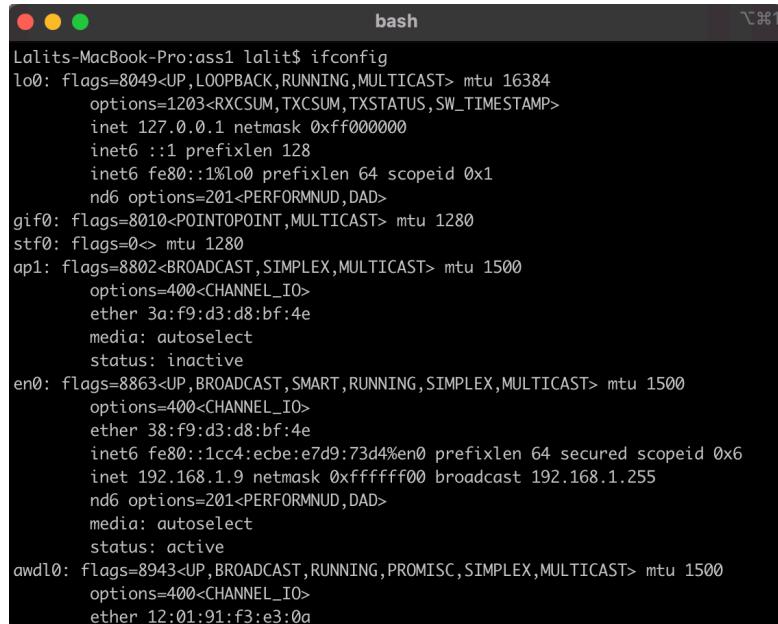


# COL334 Assignment 1

- Dhairyra Gupta, 2019CS50428

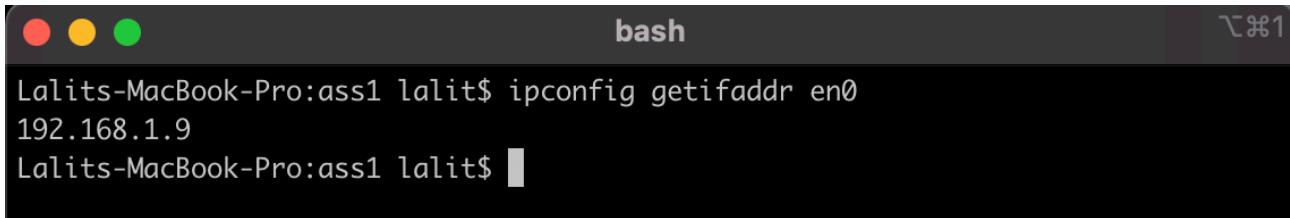
## 1. Networking Tools

- (a) We use ifconfig to get list of interfaces. The interface en0(for ethernet/wireless) holds the IP address of our machine.



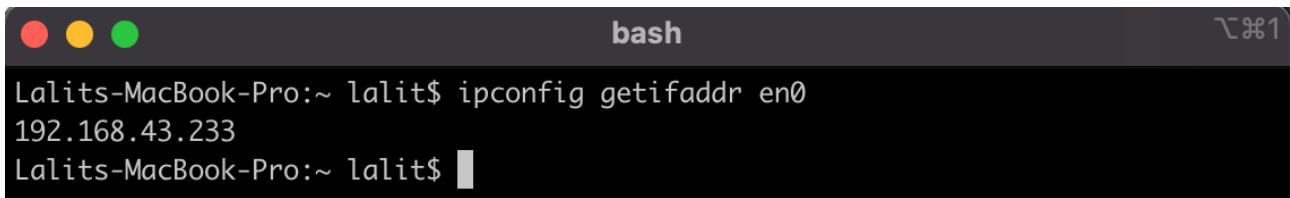
```
Lalits-MacBook-Pro:ass1 lalit$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
    inet 127.0.0.1 netmask 0xffff0000
        inet6 ::1 prefixlen 128
            inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
                nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
ap1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 3a:f9:d3:d8:bf:4e
    media: autoselect
    status: inactive
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 38:f9:d3:d8:bf:4e
    inet6 fe80::1cc4:ecbe:e7d9:73d4%en0 prefixlen 64 secured scopeid 0x6
        inet 192.168.1.9 netmask 0xffffffff broadcast 192.168.1.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 12:01:91:f3:e3:0a
```

Address when connected to Airtel WLAN is 192.168.1.9



```
Lalits-MacBook-Pro:ass1 lalit$ ipconfig getifaddr en0
192.168.1.9
Lalits-MacBook-Pro:ass1 lalit$
```

Address when connected to Airtel 4G hotspot is 192.168.43.233



```
Lalits-MacBook-Pro:~ lalit$ ipconfig getifaddr en0
192.168.43.233
Lalits-MacBook-Pro:~ lalit$
```

(b) The below file shows the default DNS server address

(default DNS server for Airtel WLAN)

Below are the results of nslookup on the default DNS server and on the open DNS server 8.8.8.8

```
○ ○ ○ bash
Last login: Sun Aug 22 12:24:13 on ttys001

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
Lalits-MacBook-Pro:~ lalit$ nslookup www.google.com
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
Name:  www.google.com
Address: 142.250.194.100

Lalits-MacBook-Pro:~ lalit$ nslookup www.google.com 8.8.8.8
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:  www.google.com
Address: 142.250.194.68

Lalits-MacBook-Pro:~ lalit$ nslookup www.facebook.com
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
www.facebook.com canonical name = star-mini.c10r.facebook.com.
Name:  star-mini.c10r.facebook.com
Address: 157.240.16.35

Lalits-MacBook-Pro:~ lalit$ nslookup www.facebook.com 8.8.8.8
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
www.facebook.com canonical name = star-mini.c10r.facebook.com.
Name:  star-mini.c10r.facebook.com
Address: 157.240.198.35

Lalits-MacBook-Pro:~ lalit$
```

As we observe, IP addresses of [www.google.com](http://www.google.com) and [www.facebook.com](http://www.facebook.com) are different in both DNS servers. This means that both DNS servers have locally stored the domain names against different addresses.

On default DNS server(192.168.1.1) -> www.google.com has address 142.250.194.100

On Open DNS server(8.8.8.8)      -> [www.facebook.com](http://www.facebook.com) has address 157.240.16.35  
    -> [www.google.com](http://www.google.com) has address 142.250.194.68  
    -> www.facebook.com has address 157.240.198.35

(c) Below are the ping results for default values of packet size and parameters for [www.iitd.ac.in](http://www.iitd.ac.in)

```

bash
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
Lalits-MacBook-Pro:~ lalit$ ping www.iitd.ac.in
PING www.iitd.ac.in (103.27.9.24): 56 data bytes
64 bytes from 103.27.9.24: icmp_seq=0 ttl=53 time=10.246 ms
64 bytes from 103.27.9.24: icmp_seq=1 ttl=53 time=13.620 ms
64 bytes from 103.27.9.24: icmp_seq=2 ttl=53 time=9.612 ms
64 bytes from 103.27.9.24: icmp_seq=3 ttl=53 time=10.329 ms
64 bytes from 103.27.9.24: icmp_seq=4 ttl=53 time=20.423 ms
64 bytes from 103.27.9.24: icmp_seq=5 ttl=53 time=18.818 ms
64 bytes from 103.27.9.24: icmp_seq=6 ttl=53 time=15.269 ms
64 bytes from 103.27.9.24: icmp_seq=7 ttl=53 time=11.011 ms
64 bytes from 103.27.9.24: icmp_seq=8 ttl=53 time=12.198 ms
64 bytes from 103.27.9.24: icmp_seq=9 ttl=53 time=19.568 ms
Request timeout for icmp_seq 10
64 bytes from 103.27.9.24: icmp_seq=11 ttl=53 time=12.192 ms
64 bytes from 103.27.9.24: icmp_seq=12 ttl=53 time=14.905 ms
64 bytes from 103.27.9.24: icmp_seq=13 ttl=53 time=17.577 ms
64 bytes from 103.27.9.24: icmp_seq=14 ttl=53 time=11.635 ms
64 bytes from 103.27.9.24: icmp_seq=15 ttl=53 time=11.629 ms
64 bytes from 103.27.9.24: icmp_seq=16 ttl=53 time=11.311 ms
^C
--- www.iitd.ac.in ping statistics ---
17 packets transmitted, 16 packets received, 5.9% packet loss
round-trip min/avg/max/stddev = 9.612/13.771/20.423/3.453 ms

```

On varying packet size and TTL, we find maximum packet size = 1472 databytes + 8 header bytes = 1480 bytes for [www.iitd.ac.in](http://www.iitd.ac.in). Minimum ttl for packets to reach = 13.

```

bash
Lalits-MacBook-Pro:~ lalit$ ping www.iitd.ac.in -s 1472
PING www.iitd.ac.in (103.27.9.24): 1472 data bytes
1480 bytes from 103.27.9.24: icmp_seq=0 ttl=53 time=14.869 ms
1480 bytes from 103.27.9.24: icmp_seq=1 ttl=53 time=16.234 ms
1480 bytes from 103.27.9.24: icmp_seq=2 ttl=53 time=15.253 ms
1480 bytes from 103.27.9.24: icmp_seq=3 ttl=53 time=101.408 ms
1480 bytes from 103.27.9.24: icmp_seq=4 ttl=53 time=20.256 ms
1480 bytes from 103.27.9.24: icmp_seq=5 ttl=53 time=14.810 ms
1480 bytes from 103.27.9.24: icmp_seq=6 ttl=53 time=18.735 ms
1480 bytes from 103.27.9.24: icmp_seq=7 ttl=53 time=247.230 ms
^C
--- www.iitd.ac.in ping statistics ---
8 packets transmitted, 8 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 14.810/56.099/247.230/77.401 ms
Lalits-MacBook-Pro:~ lalit$ ping www.iitd.ac.in -s 1473
PING www.iitd.ac.in (103.27.9.24): 1473 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
Request timeout for icmp_seq 7
^C
--- www.iitd.ac.in ping statistics ---
9 packets transmitted, 0 packets received, 100.0% packet loss
Lalits-MacBook-Pro:~ lalit$ 

```

```

bash
Lalits-MacBook-Pro:~ lalit$ ping www.iitd.ac.in -m 12
PING www.iitd.ac.in (103.27.9.24): 56 data bytes
36 bytes from 103.27.9.24: Time to live exceeded
Vr Hl TOS Len ID Flg off TTL Pro cks Src Dst
4 5 00 5400 9a13 0 0000 01 01 edbf 192.168.1.9 103.27.9.24

Request timeout for icmp_seq 0
36 bytes from 103.27.9.24: Time to live exceeded
Vr Hl TOS Len ID Flg off TTL Pro cks Src Dst
4 5 00 5400 9775 0 0000 01 01 f04f 192.168.1.9 103.27.9.24

Request timeout for icmp_seq 1
36 bytes from 103.27.9.24: Time to live exceeded
Vr Hl TOS Len ID Flg off TTL Pro cks Src Dst
4 5 00 5400 bcb5 0 0000 01 01 cb0f 192.168.1.9 103.27.9.24

^C
--- www.iitd.ac.in ping statistics ---
3 packets transmitted, 0 packets received, 100.0% packet loss
Lalits-MacBook-Pro:~ lalit$ ping www.iitd.ac.in -m 13
PING www.iitd.ac.in (103.27.9.24): 56 data bytes
64 bytes from 103.27.9.24: icmp_seq=0 ttl=53 time=14.290 ms
64 bytes from 103.27.9.24: icmp_seq=1 ttl=53 time=10.608 ms
64 bytes from 103.27.9.24: icmp_seq=2 ttl=53 time=8.937 ms
64 bytes from 103.27.9.24: icmp_seq=3 ttl=53 time=12.201 ms
^C
--- www.iitd.ac.in ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 8.937/11.509/14.290/1.977 ms
Lalits-MacBook-Pro:~ lalit$ 

```

On varying packet size and TTL, we find maximum packet size = 68 databytes + 8 header bytes = 76 bytes for [www.google.com](http://www.google.com). Minimum ttl for packets to reach [google.com](http://www.google.com) = 7.

```

bash
Lalits-MacBook-Pro:~ lalit$ ping www.google.com -s 68
PING www.google.com (142.250.194.100): 68 data bytes
76 bytes from 142.250.194.100: icmp_seq=0 ttl=118 time=9.461 ms
76 bytes from 142.250.194.100: icmp_seq=1 ttl=118 time=9.238 ms
76 bytes from 142.250.194.100: icmp_seq=2 ttl=118 time=10.310 ms
76 bytes from 142.250.194.100: icmp_seq=3 ttl=118 time=7.735 ms
^C
--- www.google.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 7.735/9.186/10.928 ms
Lalits-MacBook-Pro:~ lalit$ ping www.google.com -s 69
PING www.google.com (142.250.194.100): 69 data bytes
76 bytes from 142.250.194.100: icmp_seq=0 ttl=118 time=6.905 ms
wrong total length 96 instead of 97
76 bytes from 142.250.194.100: icmp_seq=1 ttl=118 time=10.930 ms
wrong total length 96 instead of 97
76 bytes from 142.250.194.100: icmp_seq=2 ttl=118 time=27.813 ms
wrong total length 96 instead of 97
76 bytes from 142.250.194.100: icmp_seq=3 ttl=118 time=15.472 ms
wrong total length 96 instead of 97
^C
--- www.google.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 6.905/15.280/27.813/7.845 ms
Lalits-MacBook-Pro:~ lalit$ 

```

```

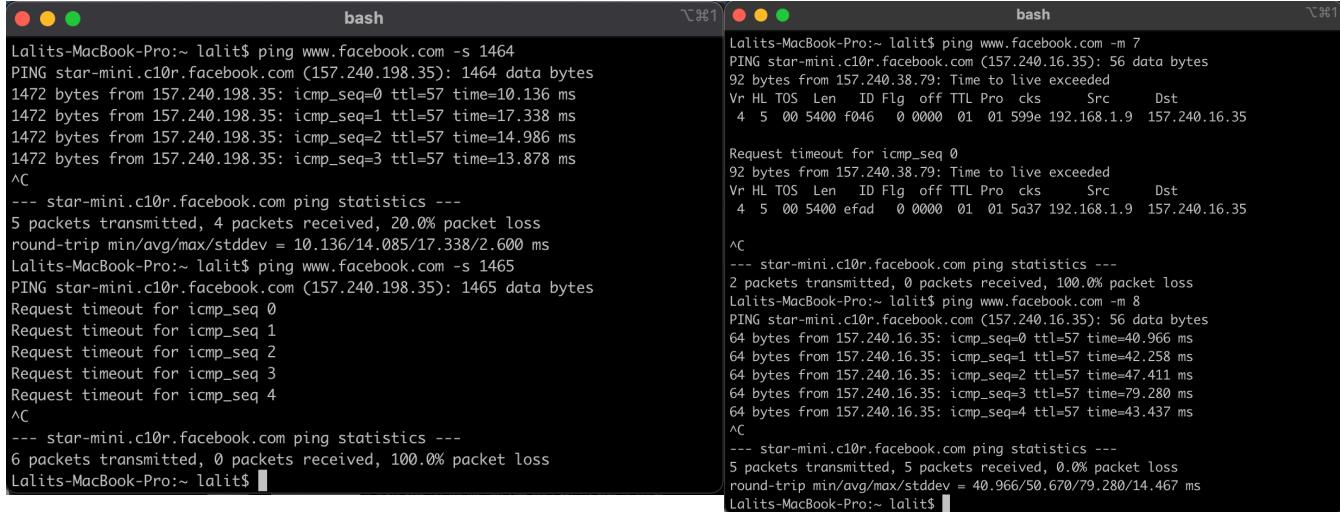
bash
Lalits-MacBook-Pro:~ lalit$ ping www.google.com -m 6
PING www.google.com (142.250.194.100): 56 data bytes
92 bytes from 142.251.52.223: Time to live exceeded
Vr Hl TOS Len ID Flg off TTL Pro cks Src Dst
4 5 60 5400 883a 0 0000 01 01 1dff 192.168.1.9 142.250.194.100

Request timeout for icmp_seq 0
92 bytes from 142.251.52.223: Time to live exceeded
Vr Hl TOS Len ID Flg off TTL Pro cks Src Dst
4 5 60 5400 fc97 0 0000 01 01 a9a1 192.168.1.9 142.250.194.100

^C
--- www.google.com ping statistics ---
2 packets transmitted, 0 packets received, 100.0% packet loss
Lalits-MacBook-Pro:~ lalit$ ping www.google.com -m 7
PING www.google.com (142.250.194.100): 56 data bytes
64 bytes from 142.250.194.100: icmp_seq=0 ttl=118 time=10.239 ms
64 bytes from 142.250.194.100: icmp_seq=1 ttl=118 time=39.776 ms
64 bytes from 142.250.194.100: icmp_seq=2 ttl=118 time=8.588 ms
64 bytes from 142.250.194.100: icmp_seq=3 ttl=118 time=7.807 ms
64 bytes from 142.250.194.100: icmp_seq=4 ttl=118 time=8.646 ms
^C
--- www.google.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 7.807/15.011/39.776/12.408 ms
Lalits-MacBook-Pro:~ lalit$ 

```

On varying packet size and TTL, we find maximum packet size = 1464 databytes + 8 header bytes = 1472 bytes for [www.facebook.com](http://www.facebook.com). Minimum ttl for packets to reach [www.facebook.com](http://www.facebook.com) = 8.



The image shows two side-by-side terminal windows on a Mac OS X desktop. Both windows have a title bar labeled 'bash' and a tab labeled 'Terminal'. The left terminal window shows the output of a 'ping' command with a size of 1464 bytes. It lists several ICMP echo requests sent to 'star-mini.c10r.facebook.com' at 157.240.198.35, with TTL values ranging from 10 to 13. The right terminal window shows the output of a 'ping' command with a size of 56 bytes. It lists several ICMP echo requests sent to 'star-mini.c10r.facebook.com' at 157.240.16.35, with TTL values ranging from 4 to 8. Both terminals show the packet count, round-trip time, and a summary line at the end.

```
Lalits-MacBook-Pro:~ lalit$ ping www.facebook.com -s 1464
PING star-mini.c10r.facebook.com (157.240.198.35): 1464 data bytes
1472 bytes from 157.240.198.35: icmp_seq=0 ttl=57 time=10.136 ms
1472 bytes from 157.240.198.35: icmp_seq=1 ttl=57 time=17.338 ms
1472 bytes from 157.240.198.35: icmp_seq=2 ttl=57 time=14.986 ms
1472 bytes from 157.240.198.35: icmp_seq=3 ttl=57 time=13.878 ms
^C
--- star-mini.c10r.facebook.com ping statistics ---
5 packets transmitted, 4 packets received, 20.0% packet loss
round-trip min/avg/max/stddev = 10.136/14.085/17.338/2.600 ms
Lalits-MacBook-Pro:~ lalit$ ping www.facebook.com -s 1465
PING star-mini.c10r.facebook.com (157.240.198.35): 1465 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
^C
--- star-mini.c10r.facebook.com ping statistics ---
6 packets transmitted, 0 packets received, 100.0% packet loss
Lalits-MacBook-Pro:~ lalit$ 

Lalits-MacBook-Pro:~ lalit$ ping www.facebook.com -m 7
PING star-mini.c10r.facebook.com (157.240.16.35): 56 data bytes
92 bytes from 157.240.38.79: Time to live exceeded
Vr HL TOS Len ID Flg off TTL Pro cks Src Dst
4 5 00 5400 f046 0 0000 01 01 599e 192.168.1.9 157.240.16.35

Request timeout for icmp_seq 0
92 bytes from 157.240.38.79: Time to live exceeded
Vr HL TOS Len ID Flg off TTL Pro cks Src Dst
4 5 00 5400 efad 0 0000 01 01 5a37 192.168.1.9 157.240.16.35

^C
--- star-mini.c10r.facebook.com ping statistics ---
2 packets transmitted, 0 packets received, 100.0% packet loss
Lalits-MacBook-Pro:~ lalit$ ping www.facebook.com -m 8
PING star-mini.c10r.facebook.com (157.240.16.35): 56 data bytes
64 bytes from 157.240.16.35: icmp_seq=0 ttl=57 time=40.966 ms
64 bytes from 157.240.16.35: icmp_seq=1 ttl=57 time=42.258 ms
64 bytes from 157.240.16.35: icmp_seq=2 ttl=57 time=47.411 ms
64 bytes from 157.240.16.35: icmp_seq=3 ttl=57 time=79.280 ms
64 bytes from 157.240.16.35: icmp_seq=4 ttl=57 time=43.437 ms
^C
--- star-mini.c10r.facebook.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 40.966/50.670/79.280/14.467 ms
Lalits-MacBook-Pro:~ lalit$ 
```

(d)Running traceroute on [www.iitd.ac.in](http://www.iitd.ac.in), we observe that most of our ping requests do not get responses. This is because by default, traceroute uses UDP ports for tracing hosts. In this case, firewalls block UDP ports and no echo response is sent back by the router.

One possible solution in such a case is to use ICMP packets which will not be blocked by most routers.(using **traceroute -I www.iitd.ac.in** on linux/mac)

```
Lalits-MacBook-Pro:~ lalit$ reset
Lalits-MacBook-Pro:~ lalit$ traceroute www.iitd.ac.in
traceroute to www.iitd.ac.in (103.27.9.24), 64 hops max, 52 byte packets
 1  dsldevice.lan (192.168.1.1)  3.253 ms  7.360 ms  2.160 ms
 2  223.182.79.255 (223.182.79.255)  7.693 ms  16.013 ms  6.921 ms
 3  nsg-corporate-5.30.187.122.airtel.in (122.187.30.5)  11.035 ms  16.758 ms  1
2.914 ms
 4  182.79.181.79 (182.79.181.79)  14.842 ms
    182.79.181.227 (182.79.181.227)  12.210 ms
    182.79.176.56 (182.79.176.56)  8.640 ms
 5  115.110.232.173.static.delhi.vsnl.net.in (115.110.232.173)  9.836 ms  9.640
ms  9.514 ms
 6  * * *
 7  14.140.210.22.static-delhi-vsnl.net.in (14.140.210.22)  12.683 ms  55.127 ms
8.171 ms
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
^C
Lalits-MacBook-Pro:~ lalit$
```

*(Traceroute default using UDP packets)*

```
Lalits-MacBook-Pro:~ lalit$ traceroute -I www.iitd.ac.in
traceroute to www.iitd.ac.in (103.27.9.24), 64 hops max, 72 byte packets
 1  dsldevice.lan (192.168.1.1)  8.429 ms  1.722 ms  3.666 ms
 2  223.182.79.255 (223.182.79.255)  6.611 ms  14.682 ms  14.072 ms
 3  nsg-corporate-5.30.187.122.airtel.in (122.187.30.5)  14.729 ms  7.459 ms  8.
903 ms
 4  182.79.149.6 (182.79.149.6)  9.703 ms  11.597 ms  7.104 ms
 5  115.110.232.173.static.delhi.vsnl.net.in (115.110.232.173)  7.924 ms  11.254
ms  14.228 ms
 6  * * *
 7  14.140.210.22.static-delhi-vsnl.net.in (14.140.210.22)  12.559 ms  13.620 ms
9.972 ms
 8  * * *
 9  * * *
10  * * *
11  103.27.9.24 (103.27.9.24)  21.130 ms  12.931 ms  13.266 ms
12  103.27.9.24 (103.27.9.24)  17.571 ms  12.555 ms  16.268 ms
13  103.27.9.24 (103.27.9.24)  11.522 ms  10.938 ms  11.575 ms
Lalits-MacBook-Pro:~ lalit$
```

*(Traceroute using ICMP packets)*

We can also see the differences over different networks(Airtel 4G and WLAN). The initial 5 hops for 4G network are different. But the routes coincide at port 182.79.153.87. Both routes coincide after reaching the nsg-corporate airtel.in node.

Some private IPs on our home network are visible in the route such as hop 1,2,3,4(on 4G network) [192.168.\*.\*] and dsldevice.lan(192.168.1.1)(on WLAN) (

Also nodes 10.119.234.161, 10.119.233.65, 10.119.233.66 are private IPs (likely belonging to IIT Delhi network)

```
The default interactive shell is now zsh.  
To update your account to use zsh, please run `chsh -s /bin/zsh`.  
For more details, please visit https://support.apple.com/kb/HT208050.  
Lalits-MacBook-Pro:~ lalit$ traceroute -I www.iitd.ac.in  
traceroute to www.iitd.ac.in (103.27.9.24), 64 hops max, 72 byte packets  
1 * 192.168.43.182 (192.168.43.182) 324.325 ms 4.077 ms  
2 192.168.59.1 (192.168.59.1) 17.717 ms 20.110 ms 19.130 ms  
3 192.168.27.45 (192.168.27.45) 35.509 ms 21.668 ms 21.557 ms  
4 192.168.27.111 (192.168.27.111) 19.047 ms 28.143 ms 22.495 ms  
5 nsg-corporate-5.30.187.122.airtel.in (122.187.30.5) 19.939 ms 21.023 ms 21.572 ms  
6 182.79.153.87 (182.79.153.87) 20.715 ms 23.225 ms 23.834 ms  
7 115.110.232.173.static.delhi.vsnl.net.in (115.110.232.173) 21.794 ms 21.711 ms 29.410 ms  
8 * * *  
9 14.140.210.22.static-delhi-vsnl.net.in (14.140.210.22) 66.684 ms 30.044 ms 36.963 ms  
10 10.119.234.161 (10.119.234.161) 40.560 ms 26.724 ms 25.939 ms  
11 10.119.233.65 (10.119.233.65) 22.892 ms 28.666 ms 24.938 ms  
12 10.119.233.66 (10.119.233.66) 24.742 ms 32.904 ms 39.855 ms  
13 103.27.9.24 (103.27.9.24) 41.890 ms 36.894 ms 36.277 ms  
14 103.27.9.24 (103.27.9.24) 44.031 ms 38.724 ms 81.235 ms  
15 103.27.9.24 (103.27.9.24) 23.107 ms 28.746 ms 24.222 ms  
Lalits-MacBook-Pro:~ lalit$
```

(Airtel 4G - mobile hotspot)

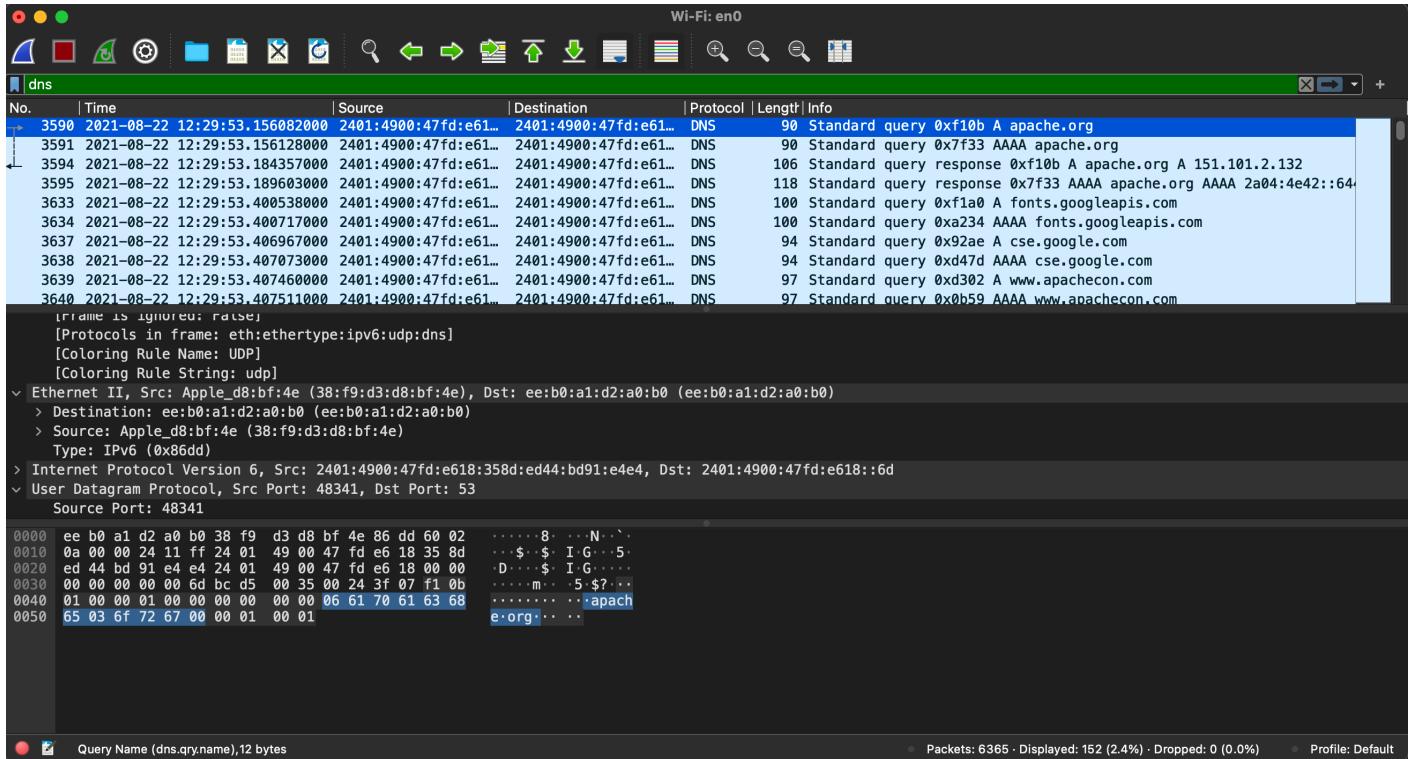
```
Lalits-MacBook-Pro:~ lalit$ traceroute -I www.iitd.ac.in  
traceroute to www.iitd.ac.in (103.27.9.24), 64 hops max, 72 byte packets  
1 dsldevice.lan (192.168.1.1) 8.429 ms 1.722 ms 3.666 ms  
2 223.182.79.255 (223.182.79.255) 6.611 ms 14.682 ms 14.072 ms  
3 nsg-corporate-5.30.187.122.airtel.in (122.187.30.5) 14.729 ms 7.459 ms 8.903 ms  
4 182.79.149.6 (182.79.149.6) 9.703 ms 11.597 ms 7.104 ms  
5 115.110.232.173.static.delhi.vsnl.net.in (115.110.232.173) 7.924 ms 11.254 ms 14.228 ms  
6 * * *  
7 14.140.210.22.static-delhi-vsnl.net.in (14.140.210.22) 12.559 ms 13.620 ms 9.972 ms  
8 * * *  
9 * * *  
10 * * *  
11 103.27.9.24 (103.27.9.24) 21.130 ms 12.931 ms 13.266 ms  
12 103.27.9.24 (103.27.9.24) 17.571 ms 12.555 ms 16.268 ms  
13 103.27.9.24 (103.27.9.24) 11.522 ms 10.938 ms 11.575 ms  
Lalits-MacBook-Pro:~ lalit$
```

(Airtel WLAN )

All the addresses here are IPv4. There is a separate command traceroute6 on macOS which returns IPv6 addresses. On linux, flags such as '-4' can be used to force the traceroute command to return IPv4 addresses.

## 2. Packet Analysis

- (a) After applying the dns filter, we can see the timestamps for the request and response DNS packets in Wireshark. Here we see 2 DNS requests(A and AAAA) corresponding to IPv4 address and IPv6 addresses respectively.



For IPv4 DNS request, time difference between request and response is 28.275ms

For IPv6 DNS request, time difference between request and response is 33.475ms

(b)

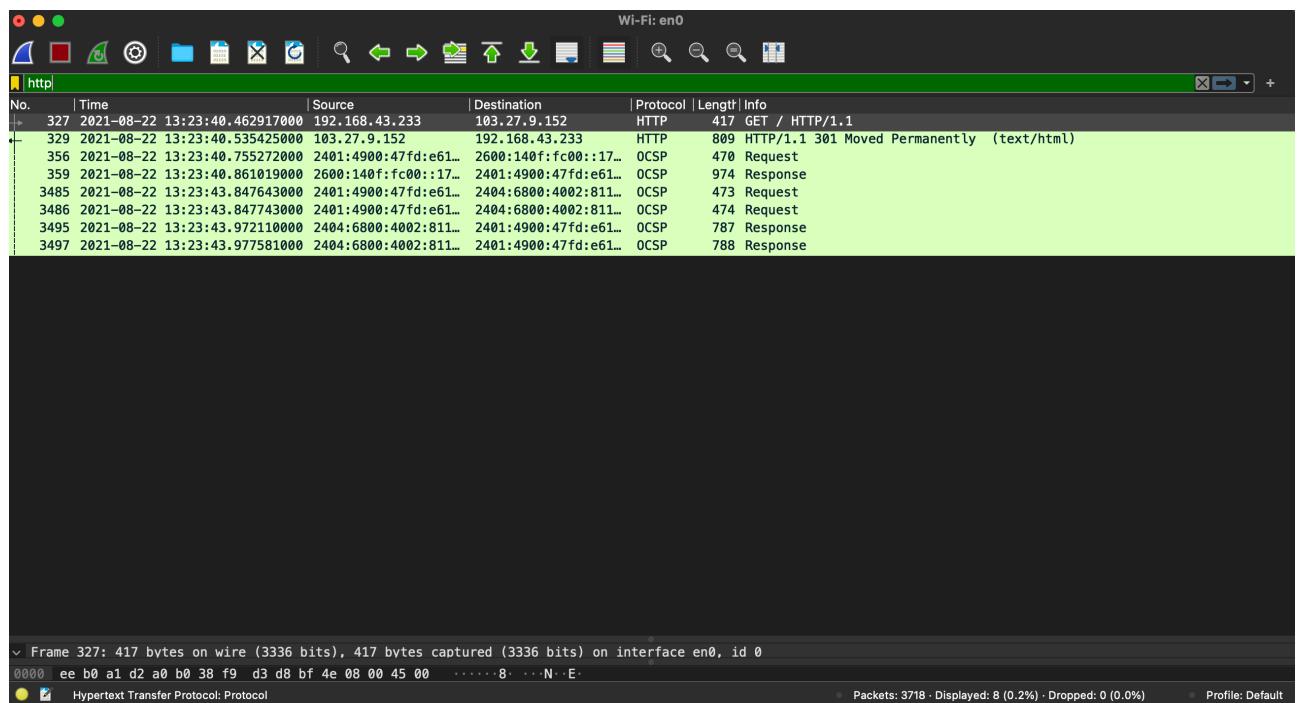
On applying the HTTP filter, we observe that there were approximately 30 HTTP requests(not counting the responses), all of them were GET requests. We can also see the order of Get Requests(response packets need not be in order). First GET request is for html file, followed by css, thumbnails(i.e. the layout files of the webpage). Then the scripting files(.js files) are requested, along with .jpg, .png images.

Frame 3600: 551 bytes on wire (4408 bits), 551 bytes captured (4408 bits) on interface en0, id 0  
0000 ee b0 a1 d2 a0 b0 38 f9 d3 d8 b7 4e 86 dd 00 09 ... 8 N+ ...  
0100 465 GET /cse.js?cx=00570343832241770421:5mgshgrgx2u HTTP/1.1  
0101 465 GET /logos/res/knox/default.png HTTP/1.1  
0102 465 GET /img/apache-con.jpg HTTP/1.1  
0103 875 HTTP/1.1 200 OK (JPEG JFIF image)  
0104 505 GET /img/trillions-and-trillions/apache-innovation-thumbnail.jpg HTTP/1.1  
0105 538 GET /img/trillions-and-trillions/apache-innovationThumbnail.jpg HTTP/1.1  
0106 538 GET /img/trillions-and-trillions/apache-everywhere-thumbnail.jpg HTTP/1.1  
0107 457 HTTP/1.1 200 OK (text/css)  
0108 440 GET /js/jquery-2.1.1.min.js HTTP/1.1  
0109 513 HTTP/1.1 200 OK (text/css)  
0110 433 GET /js/bootstrap.js HTTP/1.1  
0111 644 HTTP/1.1 200 OK (JPEG JFIF image)  
0112 433 GET /js/slideshow.js HTTP/1.1  
0113 509 HTTP/1.1 200 OK (JPEG JFIF image)  
0114 544 GET /img/trillions-and-trillions/trillions-and-trillions-thumbnail.jpg HTTP/1.1  
0115 1198 HTTP/1.1 200 OK (JPEG JFIF image)  
0116 538 GET /img/trillions-and-trillions/apache-innovation-thumbnail.jpg HTTP/1.1  
0117 221 HTTP/1.1 200 OK (application/javascript)  
0118 498 GET /img/2020-report.jpg HTTP/1.1  
0119 512 HTTP/1.1 200 OK (application/javascript)  
0120 496 GET /img/community.jpg HTTP/1.1  
0121 1088 HTTP/1.1 200 OK (JPEG JFIF image)  
0122 501 GET /img/the-apache-way.jpg HTTP/1.1  
0123 927 HTTP/1.1 200 OK (application/javascript)  
0124 496 GET /img/ApacheCon.jpg HTTP/1.1  
0125 875 HTTP/1.1 200 OK (JPEG JFIF image)  
0126 505 GET /logos/res/knox/default.png HTTP/1.1  
0127 465 GET /cse.js?cx=00570343832241770421:5mgshgrgx2u HTTP/1.1

(c) We see that the final HTTP response has time stamp 12:29:57.189115000. In part(a) we note the timestamp of 12:29:53.156082000 for the first DNS request. Hence, time taken to load the webpage is ~4.033 seconds.

No.	Time	Source	Destination	Protocol	Length	Info
4001	2021-08-22 12:29:53.784819000	2a04:4e42::644	2a01:4900:47fd:e61...	HTTP	512	HTTP/1.1 200 OK (application/javascript)
4008	2021-08-22 12:29:53.786284000	2a01:4900:47fd:e61...	2a04:4e42::644	HTTP	496	GET /img/community.jpg HTTP/1.1
4027	2021-08-22 12:29:53.802179300	2a04:4e42::644	2a01:4900:47fd:e61...	HTTP	1088	HTTP/1.1 200 OK (JPEG JFIF image)
4031	2021-08-22 12:29:53.802465000	2a01:4900:47fd:e61...	2a04:4e42::644	HTTP	501	GET /img/the-apache-way.jpg HTTP/1.1
4041	2021-08-22 12:29:53.803953000	2a04:4e42::644	2a01:4900:47fd:e61...	HTTP	927	HTTP/1.1 200 OK (application/javascript)
4052	2021-08-22 12:29:53.805002000	2a01:4900:47fd:e61...	2a04:4e42::644	HTTP	496	GET /img/ApacheCon.jpg HTTP/1.1
4106	2021-08-22 12:29:53.857136000	2a04:4e42::644	2a01:4900:47fd:e61...	HTTP	875	HTTP/1.1 200 OK (JPEG JFIF image)
4123	2021-08-22 12:29:53.8588819000	2a01:4900:47fd:e61...	2a04:4e42::644	HTTP	505	GET /logos/res/knox/default.png HTTP/1.1
4124	2021-08-22 12:29:53.858976000	2a01:4900:47fd:e61...	2a04:6800:4002:809...	HTTP	465	GET /cse.js?cx=005703438322411770421:5mgshrgx2u HTTP/1.1
4225	2021-08-22 12:29:53.900835000	2a04:4e42::644	2a01:4900:47fd:e61...	HTTP	646	HTTP/1.1 200 OK (JPEG JFIF image)
4230	2021-08-22 12:29:53.901480000	2a01:4900:47fd:e61...	2a04:4e42::644	HTTP	506	GET /fonts/glyphicons-halflings-regular.woff2 HTTP/1.1
4249	2021-08-22 12:29:53.9208934000	2a04:4e42::644	2a01:4900:47fd:e61...	HTTP	1062	HTTP/1.1 200 OK (JPEG JFIF image)
4260	2021-08-22 12:29:53.9216164000	2a01:4900:47fd:e61...	2a04:4e42::644	HTTP	509	GET /logos/res/geronimo/default.png HTTP/1.1
4473	2021-08-22 12:29:54.294741000	2a04:4e42::644	2a01:4900:47fd:e61...	HTTP	1294	HTTP/1.1 200 OK (JPEG JFIF image)
4475	2021-08-22 12:29:54.2967791000	2a01:4900:47fd:e61...	2a04:4e42::644	HTTP	506	GET /logos/res/james/default.png HTTP/1.1
4545	2021-08-22 12:29:54.477114000	2a04:4e42::644	2a01:4900:47fd:e61...	HTTP	564	HTTP/1.1 200 OK (font/woff2)
4558	2021-08-22 12:29:54.479270000	2a01:4900:47fd:e61...	2a04:4e42::644	HTTP	510	GET /logos/res/incubator/default.png HTTP/1.1
4564	2021-08-22 12:29:54.505218000	2a04:4e42::644	2a01:4900:47fd:e61...	HTTP	628	HTTP/1.1 200 OK (PNG)
4567	2021-08-22 12:29:54.506223000	2a01:4900:47fd:e61...	2a04:4e42::644	HTTP	505	GET /logos/res/spot/default.png HTTP/1.1
4596	2021-08-22 12:29:54.649870000	2a04:6800:4002:809...	2a01:4900:47fd:e61...	HTTP	694	HTTP/1.1 404 Not Found (text/html)
4950	2021-08-22 12:29:54.944674000	2a04:4e42::644	2a01:4900:47fd:e61...	HTTP	983	HTTP/1.1 200 OK (PNG)
4993	2021-08-22 12:29:54.989235000	2a04:4e42::644	2a01:4900:47fd:e61...	HTTP	1372	HTTP/1.1 200 OK (PNG)
5104	2021-08-22 12:29:55.207695000	2a04:4e42::644	2a01:4900:47fd:e61...	HTTP	944	HTTP/1.1 200 OK (PNG)
5266	2021-08-22 12:29:55.334781000	2a01:4900:47fd:e61...	2a04:6800:4002:809...	HTTP	449	GET /adsense/search/acsyng-ads.js HTTP/1.1
5247	2021-08-22 12:29:55.382087000	2a01:4900:47fd:e61...	2a04:6800:4002:81c...	HTTP	500	GET /generate_204 HTTP/1.1
5267	2021-08-22 12:29:55.421371000	2a04:6800:4002:81c...	2a01:4900:47fd:e61...	HTTP	169	HTTP/1.1 200 No Content
5403	2021-08-22 12:29:55.570161000	2a04:6800:4002:809...	2a01:4900:47fd:e61...	HTTP	88	HTTP/1.1 200 OK (text/javascript)
6358	2021-08-22 12:29:57.108730000	2a01:4900:47fd:e61...	2a04:4e42::644	HTTP	499	GET /favicons/favicon.ico HTTP/1.1
6363	2021-08-22 12:29:57.189115000	2a04:4e42::644	2a01:4900:47fd:e61...	HTTP	955	HTTP/1.1 200 OK (PNG)

(d) Below, we can see the results of http filter when <http://cse.iitd.ac.in/>. In case of apache.org, the response to HTTP request was 200 OK, but here the response is 301(Moved Permanently). A likely reason for this to occur is that all HTTP requests are redirected to HTTPS requests(visible using tls filter) so that all requests are secure. Many sites nowadays, redirect all HTTP requests to HTTPS in which transmitted packets are encrypted. For <http://apache.org>, http requests are not defaulted to https, hence the content packets were visible corresponding to HTTP protocol.



### 3. Implement traceroute using ping

Given below is the output of the traceroute implementation on [www.google.com](http://www.google.com)

```
bash
Lalits-MacBook-Pro:ass1 lalit$ python3 script.py www.google.com
hop 1:
ping 0: 3.79ms 192.168.1.1
ping 1: 7.32ms 192.168.1.1
ping 2: 1.85ms 192.168.1.1

hop 2:
ping 0: 8.41ms 192.168.1.1
ping 1: 2.94ms 192.168.1.1
ping 2: 1.81ms 192.168.1.1

hop 3:
ping 0: 7.71ms 223.182.79.255
ping 1: 9.42ms 223.182.79.255
ping 2: 9.89ms 223.182.79.255

hop 4:
ping 0: 5.72ms 122.187.30.5
ping 1: 15.56ms 122.187.30.5
ping 2: 6.61ms 122.187.30.5

hop 5:
ping 0: 11.72ms 142.250.161.56
ping 1: 16.22ms 142.250.161.56
ping 2: 11.08ms 142.250.161.56

hop 6:
ping 0: 10.28ms 142.251.66.169
ping 1: 20.75ms 142.251.66.169
ping 2: 13.65ms 142.251.66.169

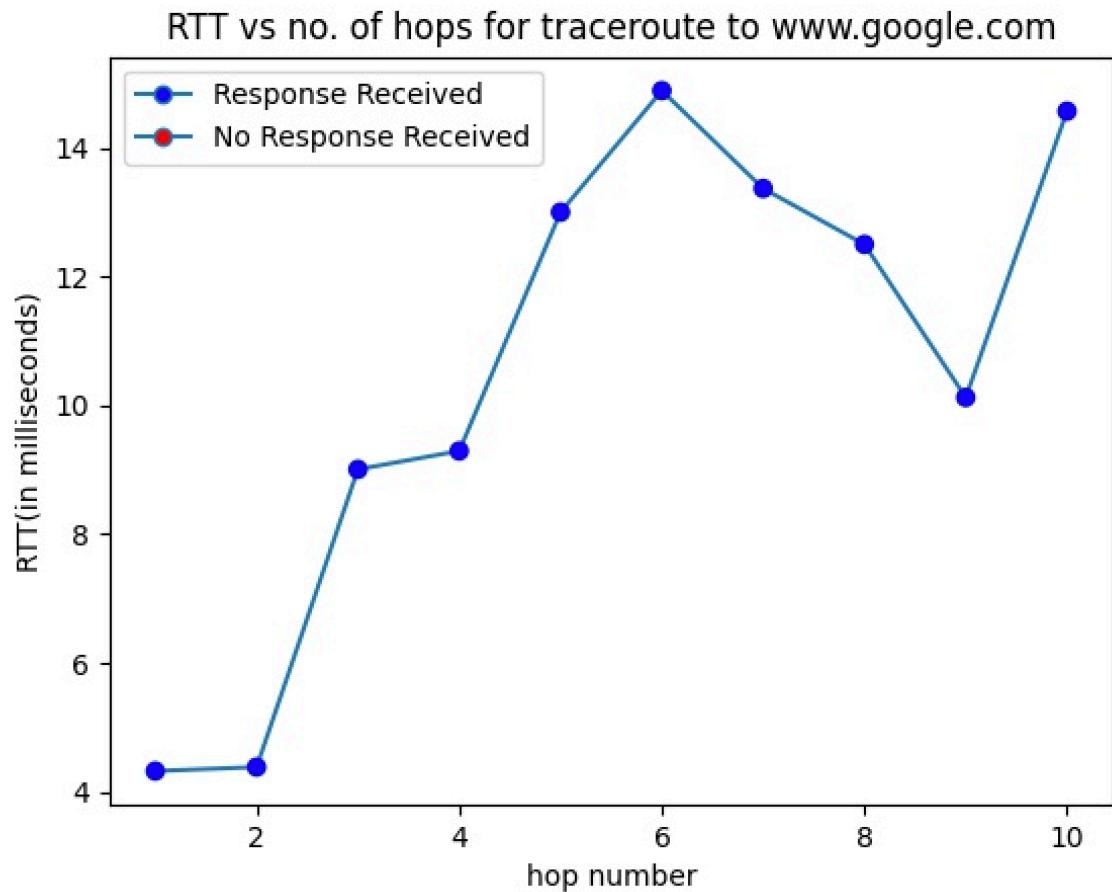
hop 7:
ping 0: 14.06ms 142.251.52.223
ping 1: 11.13ms 142.251.52.223
ping 2: 14.93ms 142.251.52.223

hop 8:
ping 0: 11.41ms 142.250.194.100
ping 1: 12.32ms 142.250.194.100
ping 2: 13.79ms 142.250.194.100

hop 9:
ping 0: 9.13ms 142.250.194.100
ping 1: 9.9ms 142.250.194.100
ping 2: 11.35ms 142.250.194.100

hop 10:
ping 0: 17.11ms 142.250.194.100
ping 1: 12.38ms 142.250.194.100
ping 2: 14.24ms 142.250.194.100
Lalits-MacBook-Pro:ass1 lalit$
```

The corresponding RTT vs no. of hops plot is given below. The RTT is the average time of all received responses in each plot



## Output for www.iitd.ac.in

```
Lalits-MacBook-Pro:ass1 lalit$ python3 script.py www.iitd.ac.in
hop 1:
ping 0: 2.4ms 192.168.1.1
ping 1: 6.59ms 192.168.1.1
ping 2: 5.78ms 192.168.1.1

hop 2:
ping 0: 2.64ms 192.168.1.1
ping 1: 4.33ms 192.168.1.1
ping 2: 3.08ms 192.168.1.1

hop 3:
ping 0: 8.77ms 223.182.79.255
ping 1: 8.46ms 223.182.79.255
ping 2: 7.07ms 223.182.79.255

hop 4:
ping 0: 10.84ms 122.187.30.5
ping 1: 7.71ms 122.187.30.5
ping 2: 5.24ms 122.187.30.5

hop 5:
ping 0: 13.4ms 182.79.149.6
ping 1: 8.13ms 182.79.149.6
ping 2: 11.26ms 182.79.149.6

hop 6:
ping 0: *
ping 1: *
ping 2: *

hop 7:
ping 0: *
ping 1: *
ping 2: *

hop 8:
ping 0: 11.97ms 14.140.210.22
ping 1: 13.05ms 14.140.210.22
ping 2: 19.3ms 14.140.210.22

hop 9:
ping 0: *
ping 1: *
ping 2: *

hop 10:
ping 0: *
ping 1: *
ping 2: *

hop 11:
ping 0: *
ping 1: *
ping 2: *

hop 12:
ping 0: 12.19ms 103.27.9.24
ping 1: 19.38ms 103.27.9.24
ping 2: 17.03ms 103.27.9.24

hop 13:
ping 0: 12.89ms 103.27.9.24
ping 1: 14.56ms 103.27.9.24
ping 2: 12.67ms 103.27.9.24

hop 14:
ping 0: 12.71ms 103.27.9.24
ping 1: 10.31ms 103.27.9.24
ping 2: 15.55ms 103.27.9.24
Lalits-MacBook-Pro:ass1 lalit$
```

Corresponding plot is given below

