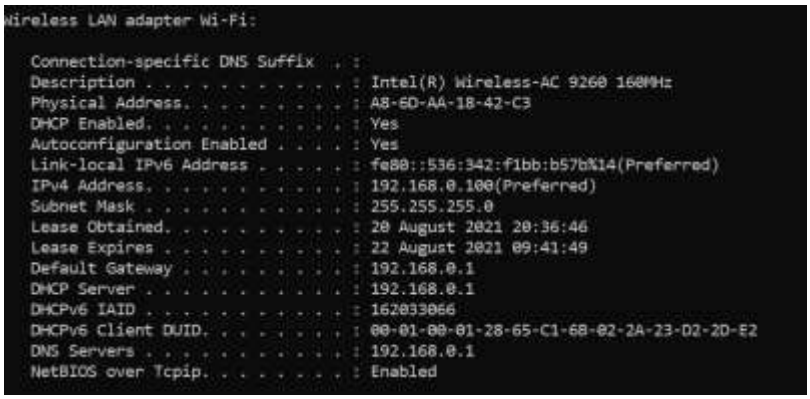
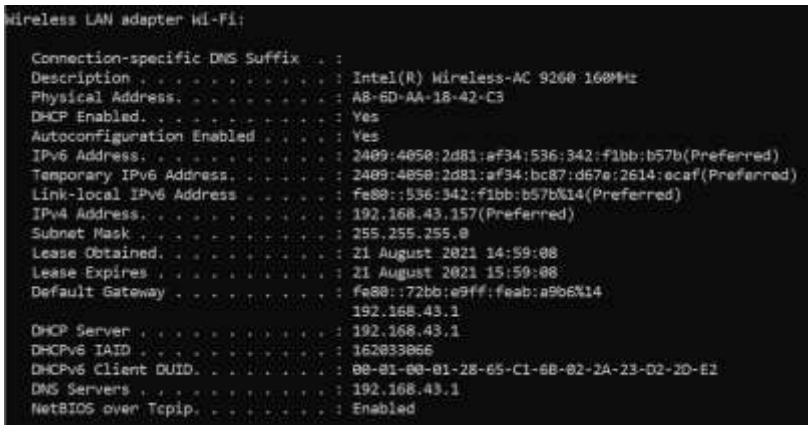
Name: Mohit Sharma Entry Number: 2019CS10372

1: Networking Tools

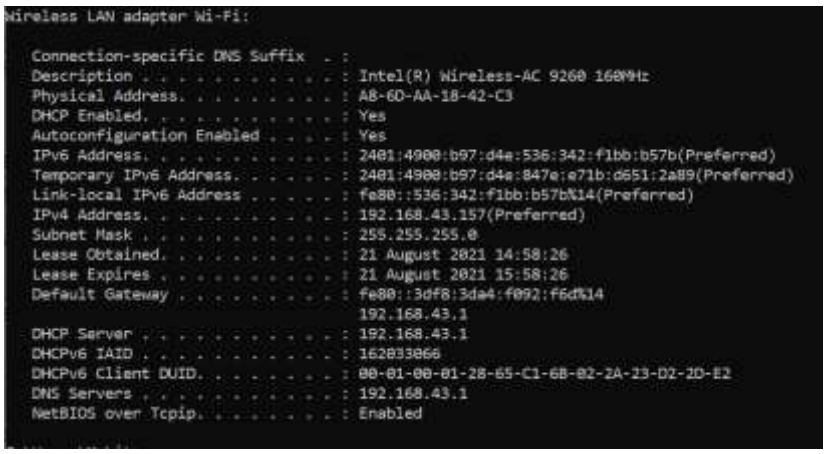
a) IPv4 address from Balaji Wi-Fi connection: 192.168.0.100



IPv4 address from JIO hotspot connection: 192.168.43.157



IPv4 address from AIRTEL hotspot connection (different mobile used): 192.168.43.157



The IP address is given to our machine by the internet service provider(ISP) and hence it is subject to change with change in ISP.

b) IP address for www.google.com :
On various run of the command the IP address come one of the following every time
142.250.77.228 or 142.250.194.164
(Even after using open DNS the same thing happened)

```
C:\WINDOWS\system32>nslookup www.google.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4002:823::2004
          142.250.77.228


C:\WINDOWS\system32>nslookup www.google.com 208.67.222.222
Server:  resolver1.opendns.com
Address:  208.67.222.222

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4002:823::2004
          142.250.194.164


C:\WINDOWS\system32>nslookup www.google.com 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4002:823::2004
          142.250.77.228
```

```
C:\WINDOWS\system32>nslookup www.google.com 208.67.222.222
Server:  dns.umbrella.com
Address:  208.67.222.222

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4002:823::2004
          142.250.77.228


C:\WINDOWS\system32>nslookup www.google.com
Server:  UnKnown
Address:  192.168.0.1

Name:    www.google.com
Addresses:  2404:6800:4002:823::2004
          142.250.194.164


C:\WINDOWS\system32>nslookup www.google.com 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4002:823::2004
          142.250.194.164
```

IP address for www.facebook.com :
With or without changing the DNS, the IP address always came to be 157.240.198.35

```
C:\WINDOWS\system32>nslookup www.facebook.com 208.67.222.222
Server:  resolver1.opendns.com
Address:  208.67.222.222

Non-authoritative answer:
Name:    star-mini.c10r.facebook.com
Addresses:  2a03:2880:f144:82:face:b00c:0:25de
          157.240.198.35
Aliases:  www.facebook.com


C:\WINDOWS\system32>nslookup www.facebook.com
Server:  UnKnown
Address:  192.168.0.1

Name:    star-mini.c10r.facebook.com
Addresses:  2a03:2880:f144:82:face:b00c:0:25de
          157.240.198.35
Aliases:  www.facebook.com


C:\WINDOWS\system32>nslookup www.facebook.com 8.8.8.8
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  8.8.8.8

Non-authoritative answer:
Name:    star-mini.c10r.facebook.com
Addresses:  2a03:2880:f144:82:face:b00c:0:25de
          157.240.198.35
Aliases:  www.facebook.com
```

(
8.8.8.8 is Google DNS
208.67.222.222 is OpenDNS
)

c) Using ping command

Flags used:

-n count : sets number of packets to be sent (default 4)

-l size : sets size of packet (default 32)

-i TTL : sets Time to Live

For www.iitd.ac.in :

The max packet size that I was able to send was around 34000 bytes. Actually, it was not fixed, sometimes a packet of 35000 bytes gave output properly but some times it showed Request timed out.

The minimum ttl value required was 13.

```
C:\Users\Mohit>ping -n 1 -i 13 www.iitd.ac.in

Pinging www.iitd.ac.in [103.27.9.24] with 32 bytes of data:
Reply from 103.27.9.24: bytes=32 time=6ms TTL=51

Ping statistics for 103.27.9.24:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 6ms, Average = 6ms

C:\Users\Mohit>ping -n 1 -i 12 www.iitd.ac.in

Pinging www.iitd.ac.in [103.27.9.24] with 32 bytes of data:
Reply from 103.27.9.24: TTL expired in transit.

Ping statistics for 103.27.9.24:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

For www.google.com :

The max packet size that I was able to send was 1472 bytes.

The minimum ttl value required was 8.

```
C:\Users\Mohit>ping -n 1 -i 8 www.google.com

Pinging www.google.com [142.250.77.228] with 32 bytes of data:
Reply from 142.250.77.228: bytes=32 time=16ms TTL=119

Ping statistics for 142.250.77.228:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 16ms, Average = 16ms

C:\Users\Mohit>ping -n 1 -i 7 www.google.com

Pinging www.google.com [142.250.77.228] with 32 bytes of data:
Reply from 142.251.54.75: TTL expired in transit.

Ping statistics for 142.250.77.228:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

For www.facebook.com :
The max packet size that I was able to send was 1472 bytes.
The minimum ttl value required was 8.

```
C:\Users\Mohit>ping -n 1 -i 7 www.facebook.com

Pinging star-mini.c10r.facebook.com [157.240.198.35] with 32 bytes of data:
Reply from 157.240.38.131: TTL expired in transit.

Ping statistics for 157.240.198.35:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),

C:\Users\Mohit>ping -n 1 -i 8 www.facebook.com

Pinging star-mini.c10r.facebook.com [157.240.198.35] with 32 bytes of data:
Reply from 157.240.198.35: bytes=32 time=3ms TTL=57

Ping statistics for 157.240.198.35:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 3ms, Average = 3ms
```

(The minimum ttl values mentioned above changes on using different service provider.
This TTL value is of the received packet and is not controlled by us, whenever the packet is passed through a router the TTL value is decreased by a minimum of 1)

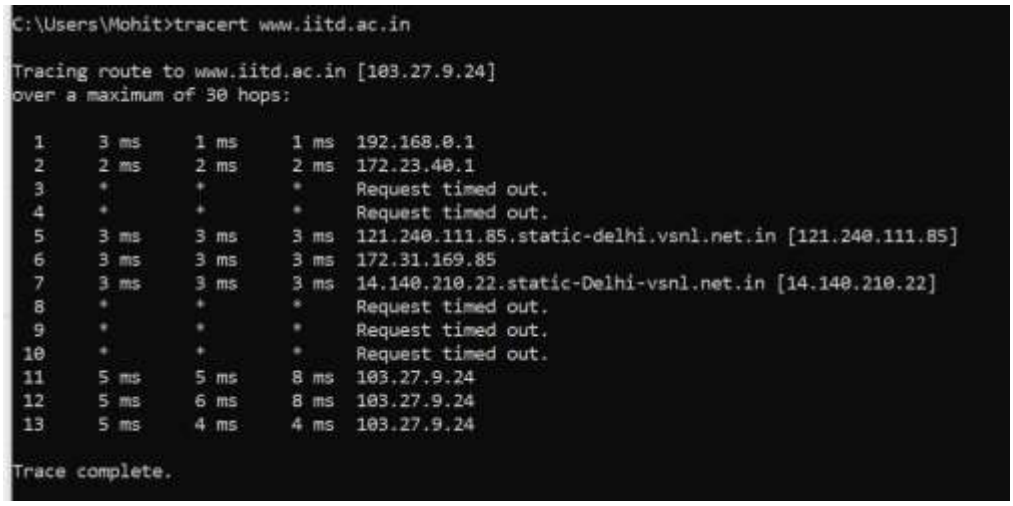
** For google and facebook domains, the max packet size was consistent to be 1472 bytes.
To automate the process of finding this max ping packet size, I binary searched the result using following code: (To run: python filename hostname)

```python
import sys
import subprocess
def ping(host, num):
  param1 = '-n'
  param2 = '-l'
  command = ['ping', param1, '1', param2, str(num), host]
  return subprocess.call(command) == 0


def check(host, mid):
  flag = True
```

```
  for x in range(5):
    flag = flag and ping(host,mid)
  return flag

def bsearch(host, low, high):
  if(high-low <= 1):
    return low
  mid = (low + high)//2
  flag = check(host, mid)
  if not flag:
    return bsearch(host, low, mid)
  else:
    return bsearch(host, mid, high)

def maxSize(host):
  low = 0
  high = 65501
  return bsearch(host, low, high)

args = sys.argv
host = args[1]
# host = "www.iitd.ac.in"
print("Max packet size is: ", maxSize(host))
```

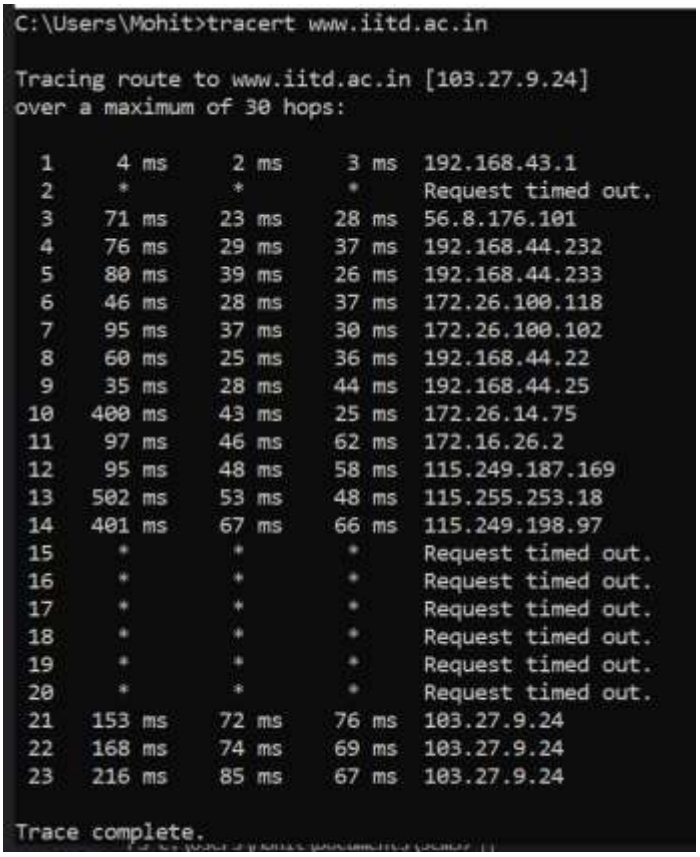
The maximum allowed packet size is not same for all domains as we can see that the maximum allowed packet size for google.com and facebook.com is much lower than that of iitd.ac.in. This is something that depends on the domains itself as how much data flow they want to allow.

d) With Balaji Wi-fi Connection:



```
C:\Users\Mohit>tracert www.iitd.ac.in

Tracing route to www.iitd.ac.in [103.27.9.24]
over a maximum of 30 hops:

  1     3 ms     1 ms     1 ms  192.168.0.1
  2     2 ms     2 ms     2 ms  172.23.40.1
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     3 ms     3 ms     3 ms  121.240.111.85.static-delhi.vsnl.net.in [121.240.111.85]
  6     3 ms     3 ms     3 ms  172.31.169.85
  7     3 ms     3 ms     3 ms  14.140.210.22.static-Delhi-vsnl.net.in [14.140.210.22]
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     5 ms     5 ms     8 ms  103.27.9.24
 12     5 ms     6 ms     8 ms  103.27.9.24
 13     5 ms     4 ms     4 ms  103.27.9.24

Trace complete.
```

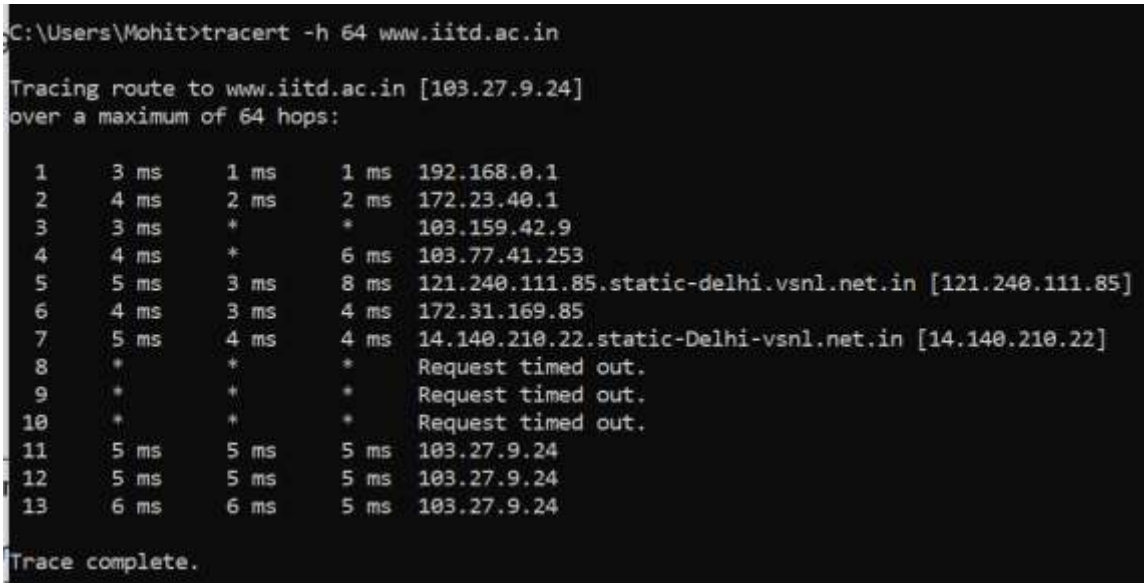
With Jio hotspot Connection:



```
C:\Users\Mohit>tracert www.iitd.ac.in

Tracing route to www.iitd.ac.in [103.27.9.24]
over a maximum of 30 hops:

  1     4 ms     2 ms     3 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3    71 ms    23 ms    28 ms  56.8.176.101
  4    76 ms    29 ms    37 ms  192.168.44.232
  5    80 ms    39 ms    26 ms  192.168.44.233
  6    46 ms    28 ms    37 ms  172.26.100.118
  7    95 ms    37 ms    30 ms  172.26.100.102
  8    60 ms    25 ms    36 ms  192.168.44.22
  9    35 ms    28 ms    44 ms  192.168.44.25
 10   400 ms    43 ms    25 ms  172.26.14.75
 11    97 ms    46 ms    62 ms  172.16.26.2
 12    95 ms    48 ms    58 ms  115.249.187.169
 13   502 ms    53 ms    48 ms  115.255.253.18
 14   401 ms    67 ms    66 ms  115.249.198.97
 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   153 ms    72 ms    76 ms  103.27.9.24
 22   168 ms    74 ms    69 ms  103.27.9.24
 23   216 ms    85 ms    67 ms  103.27.9.24

Trace complete.
```

The ttl for the hopes can be increased (using “-h ttl_value” flag) to make some of the missing routers to reply.

Like when I set the ttl value to 64 the missing router at hop 3 and 4 reply (in first network: Balaji Wi-fi)



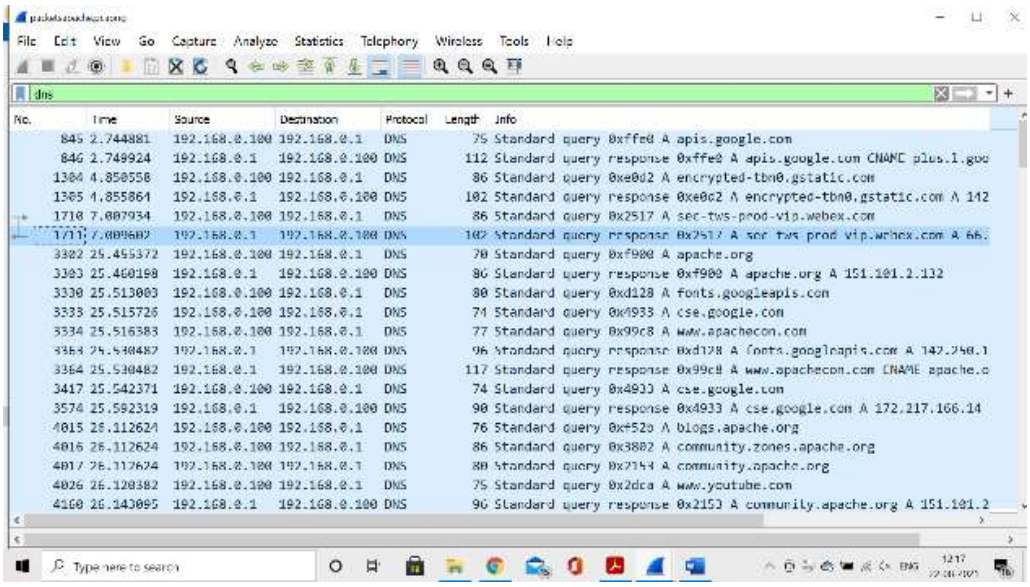
There are still some routers that do not reply to the request (even with ttl value set to 255). This can be because of some firewall blocking access to them, or may be the return path from the router may be different and there may be some problem in that path.

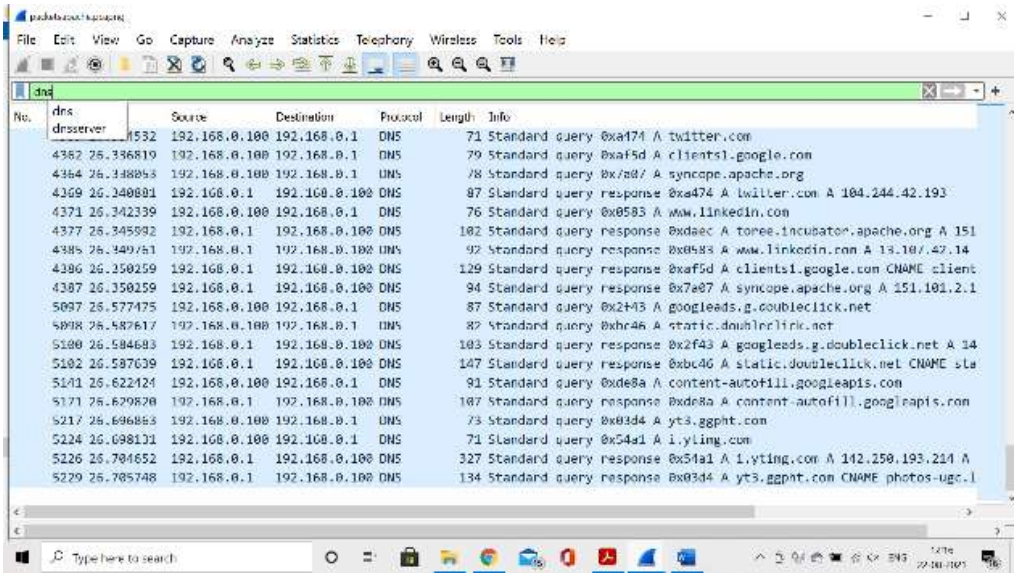
To force tracert to use IPv4 address, we can use the -4 flag in the command as tracert -4 www.google.com
For www.iitd.ac.in all the IP address were already default to IPv4 and hence change was not needed

2: Packet analysis

Captured Packets for http://apache.org for part a, b, c.

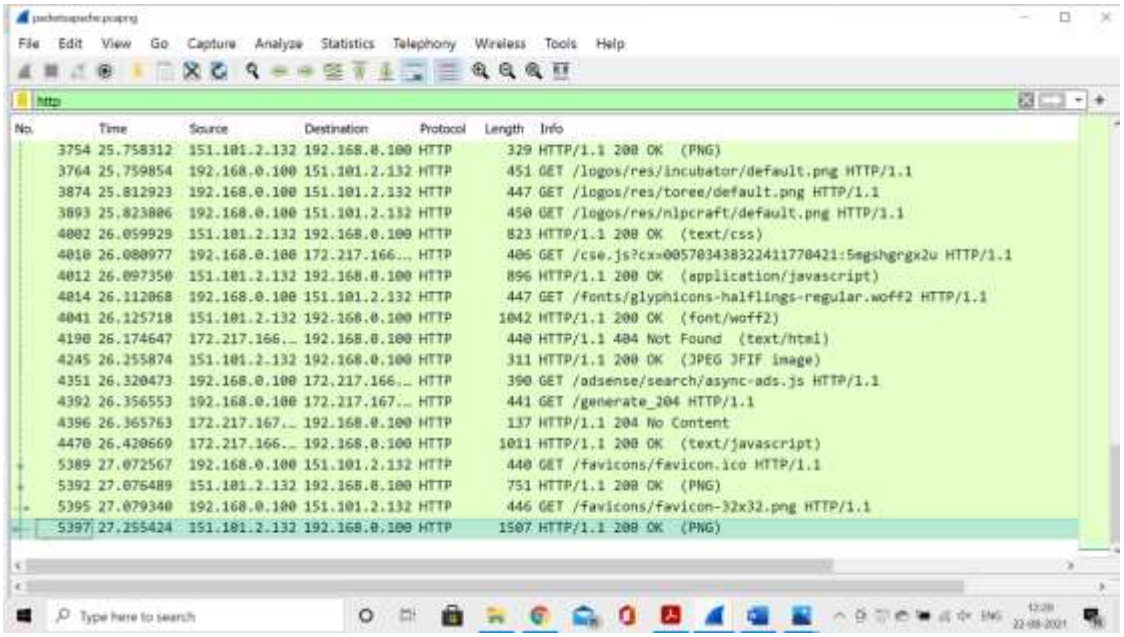
a) The first DNS protocol request was captured at 25.455372 seconds and the last was at 25.460198 seconds. So, the total time taken for DNS request-response was 0.004826 seconds.





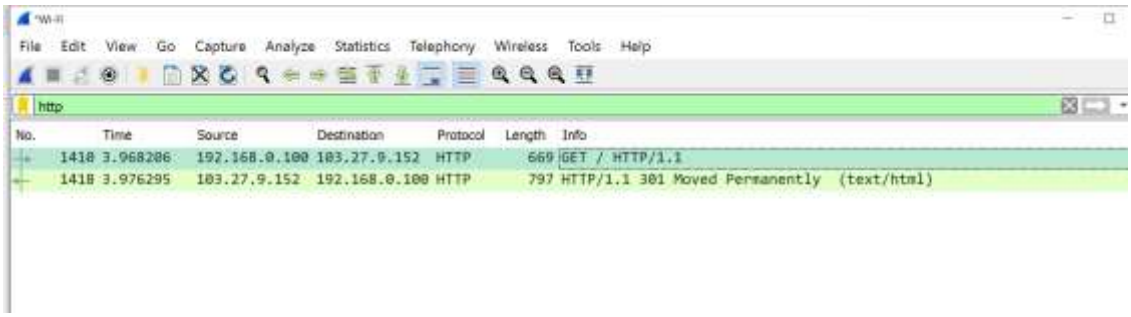
b) A total of 51 queries were captured with http protocol.
The webpages consist of a lot of files and for each file browsers need to make an http request to get the data. CSS, JS, Images, Docs all these data are fragmented and are retrieved when the web page is to be rendered through http requests.

c) The first DNS protocol request was captured at 25.455372 seconds.
The last http request was captured at 27.255424 seconds.
So, the total time taken to load the web page is 1.800052 seconds.



Captured Packets for http://www.cse.iitd.ac.in for part d.

d) Only two HTTP protocol packets were captured for the website. No other http traffic was found as out http search was redirected to https through the servers which is serving the required domain.



There are only two http request because all other required data is fetched through https requests and not http requests.

3: Implement Traceroute Using Ping

a) Output of program:

```
PS C:\Users\Mohit\Documents\sem5> python rtt.py www.iitd.ac.in
tracert using ping for  www.iitd.ac.in

Hop      RTT     IP Address

1        1       192.168.0.1
2        2       172.23.40.1
3        0       *
4        0       *
5        3       121.240.111.85
6        0       172.31.169.85
7        4       14.140.210.22
8        0       *
9        0       *
10       0       *
11       6       103.27.9.24
12       4       103.27.9.24
13       5       103.27.9.24
PS C:\Users\Mohit\Documents\sem5>
```

b) RTT vs Hop plot: