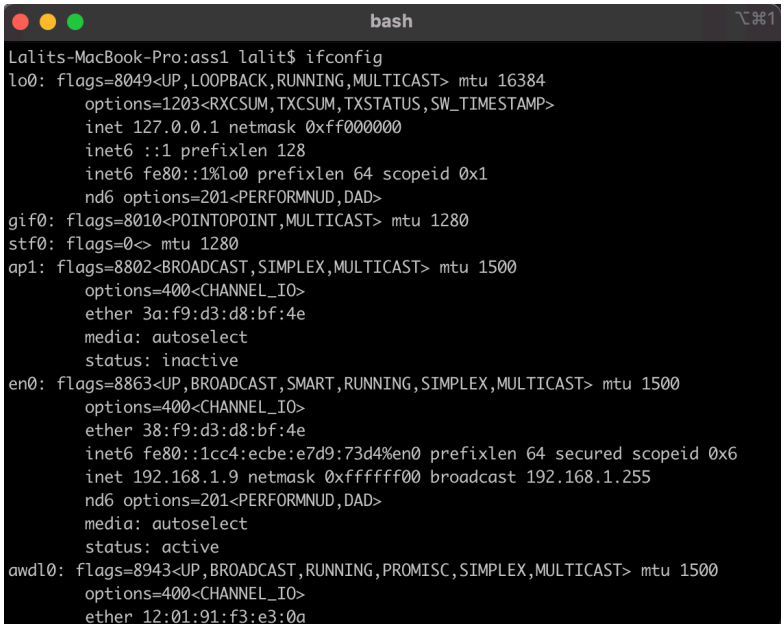
COL334 Assignment 1

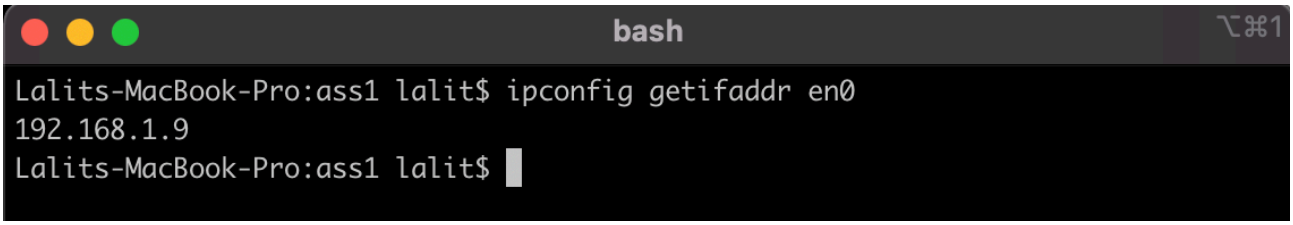
- Dhairya Gupta, 2019CS50428

1. Networking Tools

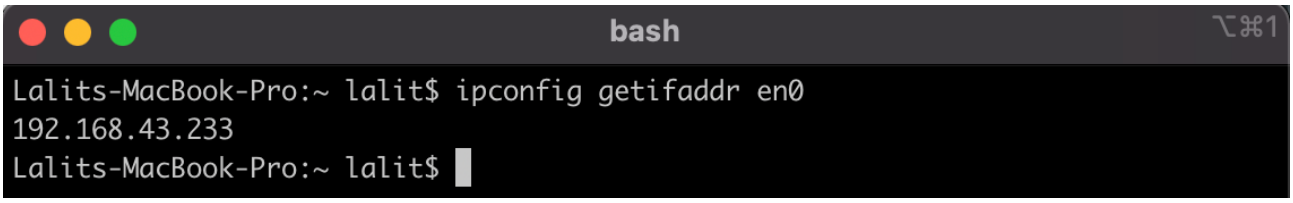
(a) We use ifconfig to get list of interfaces. The interface en0(for ethernet/wireless) holds the IP address of our machine.



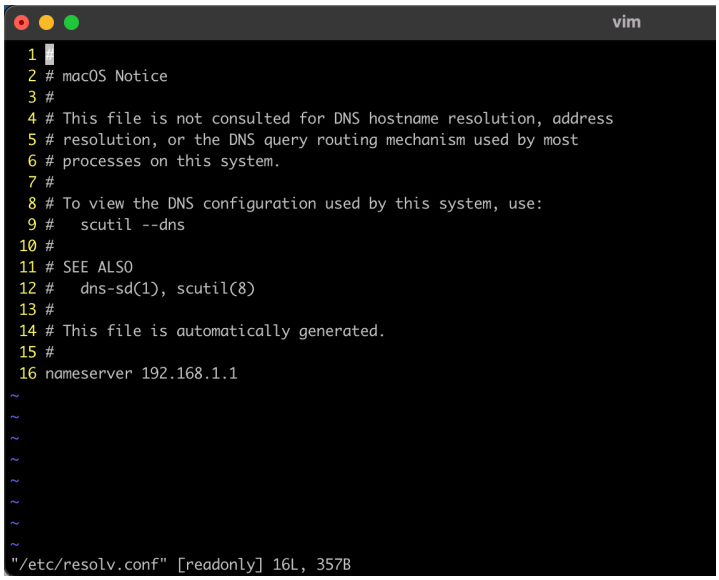
Address when connected to Airtel WLAN is 192.168.1.9



Address when connected to Airtel 4G hotspot is 192.168.43.233

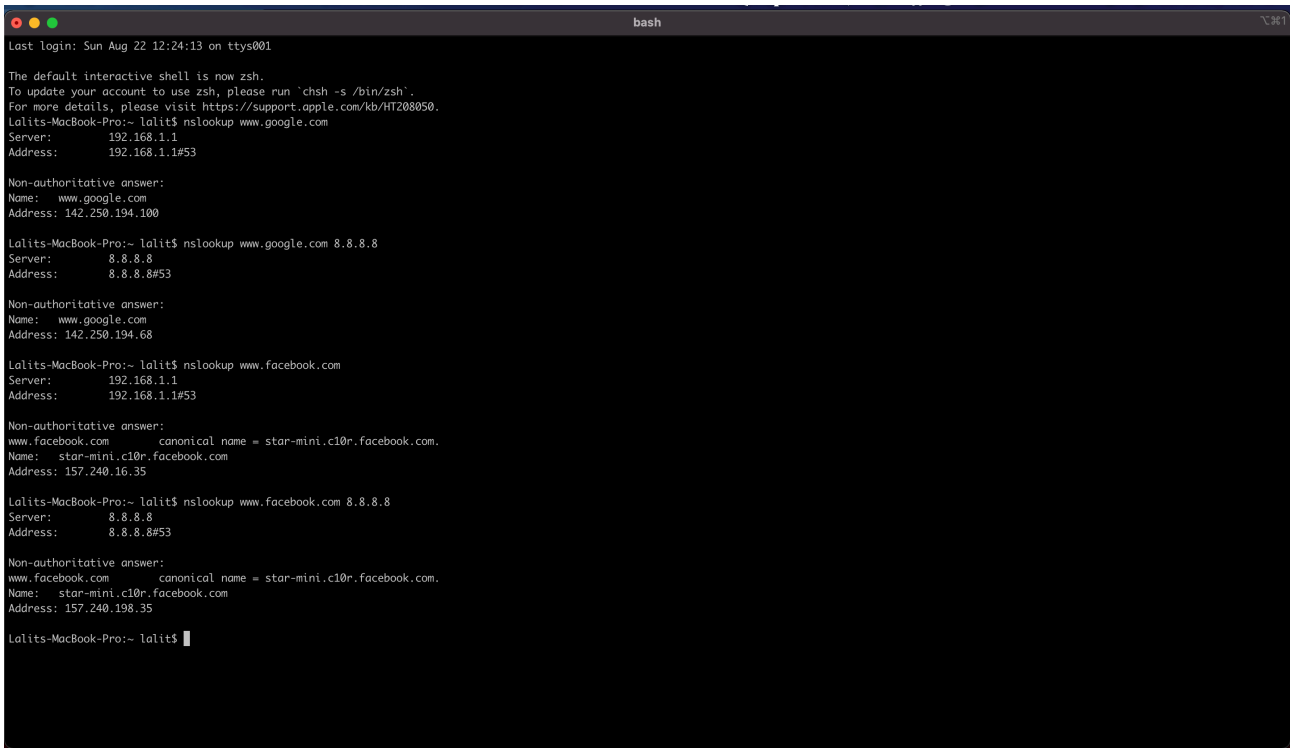


(b) The below file shows the default DNS server address



(default DNS server for Airtel WLAN)

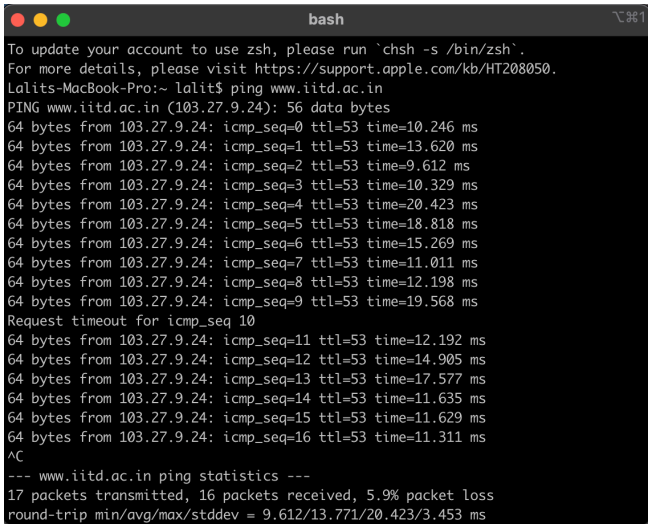
Below are the results of nslookup on the default DNS server and on the open DNS server 8.8.8.8



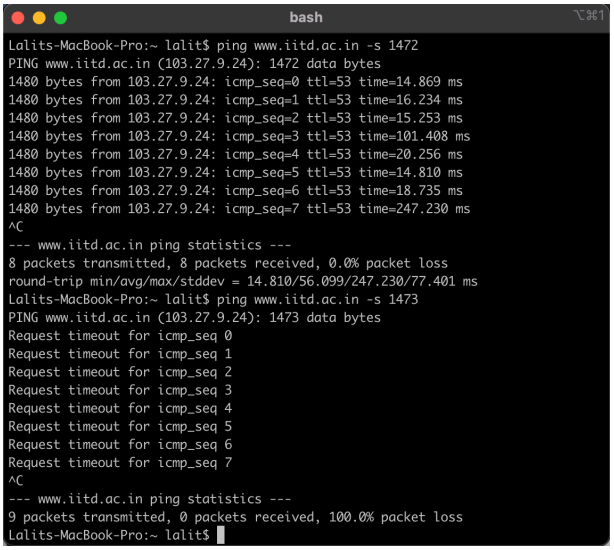
As we observe, IP addresses of www.google.com and www.facebook.com are different in both DNS servers. This means that both DNS servers have locally stored the domain names against different addresses.

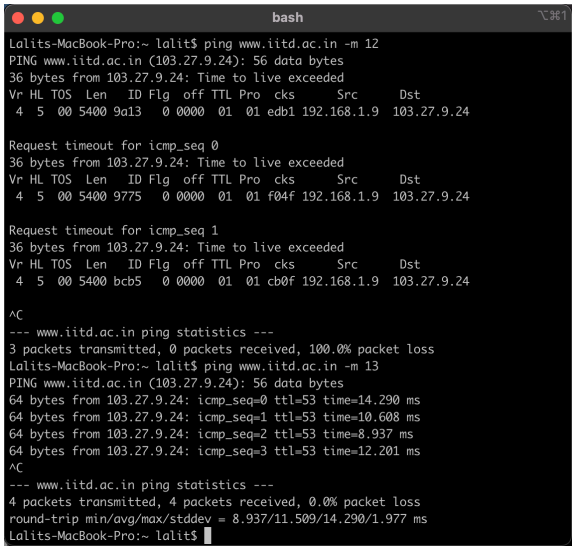
On default DNS server(192.168.1.1) -> www.google.com has address 142.250.194.100
-> www.facebook.com has address 157.240.16.35
On Open DNS server(8.8.8.8) -> www.google.com has address 142.250.194.68
-> www.facebook.com has address 157.240.198.35

(c)Below are the ping results for default values of packetsize and parameters for www.iitd.ac.in

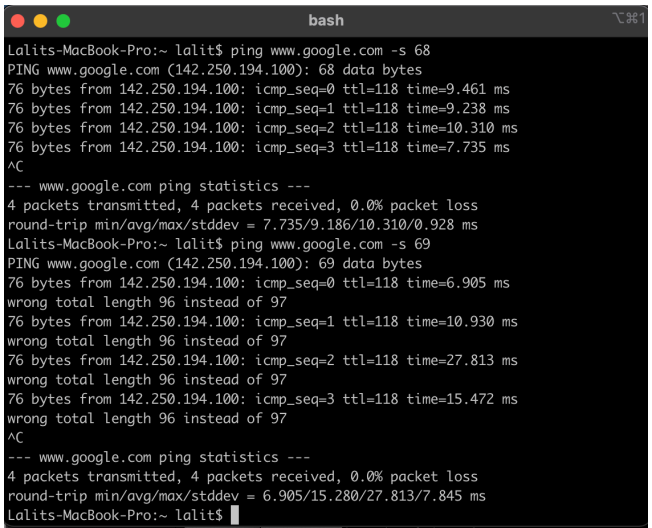


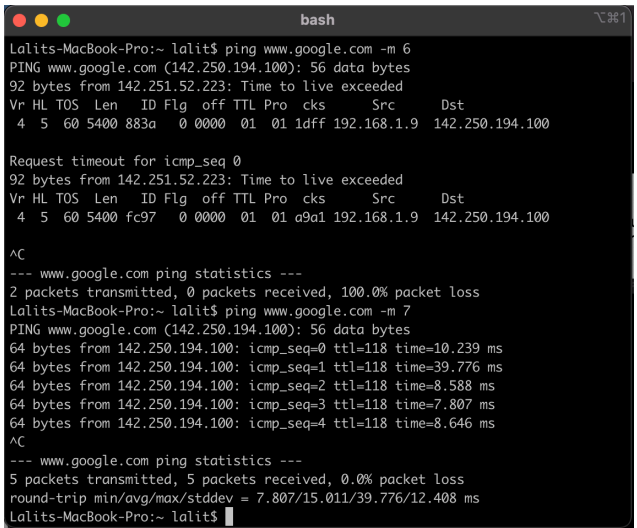
On varying packetsize and TTL, we find maximum packetsize = 1472 databytes + 8 header bytes = 1480 bytes for www.iitd.ac.in. Minimum ttl for packets to reach = 13.



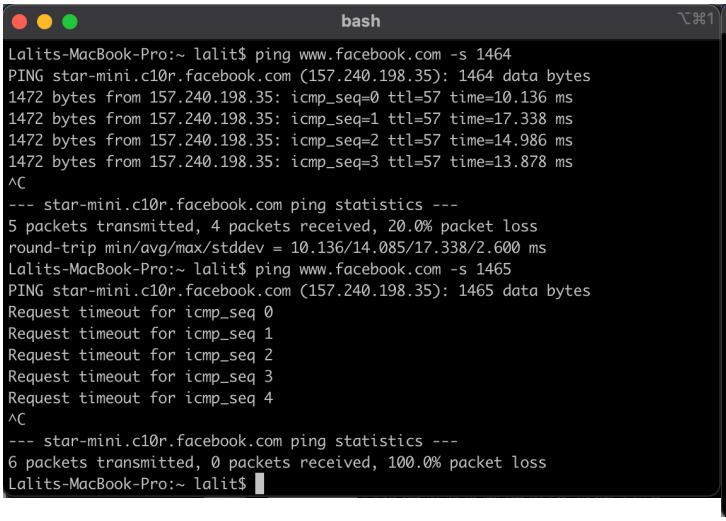


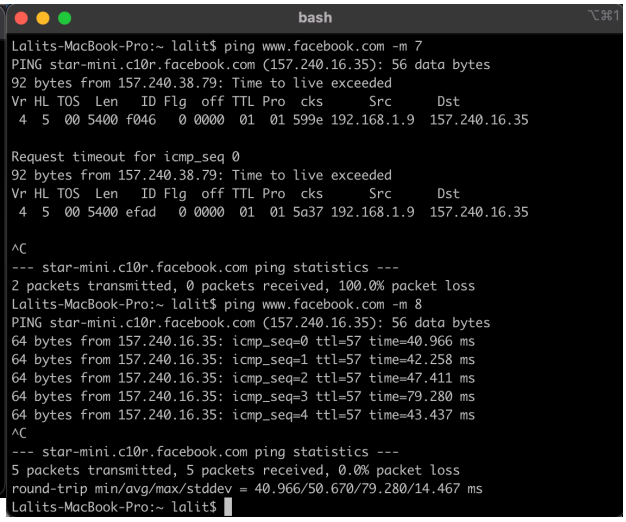
On varying packetsize and TTL, we find maximum packetsize = 68 databytes + 8 header bytes = 76 bytes for www.google.com. Minimum ttl for packets to reach google.com = 7.





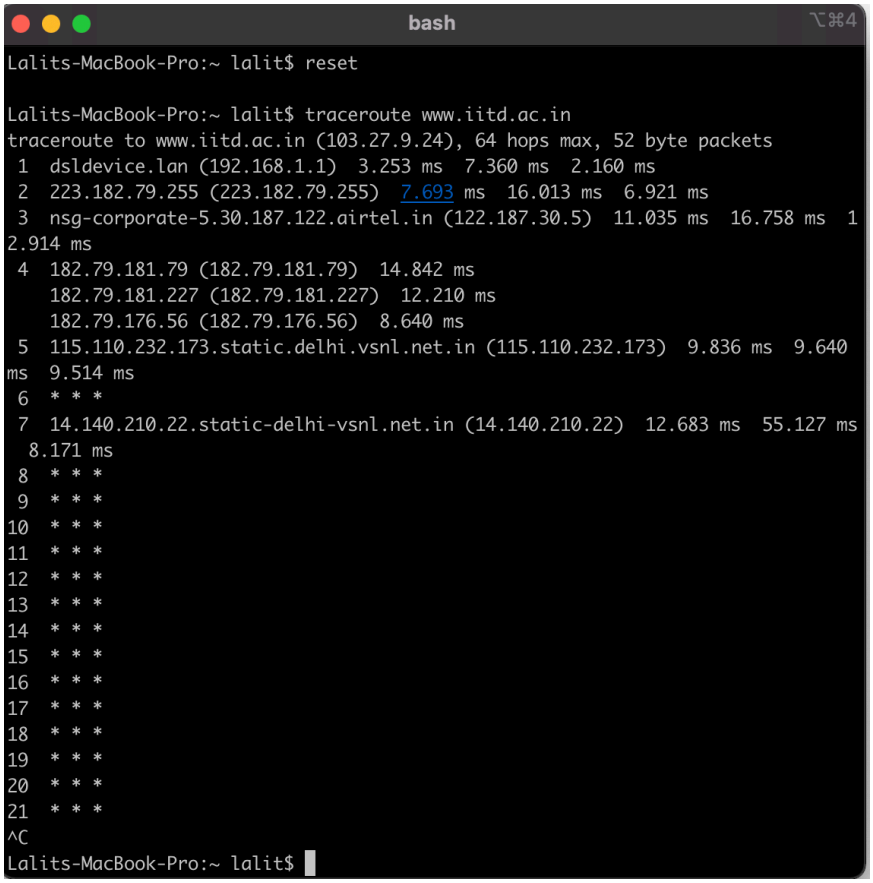
On varying packetsize and TTL, we find maximum packetsize = 1464 databytes + 8 header bytes = 1472 bytes for www.facebook.com. Minimum ttl for packets to reach www.facebook.com = 8.



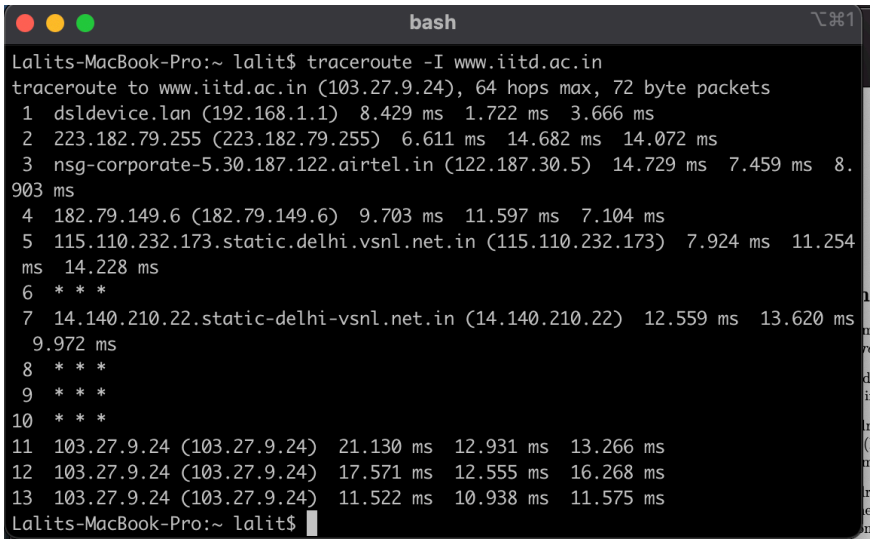


(d)Running traceroute on www.iitd.ac.in, we observe that most of our ping requests do not get responses. This is because by default, traceroute uses UDP ports for tracing hosts. In this case, firewalls block UDP ports and no echo response is sent back by the router.

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)



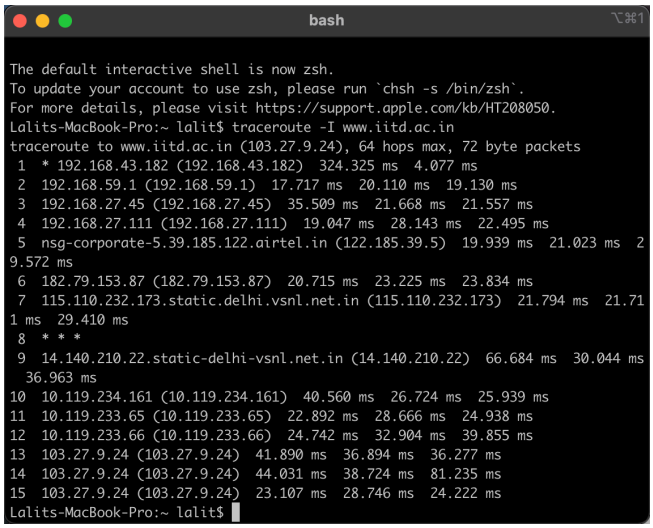
(Traceroute default using UDP packets)

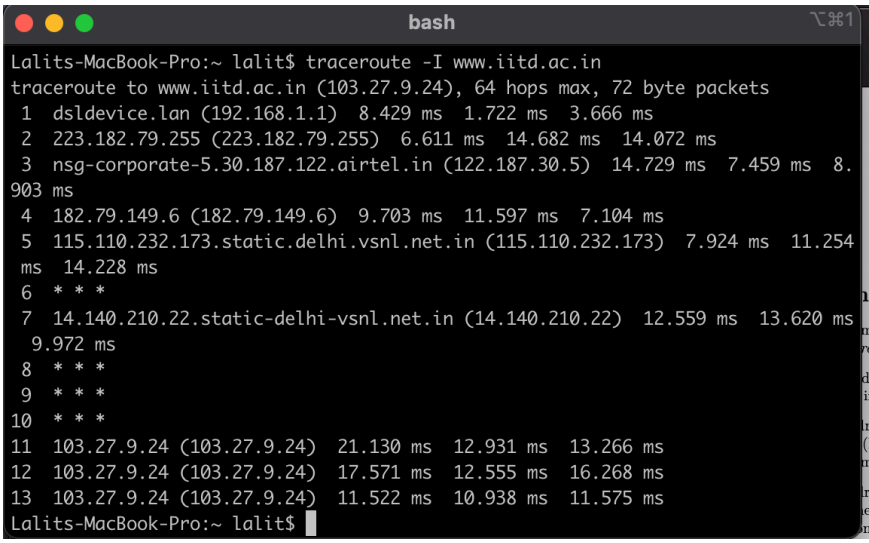


(Traceroute using ICMP packets)

We can also see the differences over different networks(Airtel 4G and WLAN). The inital 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 aree private IPs (likely belonging to IIT Delhi network)



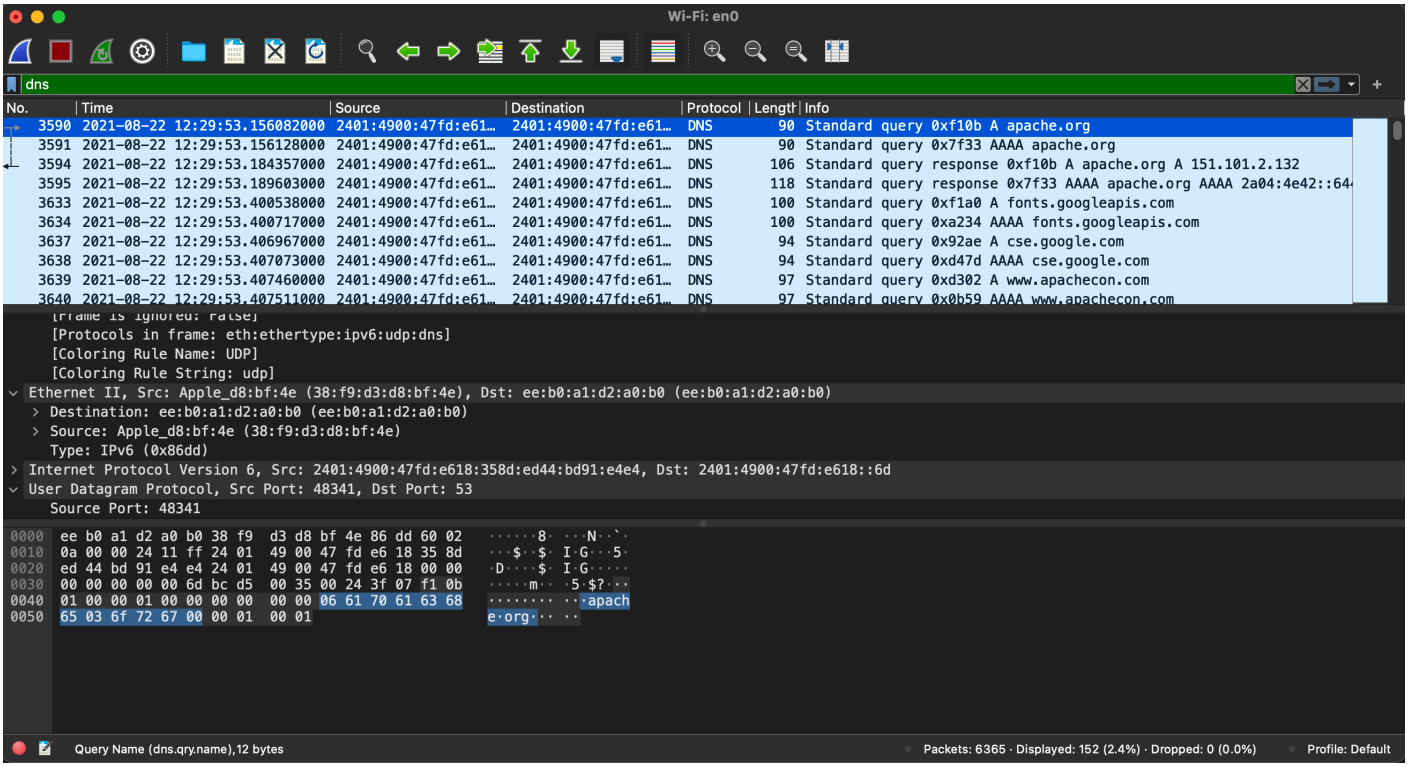


(Airtel 4G - mobile hotspot) *(Airtel WLAN)*

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.

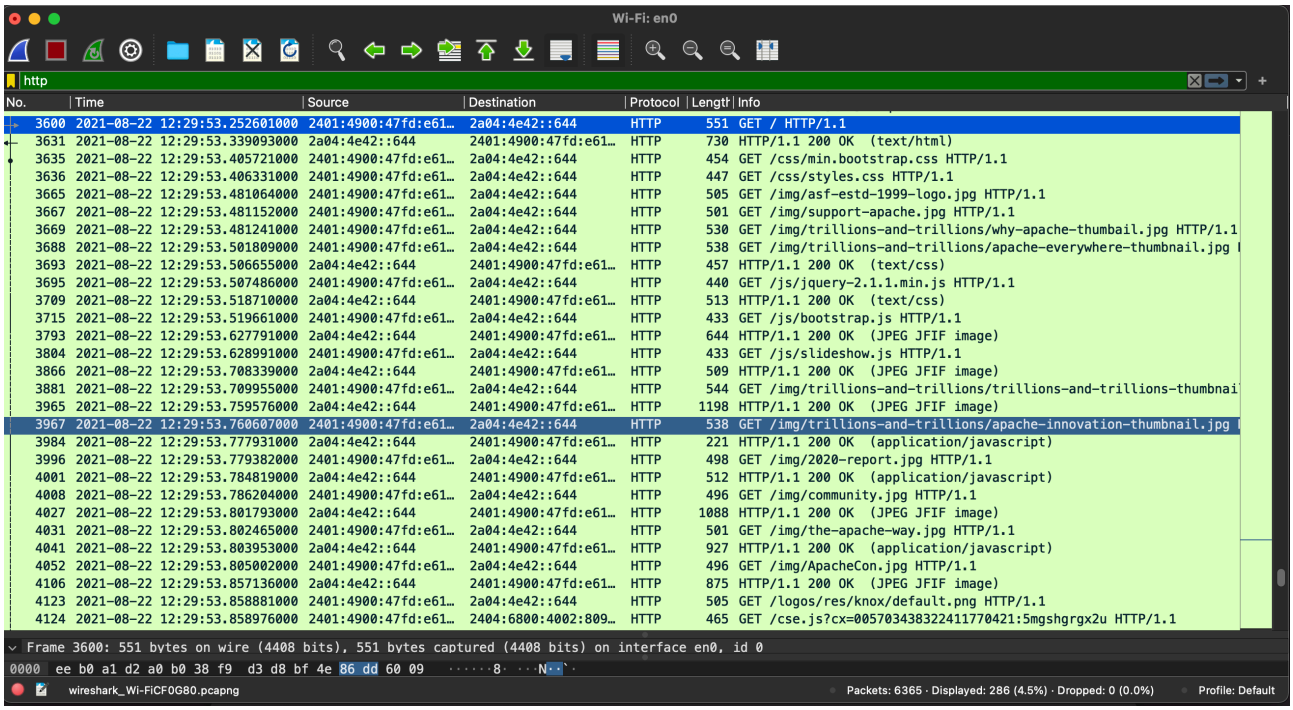


For IPv4 DNS request, time difference between request and response is 28.275ms

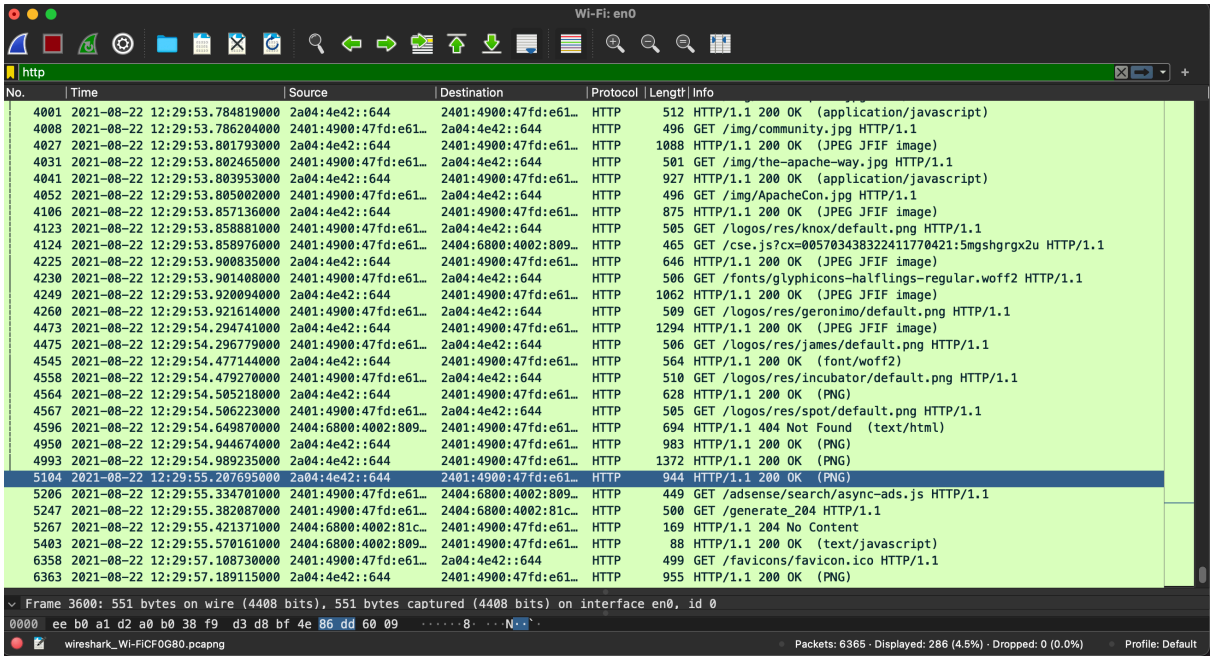
For IPv6 DNS request, time difference between request and response is 33.475ms

(b)

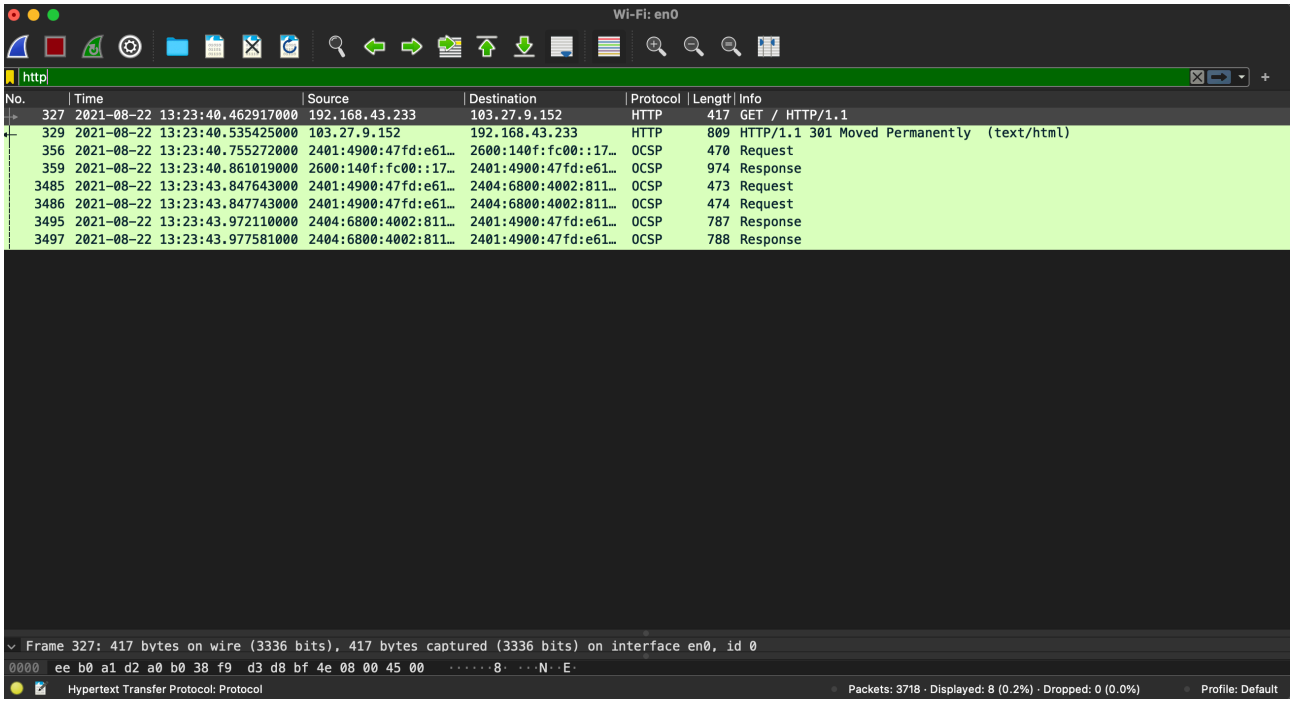
On applying the HTTP filter, we observe that there were approximately 30 HTTP requests(not counting the responses), all of them were GET requests. We can also see the order of Get Requests(response packets need not be in order). First GET request is for html file, followed by css, thumbnails(i.e. the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



(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.

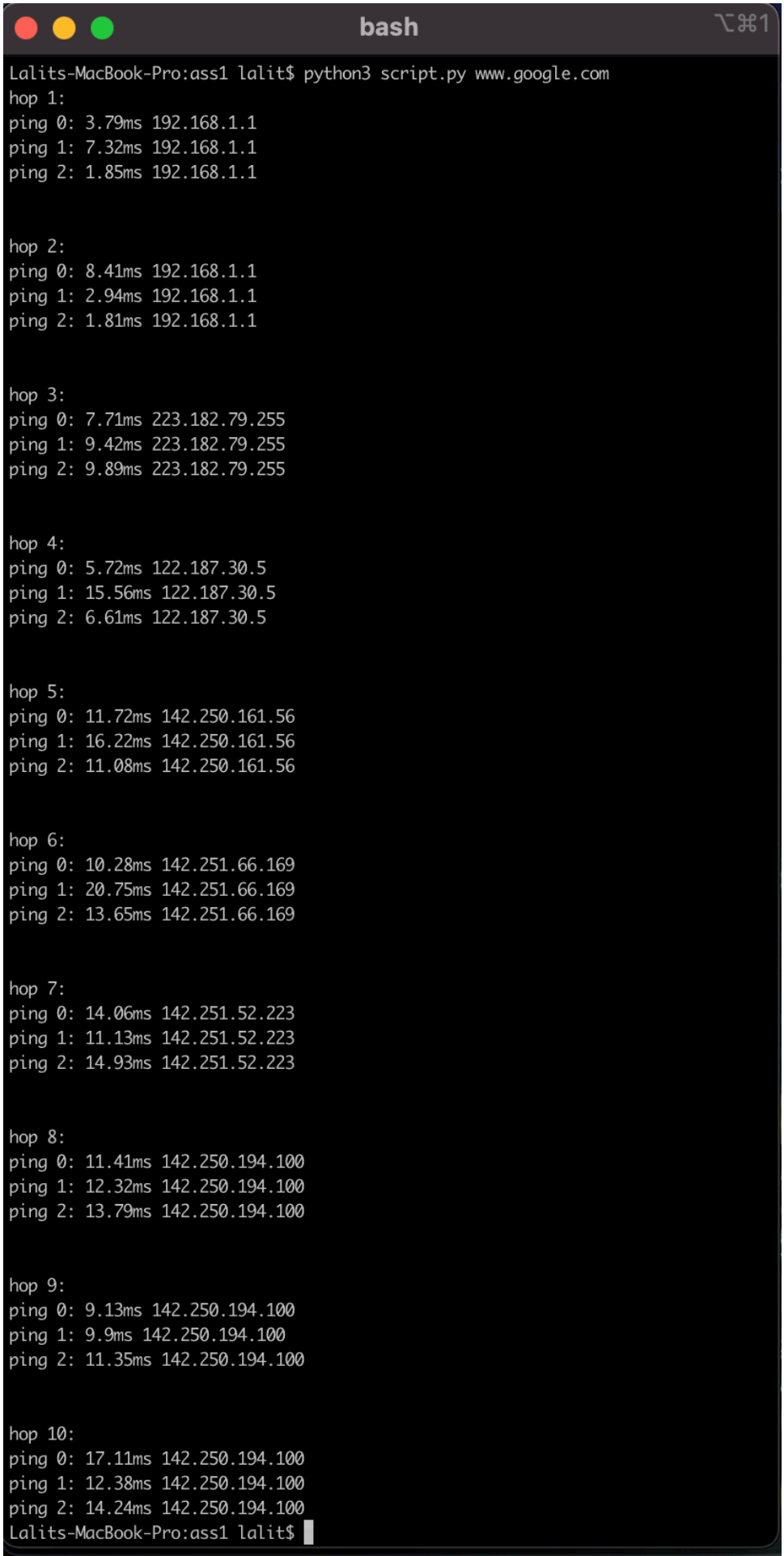


(d)Below, we can see the results of http filter when http://cse.iitd.ac.in/ .In case of apache.org, the response to HTTP request was 200 OK, but here the response is 301(Moved Permanently). A likely reason for this to occur is that all HTTP requests are redirected to HTTPS requests(visible using tls 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.

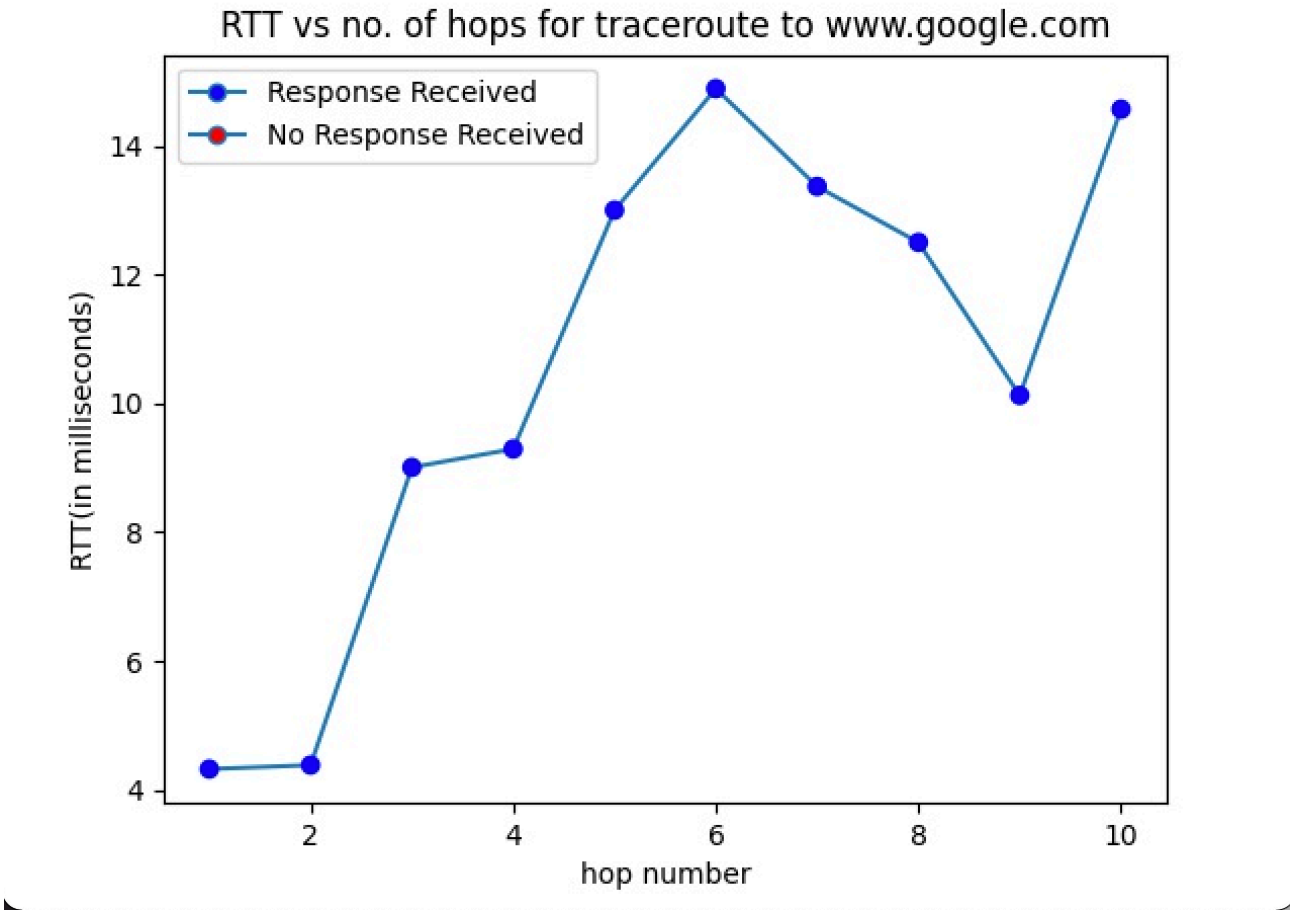


3. Implement traceroute using ping

Given below is the output of the traceroute implementation on www.google.com



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 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