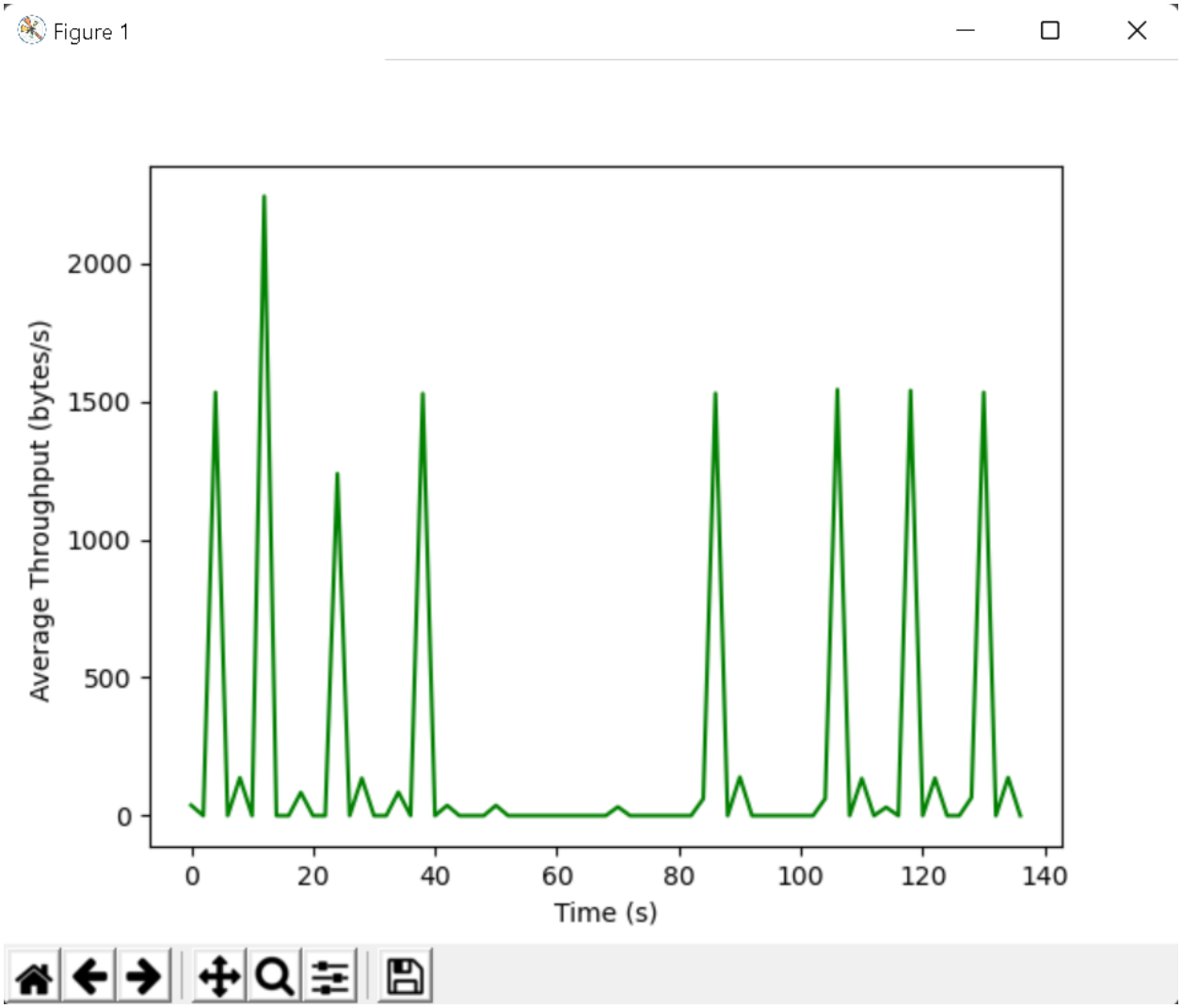


Figure 1
Average Throughput (bytes/s)
2000
1500
1000
500
0
0
20
40
60
80
100
120
140
Time (s)

**Question 2 -**

- We received 4 packets of HTTP type when we loaded the given site.

  First Packet

  Http request type - GET
  User-agent type - Mozilla/5.0
  Name and version of web browser - Chrome/94.0.4606.71

  Second Packet

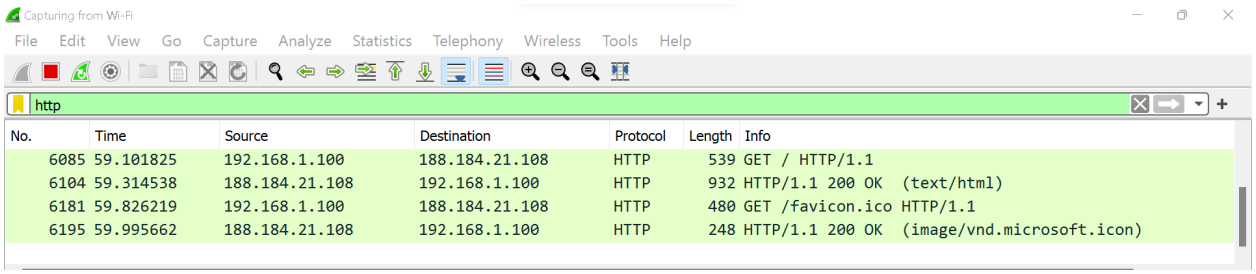
  Http code response - 200
  Http response description - OK

  Third Packet

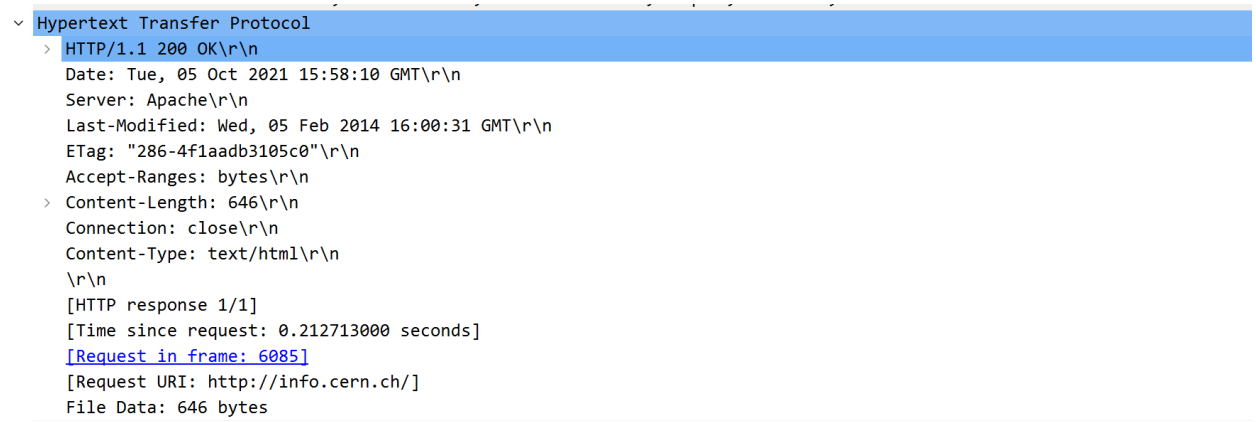
  Http request type - GET
  User agent type - Mozilla/5.0
  Name and version of web browser - Chrome/94.0.4606.71

  Fourth Packet

  Http code response - 200
  Http response description - OK


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
6085 59.101825 192.168.1.100 188.184.21.108 HTTP 539 GET / HTTP/1.1
6104 59.314538 188.184.21.108 192.168.1.100 HTTP 932 HTTP/1.1 200 OK (text/html)
6181 59.826219 192.168.1.100 188.184.21.108 HTTP 480 GET /favicon.ico HTTP/1.1
6195 59.995662 188.184.21.108 192.168.1.100 HTTP 248 HTTP/1.1 200 OK (image/vnd.microsoft.icon)


Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: info.cern.ch\r\n
Connection: keep-alive\r\n
Pragma: no-cache\r\n
Cache-Control: no-cache\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.71 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
Sec-GPC: 1\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://info.cern.ch/]
[HTTP request 1/1]
[Response in frame: 6104]


Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Tue, 05 Oct 2021 15:58:10 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: 0.212713000 seconds]
[Request in frame: 6085]
[Request URI: http://info.cern.ch/]
File Data: 646 bytes

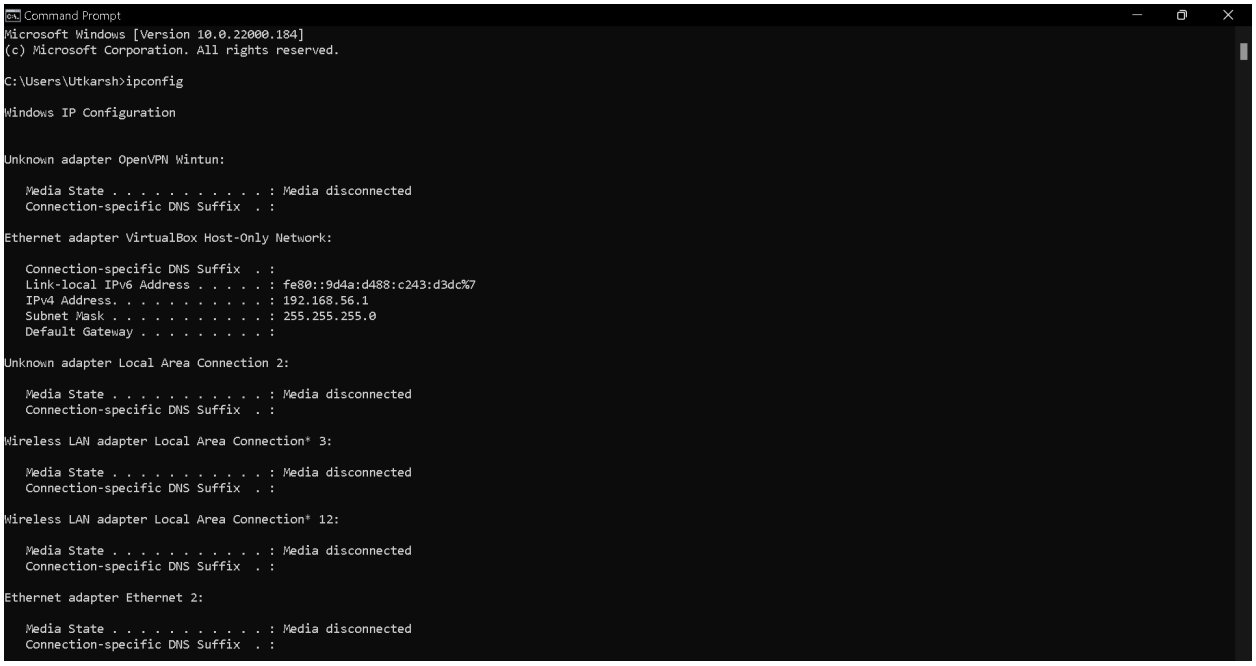

Hypertext Transfer Protocol
GET /favicon.ico HTTP/1.1\r\n
Host: info.cern.ch\r\n
Connection: keep-alive\r\n
Pragma: no-cache\r\n
Cache-Control: no-cache\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.71 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
Sec-GPC: 1\r\n
Referer: http://info.cern.ch/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://info.cern.ch/favicon.ico]
[HTTP request 1/1]
[Response in frame: 6195]

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Tue, 05 Oct 2021 15:58:11 GMT\r\n
  Server: Apache\r\n
  Last-Modified: Fri, 18 Jan 2008 15:26:11 GMT\r\n
  ETag: "57e-44400c31d2ac0"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 1406\r\n
  Connection: close\r\n
  Content-Type: image/vnd.microsoft.icon\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.169443000 seconds]
  [Request in frame: 6181]
  [Request URI: http://info.cern.ch/favicon.ico]
  File Data: 1406 bytes
```

# Question 3

Ans a -

Windows  (ipconfig is equivalent of ifconfig in windows)



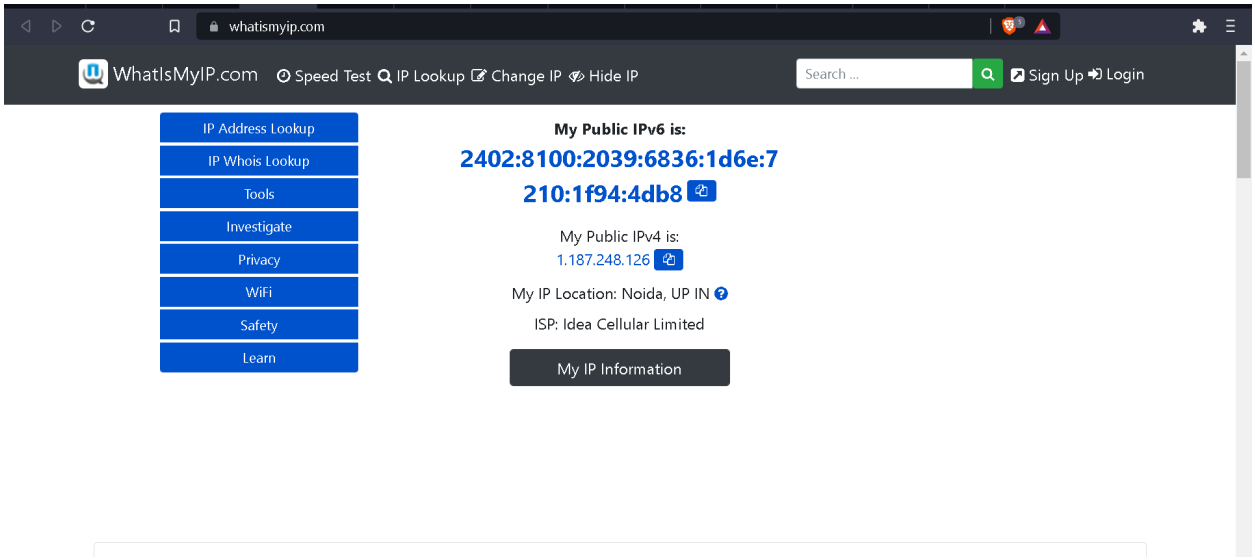
```
Wireless LAN adapter Local Area Connection* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2402:8100:2039:6836:3cc1:8367:5a9a:8eee
   Temporary IPv6 Address. . . . . . : 2402:8100:2039:6836:1d6e:7210:1f94:4db8
   Link-local IPv6 Address . . . . . : fe80::3cc1:8367:5a9a:8eee%18
   IPv4 Address. . . . . . . . . . . : 192.168.58.127
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::b8a8:74ff:feb5:6135%18
                                       192.168.58.192

C:\Users\Utkarsh>
```

Ubuntu (ifconfig)

```
utkarsh@utkarsh-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::79ce:c25f:5a8e:4d7b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e1:3f:72  txqueuelen 1000  (Ethernet)
        RX packets 43694  bytes 61416395 (61.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11682  bytes 753934 (753.9 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 226  bytes 21817 (21.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 226  bytes 21817 (21.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Observation - we see many IP addresses for different network adapters like ethernet and wifi.

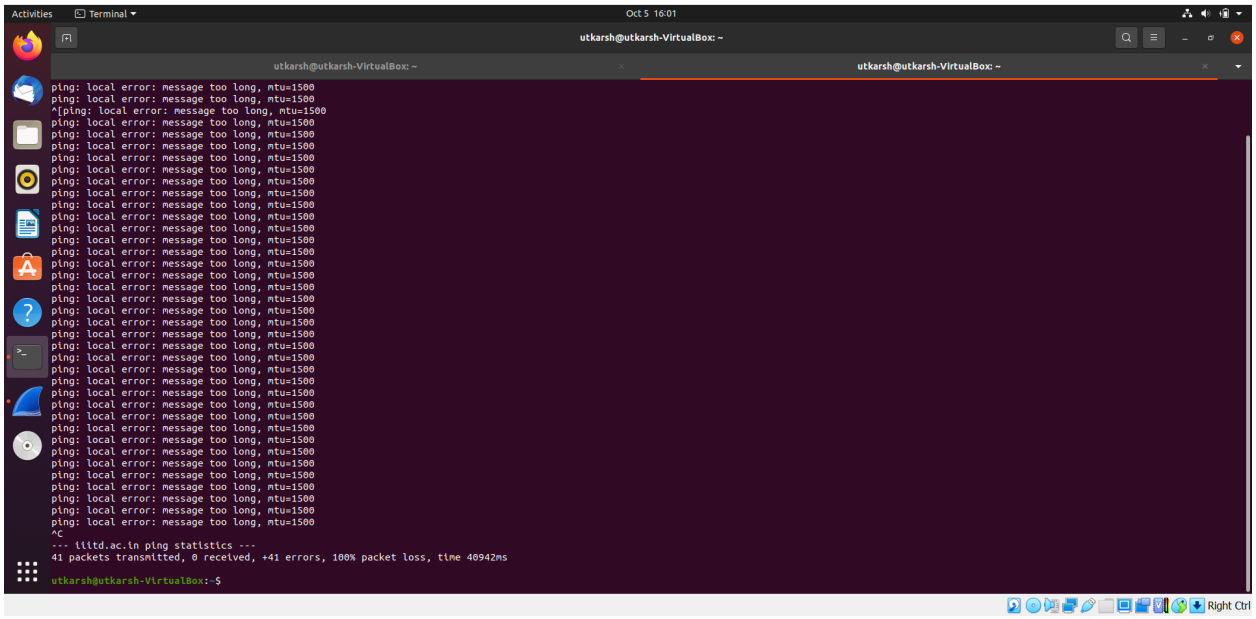
Ans b -




They are different, as what I see on the website is my public IP and what I see on the terminal is my private IP which is of local my machine.
It is different because my local machine uses its IP to connect to the router for and router then connect to a bigger network like an ISP, which has its own IP and that IP is used to further connect to the websites.

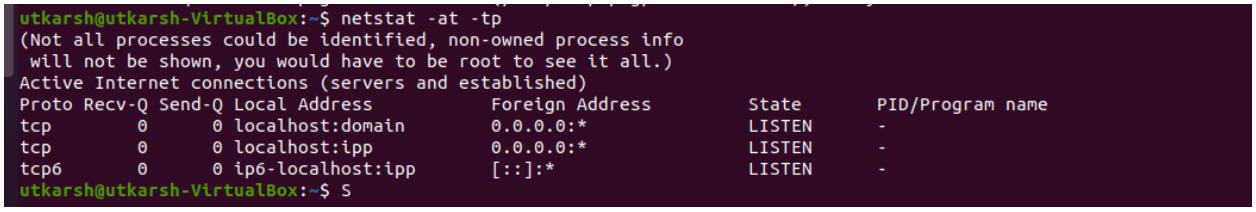
## Question 4 -

Ans a -
Command - ping www.iiitd.ac.in -M do -s 2972
2972 for 3000 bytes




The standard MTU size is 1500 bytes, that's why even after sending 3000bytes we can observe a mtu of 1500.
Hence we can't send a packet with mtu 3000.

Ans b -
Command - netstat -at -tp



## Question 5-

Ans a -

```
utkarsh@utkarsh-VirtualBox:~$ nslookup -type=soa instagram.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
instagram.com
        origin = ns-384.awsdns-48.com
        mail addr = awsdns-hostmaster.amazon.com
        serial = 3
        refresh = 7200
        retry = 900
        expire = 1209600
        minimum = 3600

Authoritative answers can be found from:

utkarsh@utkarsh-VirtualBox:~$ nslookup instagram.com ns-384.awsdns-48.com
Server:         ns-384.awsdns-48.com
Address:        205.251.193.128#53

Name:   instagram.com
Address: 31.13.71.174
Name:   instagram.com
Address: 2a03:2880:f203:1e6:face:b00c:0:4420
```

Mostly is we do nslookup on popular websites, we will end up getting a non-authoritative response.
Now in order to get their authoritative response, we need to specify the origin server and we got the origin server by using -type=soa flag
then we ran nslookup on that server, in the case of Instagram it was ns-384.awsdns-48.com

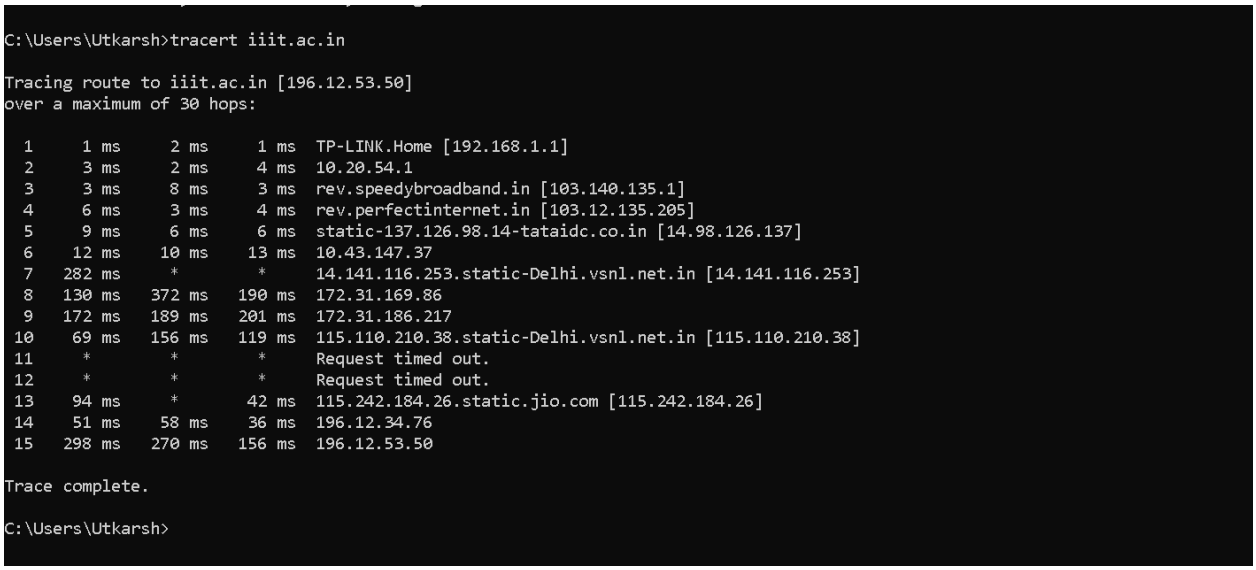
Ans b -

```
C:\Users\Utkarsh>nslookup -type=soa www.instagram.com
Server:  TP-LINK.Home
Address:  192.168.1.1

Non-authoritative answer:
www.instagram.com       canonical name = z-p42-instagram.c10r.instagram.com

c10r.instagram.com
        primary name server = a.ns.c10r.instagram.com
        responsible mail addr = dns.facebook.com
        serial  = 1633454345
        refresh = 300 (5 mins)
        retry   = 600 (10 mins)
        expire  = 600 (10 mins)
        default TTL = 300 (5 mins)
```

We got TTL of 5mins, meaning that it will expire in 5 mins. TTL stands for time to live and it is an expiration time on DNS record.

## Question 6 -

Ans a -



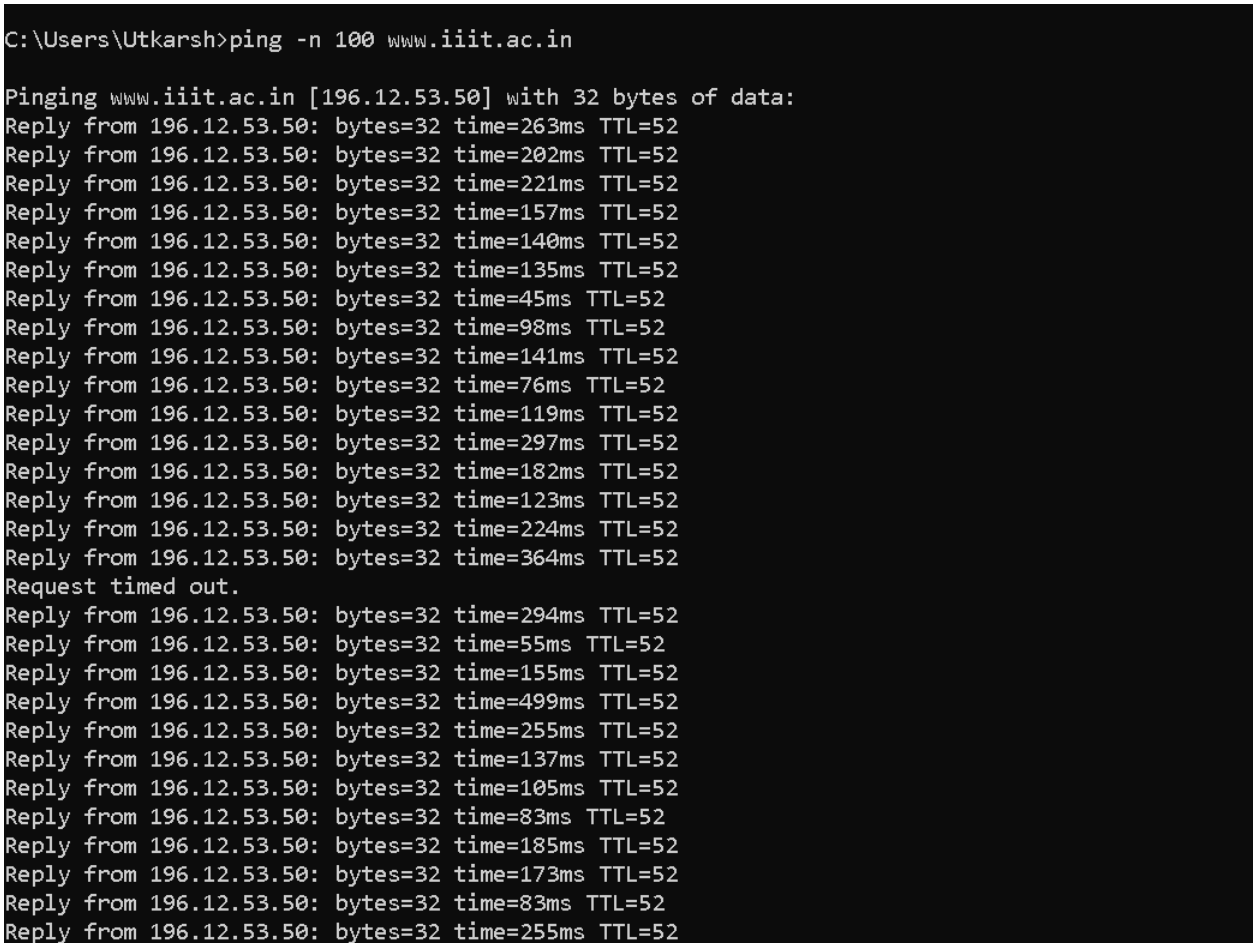
```
C:\Users\Utkarsh>tracert iiit.ac.in

Tracing route to iiit.ac.in [196.12.53.50]
over a maximum of 30 hops:

  1     1 ms     2 ms     1 ms  TP-LINK.Home [192.168.1.1]
  2     3 ms     2 ms     4 ms  10.20.54.1
  3     3 ms     8 ms     3 ms  rev.speedybroadband.in [103.140.135.1]
  4     6 ms     3 ms     4 ms  rev.perfectinternet.in [103.12.135.205]
  5     9 ms     6 ms     6 ms  static-137.126.98.14-tataidc.co.in [14.98.126.137]
  6    12 ms    10 ms    13 ms  10.43.147.37
  7   282 ms     *        *     14.141.116.253.static-Delhi.vsnl.net.in [14.141.116.253]
  8   130 ms   372 ms   190 ms  172.31.169.86
  9   172 ms   189 ms   201 ms  172.31.186.217
 10    69 ms   156 ms   119 ms  115.110.210.38.static-Delhi.vsnl.net.in [115.110.210.38]
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13    94 ms     *       42 ms  115.242.184.26.static.jio.com [115.242.184.26]
 14    51 ms    58 ms    36 ms  196.12.34.76
 15   298 ms   270 ms   156 ms  196.12.53.50

Trace complete.

C:\Users\Utkarsh>
```

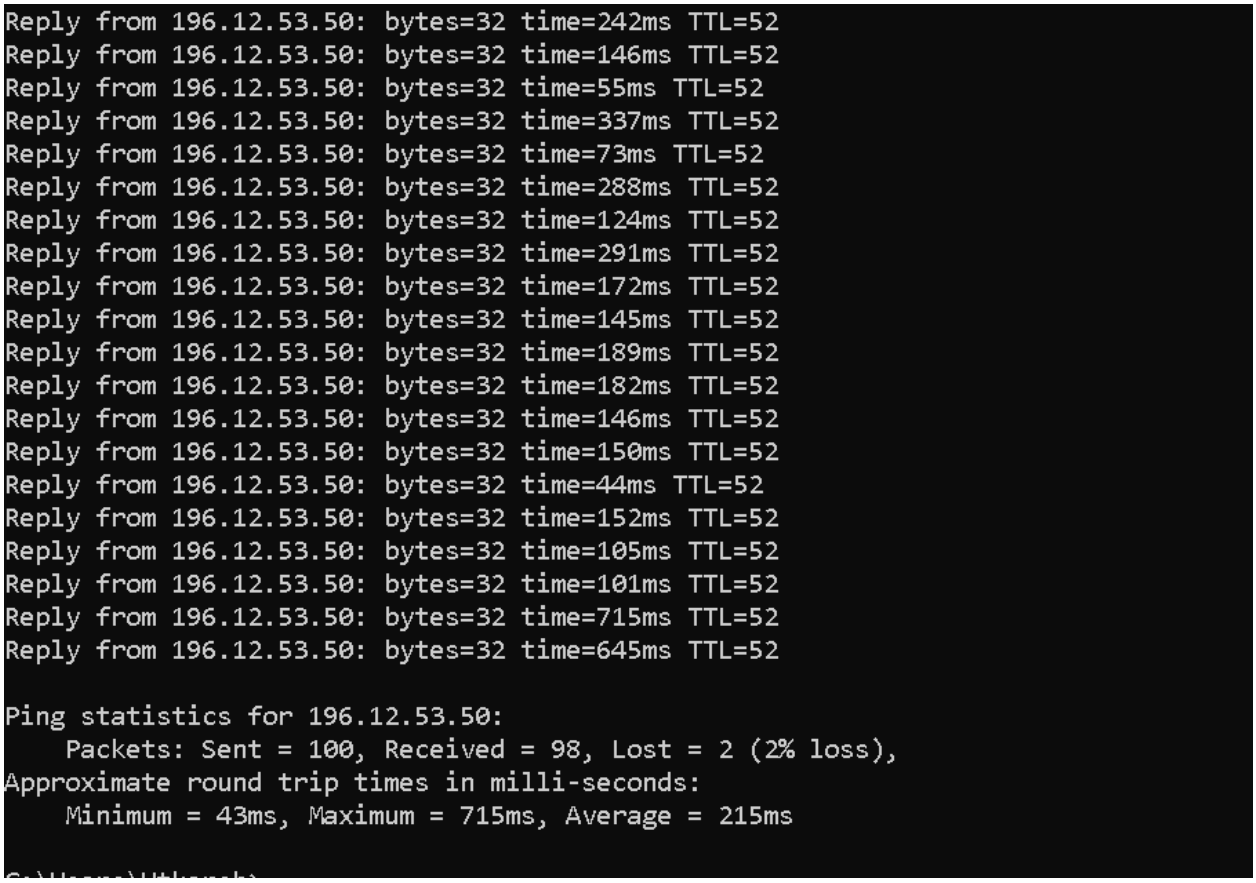
Average latency of each intermediate host -

1- TP-LINK.Home [192.168.1.1] = (1+2+1)/3 = 1.33ms
2 - 10.20.54.1 = (3+2+4)/3 = 3ms
3 - rev.speedybroadband.in [103.140.135.1] = (3+8+3)/3 = 4.66ms
4 - rev.perfectinternet.in [103.12.135.205] = (6+3+4)/3 = 4.33ms
5 - static-137.126.98.14-tataidc.co.in [14.98.126.137] = (9+6+6)/3 = 7 ms
6 - 10.43.147.37 =(12+10+13)/3 = 8.33ms
7 - 115.110.210.38.static-Delhi.vsnl.net.in [115.110.210.38] = (69+156+119)/3 = 114.66ms

8- 115.242.184.26.static.jio.com [115.242.184.26] = (94+42)/2 = 68ms
9 - 196.12.34.76 = (51+58+36)/3 = 48.33ms
10 - 196.12.53.50 = (298+270+156)/3 = 241.33ms

Ans b -






Average latency = 215ms

Ans c -

After adding all the intermediate latency in part we get 1200.96ms.
This is way different from the average latency we got in part b which was 215ms.
This is because the latency in part a between intermediate host is a round trip time of packet to get to that host and back to my computer, hence we can’t directly add the latency of intermediate to get the return time to the final host.

Ans d -
The maximum latency value I got in part a was 114.66 ms and the average in part b is 215ms.
Hence we observe they are not same.
This is happening because we might not have bottlenecks, and the latency gradually increases as we go along, Hence we only get the average latency of the host almost similar to that in part b

Ans e -

```
C:\Users\Utkarsh>nslookup 192.168.1.1
Server:  TP-LINK.Home
Address:  192.168.1.1

Name:    TP-LINK.Home
Address:  192.168.1.1


C:\Users\Utkarsh>nslookup 10.20.54.1
Server:  TP-LINK.Home
Address:  192.168.1.1

*** TP-LINK.Home can't find 10.20.54.1: Non-existent domain

C:\Users\Utkarsh>nslookup 103.140.135.1
Server:  TP-LINK.Home
Address:  192.168.1.1

Name:    rev.speedybroadband.in
Address:  103.140.135.1


C:\Users\Utkarsh>nslookup 103.12.135.205
Server:  TP-LINK.Home
Address:  192.168.1.1

Name:    rev.perfectinternet.in
Address:  103.12.135.205
```

```
C:\Users\Utkarsh>nslookup 14.98.126.137
Server:  TP-LINK.Home
Address:  192.168.1.1

Name:    static-137.126.98.14-tataidc.co.in
Address:  14.98.126.137


C:\Users\Utkarsh>nslookup 14.141.116.253
Server:  TP-LINK.Home
Address:  192.168.1.1

Name:    14.141.116.253.static-Delhi.vsnl.net.in
Address:  14.141.116.253


C:\Users\Utkarsh>nslookup 172.31.169.86
Server:  TP-LINK.Home
Address:  192.168.1.1

*** TP-LINK.Home can't find 172.31.169.86: Non-existent domain

C:\Users\Utkarsh>nslookup 172.31.186.217
Server:  TP-LINK.Home
Address:  192.168.1.1

DNS request timed out.
    timeout was 2 seconds.
*** Request to TP-LINK.Home timed-out

C:\Users\Utkarsh>nslookup 115.110.210.38
Server:  TP-LINK.Home
Address:  192.168.1.1

Name:    115.110.210.38.static-Delhi.vsnl.net.in
Address:  115.110.210.38
```

```
C:\Users\Utkarsh>nslookup 196.12.34.76
Server:  TP-LINK.Home
Address:  192.168.1.1

*** TP-LINK.Home can't find 196.12.34.76: Non-existent domain

C:\Users\Utkarsh>nslookup 196.12.53.50
Server:  TP-LINK.Home
Address:  192.168.1.1

*** TP-LINK.Home can't find 196.12.53.50: Non-existent domain

C:\Users\Utkarsh>
```

```
C:\Users\Utkarsh>nslookup 115.242.184.26
Server:  TP-LINK.Home
Address:  192.168.1.1

Name:    115.242.184.26.static.jio.com
Address:  115.242.184.26
```

```
C:\Users\Utkarsh>nslookup 10.43.147.37
Server:  TP-LINK.Home
Address:  192.168.1.1

*** TP-LINK.Home can't find 10.43.147.37: Non-existent domain
```

## Question 7

Disabled the looping interface using ifconfig lo down and this causes the driver to shut down.

```
utkarsh@utkarsh-VirtualBox:~$ sudo ifconfig lo down
[sudo] password for utkarsh:
```

and then pinging the localhost

```
utkarsh@utkarsh-VirtualBox:~$ 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 ---
168 packets transmitted, 0 received, 100% packet loss, time 171810ms

utkarsh@utkarsh-VirtualBox:~$
```

As we can see, we got 100% packet loss