CN Assignment - 2

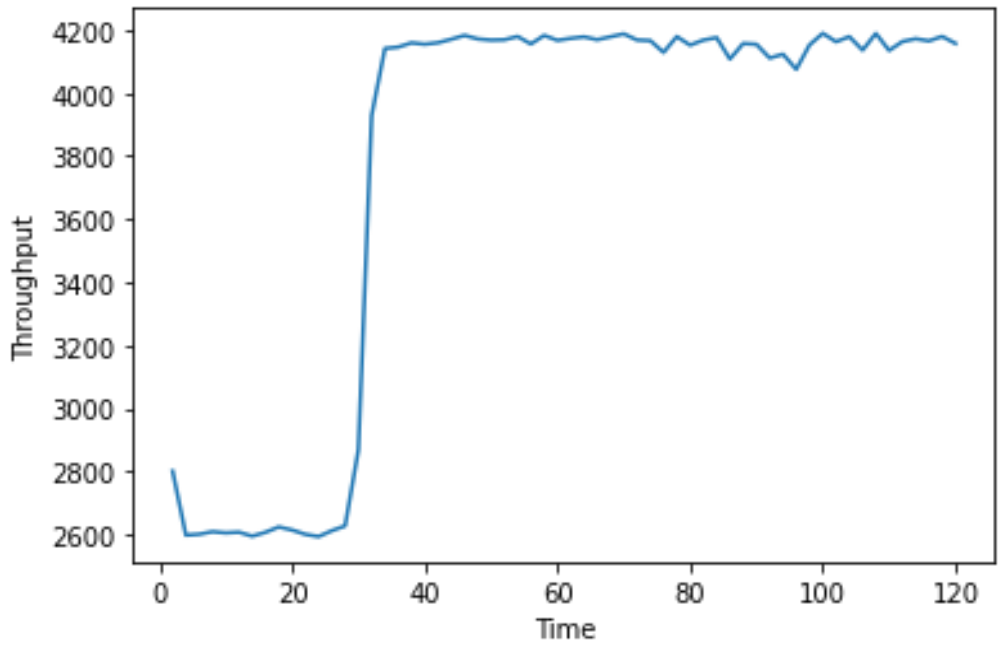
Samyak Jain, 2019098

Q1

Firstly, I capture the packets using tcpdump [sudo tcpdump -i lo port 3000 -s 65535 -w Q1_OP.pcap] and then filter out the TCP packets using a filter in Wireshark such that I only get the packets for server side (sent by server side).
[filter : tcp.srcport == 3000] (3000 is my server port)

Then I compute the aggregate throughput every two seconds using the way that I compute the number of bytes sent in that interval of two seconds and divide it by the time in that interval (endtime - starttime).

Note that: In the graphs, on Y-axis we have the throughput (in bytes/second) and on the x-axis, we have the time (in seconds)



From the plot, we can see that initially, the throughput is less but at around time t=30s, it increases and bounces up and down in a small range further on.

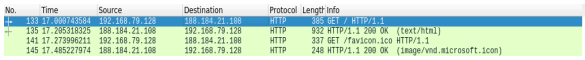
Q2 :

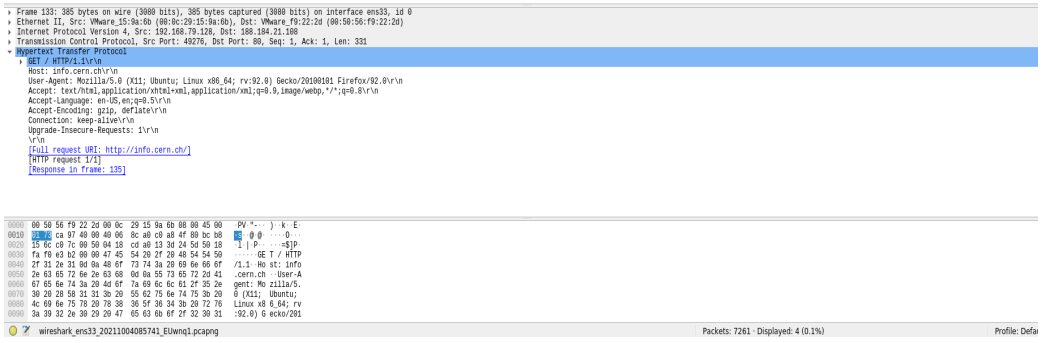
After observing the IP for at which the server is, is **188.184.21.108**, I filtered the packets with the following filter : “ http && (ip.src == 188.184.21.108 || ip.dst == 188.184.21.108) “ and got the following result :

4 HTTP packets between the required sources and destinations.

No.	Time	Source	Destination	Protocol	Length	Info
133	17.000743584	192.168.79.128	188.184.21.108	HTTP	385	GET / HTTP/1.1
135	17.205318325	188.184.21.108	192.168.79.128	HTTP	932	HTTP/1.1 200 OK (text/html)
141	17.273996211	192.168.79.128	188.184.21.108	HTTP	337	GET /favicon.ico HTTP/1.1
145	17.485227974	188.184.21.108	192.168.79.128	HTTP	248	HTTP/1.1 200 OK (image/vnd.microsoft.icon)

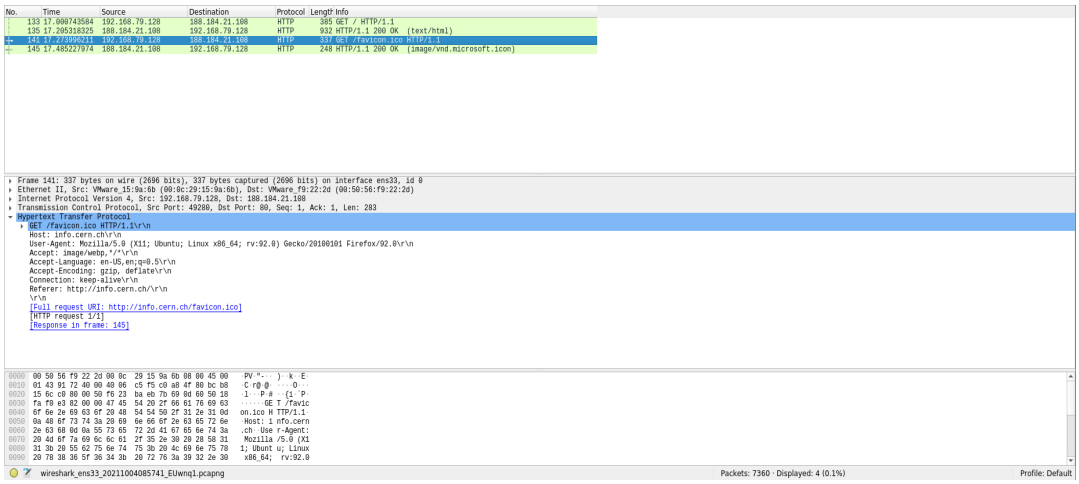
1. For the first packet (S.No 133) :
    - HTTP packet type : HTTP Request
    - HTTP request type : GET request
    - User agent type : Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/20100101 Firefox/92.0
    - HTTP request packet’s URL : http://info.cern.ch/



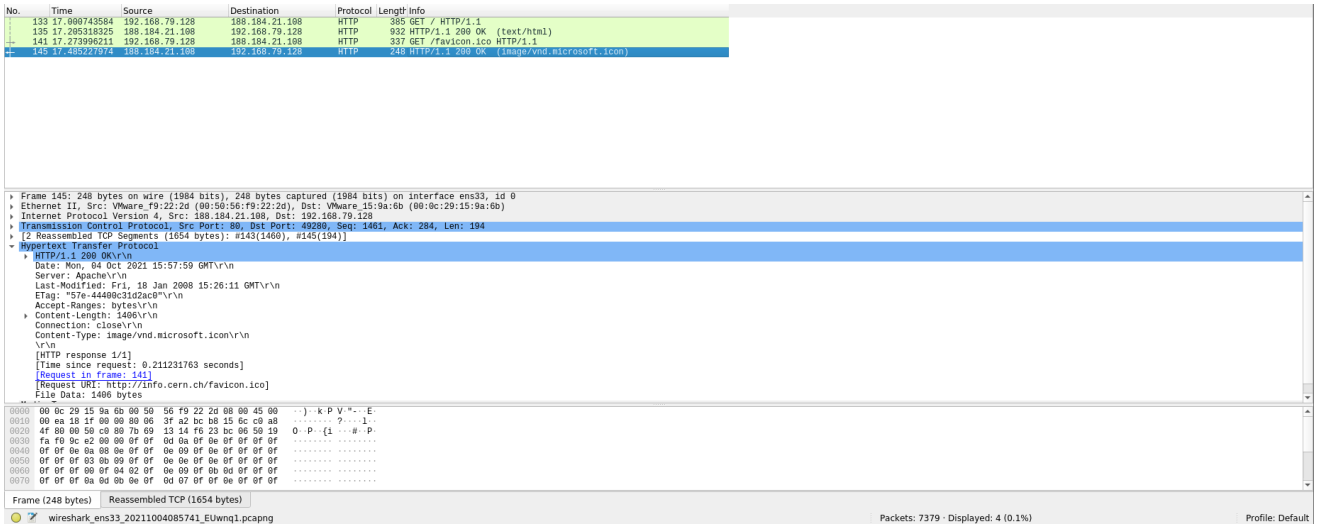


2. For the second packet (S.No 135) :
    - HTTP packet type : HTTP Response
    - HTTP Response code : 200
    - HTTP response description : OK
    - Name and version of the web server: Apache

3. For the third packet (S.No 141) :
    - HTTP packet type : HTTP Request
    - HTTP request type : GET request
    - User agent type : Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/20100101 Firefox/92.0
    - HTTP request packet's URL: http://info.cern.ch/favicon.ico

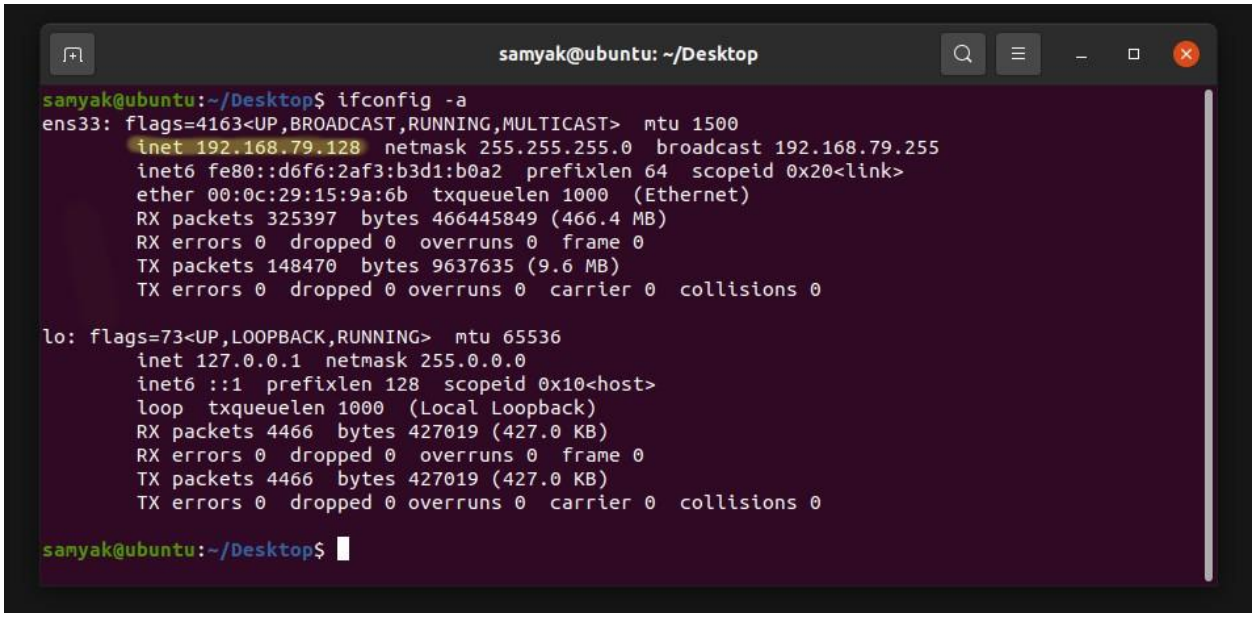


4. For the second packet (S.No 145) :
    - HTTP packet type : HTTP Response
    - HTTP Response code : 200
    - HTTP response description : OK
    - Name and version of the web server: Apache



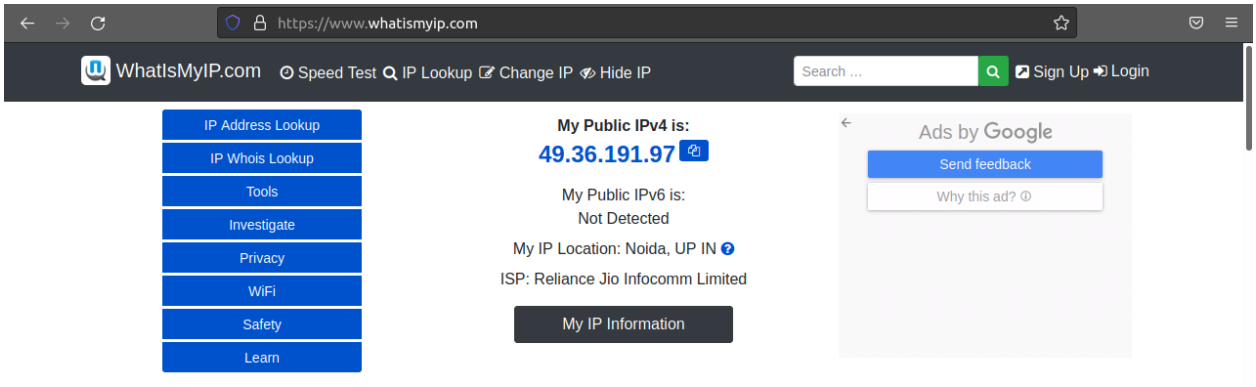
Q3

(a) Using the command: **ifconfig -a**



According to the observed result, we can see that the IP address of my network interface is **192.168.79.128** (highlighted in yellow).

(b)



This website shows that my public IP is: **49.36.191.97**

We can see that the results obtained from both parts are different. The reason behind this is simply that in part (a) what I have obtained is my private IP address (**192.168.79.128)** and in part (b) it is the public IP address(**49.36.191.97)**. The key difference between these two is that a private IP address is used to identify a device uniquely within a particular local area network. Private IP facilitates communication between devices within a network, for example a laptop communicates to the connected WiFi router using this private IP. Thus it is unique for all devices within a particular local network and has a local scope. The public IP has a global scope and is used to access the Internet and is unique on a global scope. It is provided by the internet service provider and is used to access internet service. For example, consider the example: Multiple devices say different laptops, phones connected within the same network (same WiFi router) will have different private IP addresses that will uniquely identify them within that network but their request to access the internet will be forwarded by the router through the same public IP address.

Q4

(a) Command : ping www.google.com -c 1 -M do -s 3000

-c : count of packets in the ping process
-M do : It prevents fragmentation
-s : It denotes packet size (number of bytes to send)

Through the command, I ping 1 packet without fragmentation having data of size 3000 bytes.

```
samyak@ubuntu:/$ ping www.google.com -c 1 -M do -s 3000
PING www.google.com (142.250.206.164) 3000(3028) bytes of data.
ping: local error: message too long, mtu=1500

--- www.google.com ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```

Assuming all the intermediate nodes and client and server all are up we still can see that the ping will fail if we try to send a packet with size 3000 bytes. It throws an error :
ping: local error: message too long, mtu=1500

From this, we can infer that the support mtu is 1500. MTU is the largest packet size that can be transmitted over a network connection. Here the MTU is 1500 meaning the maximum size packet supported for transmitting is 1500 bytes. There, when we try to send a packet with data size 3000 bytes, it will not be transmitted (100% packet loss)

(b) Command : **sudo netstat -a -t -p**
Note: sudo permission was required to see info about all processes.

```
samyak@ubuntu:/$ sudo netstat -a -t -p
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      724/systemd-resolve
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      33113/cupsd
tcp        0      0 ubuntu:35908            ec2-52-43-219-222:https ESTABLISHED 49854/firefox
tcp        0      0 ubuntu:58018            server-13-35-191-:https ESTABLISHED 49854/firefox
tcp        0      0 ubuntu:51728            239.237.117.34.bc:https ESTABLISHED 49854/firefox
tcp        0      0 ubuntu:52298            240.207.227.35.bc:https ESTABLISHED 49854/firefox
tcp        0      0 ubuntu:60660            bom12s20-in-f10.1:https ESTABLISHED 50102/chrome --type
tcp        0      0 ubuntu:47172            bom12s18-in-f14.1:https ESTABLISHED 50102/chrome --type
tcp        0      0 ubuntu:41948            del03s09-in-f14.1:https ESTABLISHED 50102/chrome --type
tcp        0      0 ubuntu:39414            117.18.237.29:http      ESTABLISHED 49854/firefox
tcp        0      0 ubuntu:48068            del11s05-in-f1.1e:https ESTABLISHED 50102/chrome --type
tcp        0      0 ubuntu:55078            del11s08-in-f3.1e:https ESTABLISHED 50102/chrome --type
tcp        0      0 ubuntu:58024            server-13-35-191-:https ESTABLISHED 49854/firefox
tcp        0      0 ubuntu:52416            49.44.117.112:http      ESTABLISHED 49854/firefox
tcp        0      0 ubuntu:40668            del03s10-in-f3.1e1:http ESTABLISHED 49854/firefox
tcp        0      0 ubuntu:59498            bom12s15-in-f4.1e:https CLOSE_WAIT  50102/chrome --type
tcp        0      0 ubuntu:37664            82.221.107.34.bc.g:http ESTABLISHED 49854/firefox
tcp        0      0 ubuntu:48488            221.5.120.34.bc.g:https ESTABLISHED 49854/firefox
tcp        0      0 ubuntu:59206            102.115.120.34.bc:https ESTABLISHED 49854/firefox
tcp        0      0 ubuntu:39562            sa-in-f188.1e100.n:5228 ESTABLISHED 50102/chrome --type
tcp        0      0 ubuntu:37978            bom07s24-in-f3.1e:https ESTABLISHED 50102/chrome --type
tcp        0      0 ubuntu:40348            server-99-86-47-7:https ESTABLISHED 49854/firefox
tcp        0      0 ubuntu:37666            82.221.107.34.bc.g:http ESTABLISHED 49854/firefox
tcp        0      0 ubuntu:52568            76.237.120.34.bc.:https ESTABLISHED 49854/firefox
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN      33113/cupsd
```

Q5 :

(a) To get an authoritative result, I firstly found out the origin nameserver for google.com through the command : nslookup -type=soa google.com
Note : -type=soa : State of Authority record
It was found out to be ns1.google.com.Using this I again do nslookup by running the command : nslookup google.com ns1.google.com and get the authoritative answer.

```
samyak@ubuntu:~$ nslookup -type=soa google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.com
        origin = ns1.google.com
        mail addr = dns-admin.google.com
        serial = 400672185
        refresh = 900
        retry = 900
        expire = 1800
        minimum = 60

Authoritative answers can be found from:

samyak@ubuntu:~$ nslookup google.com ns1.google.com
Server:         ns1.google.com
Address:        216.239.32.10#53

Name:   google.com
Address: 142.250.206.110
Name:   google.com
Address: 2404:6800:4002:82b::200e
```

(b)

```
samyak@ubuntu:~$ dig A +ttlunits www.google.com

; <<>> DiG 9.16.1-Ubuntu <<>> A +ttlunits www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6947
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         5s      IN      A       142.250.192.36

;; Query time: 8 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Oct 05 08:15:14 PDT 2021
;; MSG SIZE  rcvd: 59
```

The time to live for this website on local DNS is 5 seconds. Time to live or TTL basically represents the time a dns record will be stored on the local dns cache. This entry will expire after 5 seconds.

Q6 :

(a) Running the command on a Windows machine,

```
C:\Users\Samyak Jain>tracert www.iiith.ac.in

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

  1    11 ms     2 ms     1 ms  reliance.reliance [192.168.29.1]
  2    10 ms    18 ms     8 ms  10.1.16.1
  3     6 ms     4 ms     5 ms  172.16.18.1
  4     5 ms     5 ms     5 ms  192.168.128.138
  5     7 ms    11 ms    10 ms  172.27.248.53
  6     9 ms     5 ms     5 ms  172.27.248.35
  7     5 ms     5 ms     8 ms  192.168.44.26
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13    34 ms    53 ms    74 ms  115.242.184.26.static.jio.com [115.242.184.26]
 14    46 ms    46 ms    48 ms  196.12.34.76
 15    48 ms    45 ms    45 ms  196.12.53.50

Trace complete.
```

Hop Count	Intermediate Host Address	Latency-1 (ms)	Latency-2 (ms)	Latency-3 (ms)	Average Latency
1	192.168.29.1	11	2	1	4.6667
2	10.1.16.1	10	18	8	12
3	172.16.18.1	6	4	5	3
4	192.168.128.138	5	5	5	5
5	172.27.248.53	7	11	10	9.3333
6	172.27.248.35	9	5	5	6.3333
7	192.168.44.26	5	5	8	6
8	***				
9	***				
10	***				
11	***				
12	***				

13	115.242.184.26	34	53	74	53.6667
14	196.12.34.76	46	46	48	46.6667
15	196.12.53.50	48	45	45	46

Number of intermediate hosts (visible) : 10

(b)

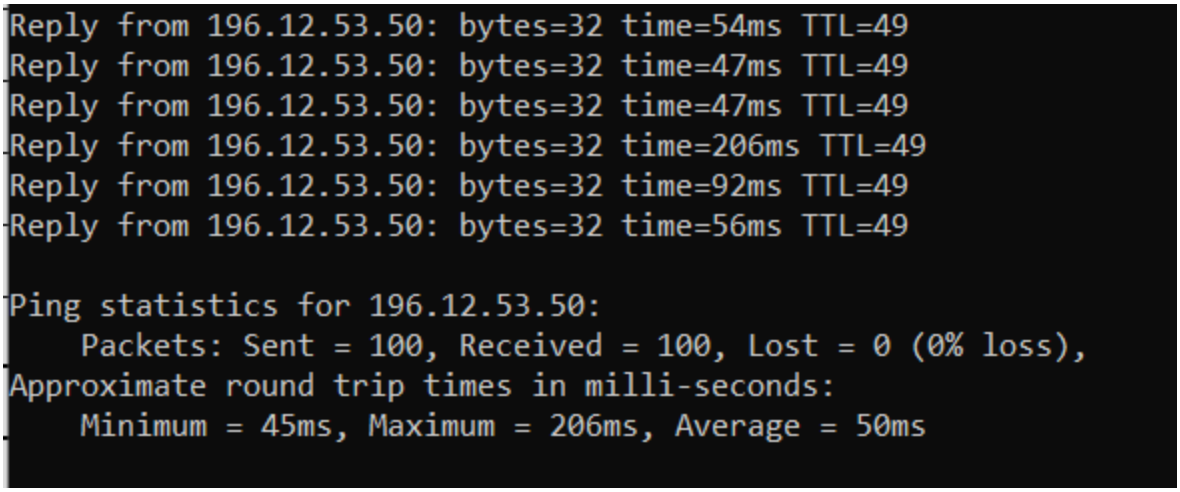
Command : ping -n 100 www.iiith.ac.in

```
C:\Users\Samyak Jain>ping -n 100 www.iiith.ac.in

Pinging www.iiit.ac.in [196.12.53.50] with 32 bytes of data:
Reply from 196.12.53.50: bytes=32 time=46ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=46ms TTL=49
Reply from 196.12.53.50: bytes=32 time=49ms TTL=49
Reply from 196.12.53.50: bytes=32 time=63ms TTL=49
Reply from 196.12.53.50: bytes=32 time=46ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=50ms TTL=49
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
Reply from 196.12.53.50: bytes=32 time=49ms TTL=49
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=46ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=46ms TTL=49
Reply from 196.12.53.50: bytes=32 time=49ms TTL=49
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
Reply from 196.12.53.50: bytes=32 time=46ms TTL=49
Reply from 196.12.53.50: bytes=32 time=49ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
```

```
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
Reply from 196.12.53.50: bytes=32 time=57ms TTL=49
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
Reply from 196.12.53.50: bytes=32 time=50ms TTL=49
Reply from 196.12.53.50: bytes=32 time=50ms TTL=49
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
Reply from 196.12.53.50: bytes=32 time=49ms TTL=49
Reply from 196.12.53.50: bytes=32 time=45ms TTL=49
Reply from 196.12.53.50: bytes=32 time=46ms TTL=49
Reply from 196.12.53.50: bytes=32 time=50ms TTL=49
Reply from 196.12.53.50: bytes=32 time=52ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=46ms TTL=49
Reply from 196.12.53.50: bytes=32 time=46ms TTL=49
Reply from 196.12.53.50: bytes=32 time=51ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=49ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=46ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=46ms TTL=49
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=46ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=45ms TTL=49
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
Reply from 196.12.53.50: bytes=32 time=52ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
```

```
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=50ms TTL=49
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
Reply from 196.12.53.50: bytes=32 time=45ms TTL=49
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=46ms TTL=49
Reply from 196.12.53.50: bytes=32 time=50ms TTL=49
Reply from 196.12.53.50: bytes=32 time=46ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=50ms TTL=49
Reply from 196.12.53.50: bytes=32 time=49ms TTL=49
Reply from 196.12.53.50: bytes=32 time=57ms TTL=49
Reply from 196.12.53.50: bytes=32 time=46ms TTL=49
Reply from 196.12.53.50: bytes=32 time=46ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
Reply from 196.12.53.50: bytes=32 time=48ms TTL=49
Reply from 196.12.53.50: bytes=32 time=53ms TTL=49
Reply from 196.12.53.50: bytes=32 time=50ms TTL=49
Reply from 196.12.53.50: bytes=32 time=57ms TTL=49
Reply from 196.12.53.50: bytes=32 time=47ms TTL=49
Reply from 196.12.53.50: bytes=32 time=72ms TTL=49
Reply from 196.12.53.50: bytes=32 time=96ms TTL=49
```



Average latency: 50ms

(c)

I ping 10 packets to each intermediate host

Command : ping -n 10 [Intermediate-Host-IP]

For Intermediate host :

Address	Average latency
192.168.29.1	2ms
10.1.16.1	6ms
172.16.18.1	Request timed out while ping
192.168.128.138	Request timed out while ping
172.27.248.53	Request timed out while ping
172.27.248.35	Request timed out while ping
192.168.44.26	Request timed out while ping
115.242.184.26	31 ms
196.12.34.76	55 ms
196.12.53.50	47 ms

Firstly I observe for some intermediate IP addresses, the ping request is timing out.
Adding up the ping latencies for the visible intermediate hosts (for hosts that do no time out while pinging) is : 141 ms
This does not match with the average latency obtained in (b), this is because at any time if we ping an IP, it will pass through the previous IPs in the route and the latency for that IP address will be an aggregation of latency of previous IPs. Thus, they won't add up to be equal to (b).

(d)

Address	Average latency
192.168.29.1	2ms
10.1.16.1	6ms
172.16.18.1	Request timed out while ping
192.168.128.138	Request timed out while ping
172.27.248.53	Request timed out while ping
172.27.248.35	Request timed out while ping
192.168.44.26	Request timed out while ping
115.242.184.26	31 ms
196.12.34.76	55 ms
196.12.53.50	47 ms

The maximum latency amongst the intermediate hosts is 55ms which is kind of matching with (b) [50 ms], this is because it corresponds to the second last hop in the route. They have to be comparable because it is almost close to the destination. As we see that at any particular IP, the latency is kind of an aggregate of latencies of previous IPs (because they occur in the route). Close to the destination, it should be highly comparable to the destination latency because the route for reaching the destination has almost been covered.

(e)

Command : dig +noall +answer -x [Intermediate-Host-IP]
(run on Ubuntu VM)

192.168.29.1	reliance.reliance
10.1.16.1	-
172.16.18.1	-
192.168.128.138	-
172.27.248.53	-
172.27.248.35	-
192.168.44.26	-
***	-
***	-
***	-
***	-
***	-
115.242.184.26	115.242.184.26.static.jio.com
196.12.34.76	-
196.12.53.50	-

It is observed for some cases the domain name is not visible. The reason may be that these are private IPs and the domain name may not be visible.

Q7

```
samyak@ubuntu:~$ sudo ifconfig lo down
samyak@ubuntu:~$ ping -c 20 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.

--- 127.0.0.1 ping statistics ---
20 packets transmitted, 0 received, 100% packet loss, time 19450ms
```

Firstly, the loopback interface is disabled using the command : **sudo ifconfig lo down**
Once it has been disabled, we won't be able to communicate through that i.e a 100% packet loss will occur every time. Now if we try to ping 127.0.0.1, i.e through the loopback interface or the localhost with say, 20 packets and wait, we will ultimately see that we have 100% packet loss and the ping command will fail.