Assignment 1 - COL334

Aayush Goyal

August 2021

1 Networking Tools

1.1 ifconfig

For this part I have considered the private IP address of my machine provided by the router. The router provides each machine a IP address and this changes when we change the Internet service provider is changed. When the command "ifconfig" is run in the terminal, once with Jio Mobile Hotspot and second time with IITD WiFi the IPv4 and IPv6 both were different as we can see in the below images (IPv4 - inet value in the first line and IPv6 - inet6 value in the third line)

Figure 1: IP Address with IITD WiFi

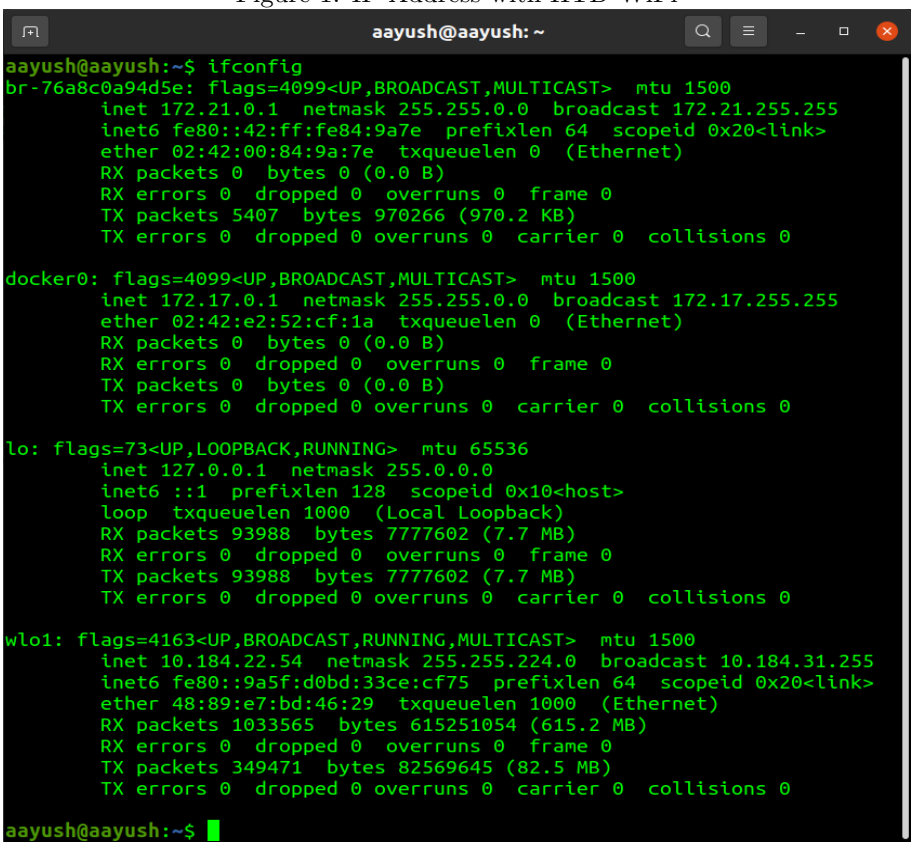
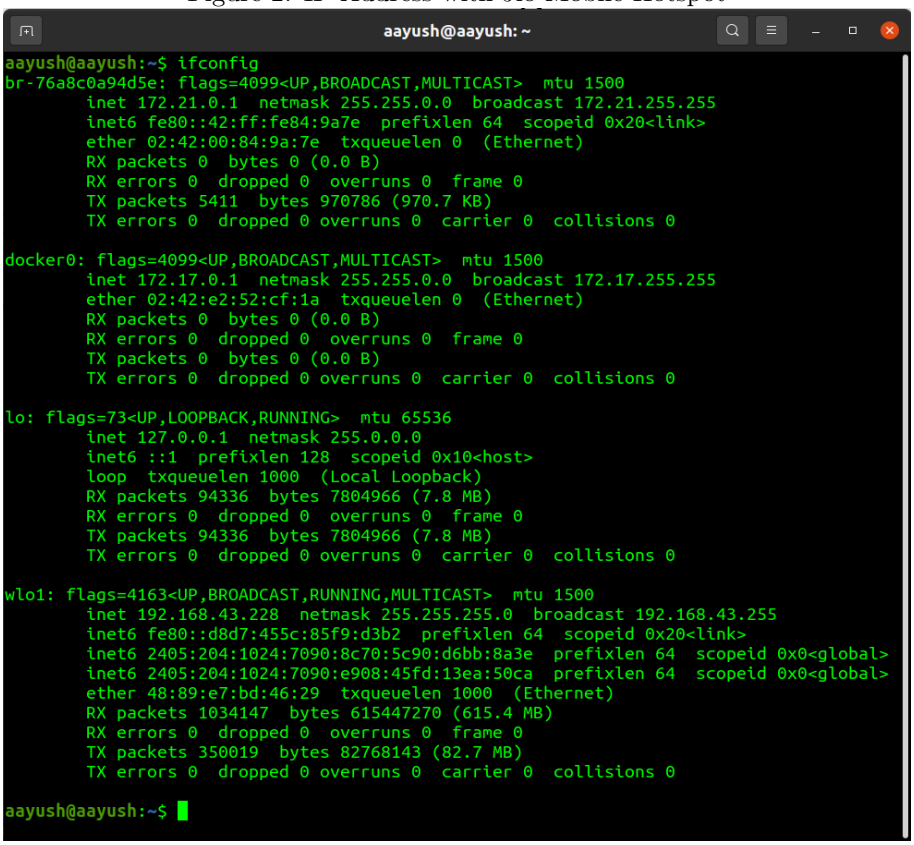


Figure 2: IP Address with Jio Mobile Hotspot



1.2 nslookup

The "nslookup" command is used to find the IPv4 and IPv6 address associated with a domain name. This keeps changing even for the same DNS server. For human beings it is not easy to remember the the IP address of a server, so they are given a domain name, but for computer we need the IP address and hence the DNS servers help in this conversion from domain name to it's IP. Domain names like www.google.com have many IP addresses reserved with it, thus depending on the DNS server to which we are asking, the resultant IPv4 and IPv6 values reported maybe different.

Figure 3: nameserver lookup using 127.0.0.53 DNS server

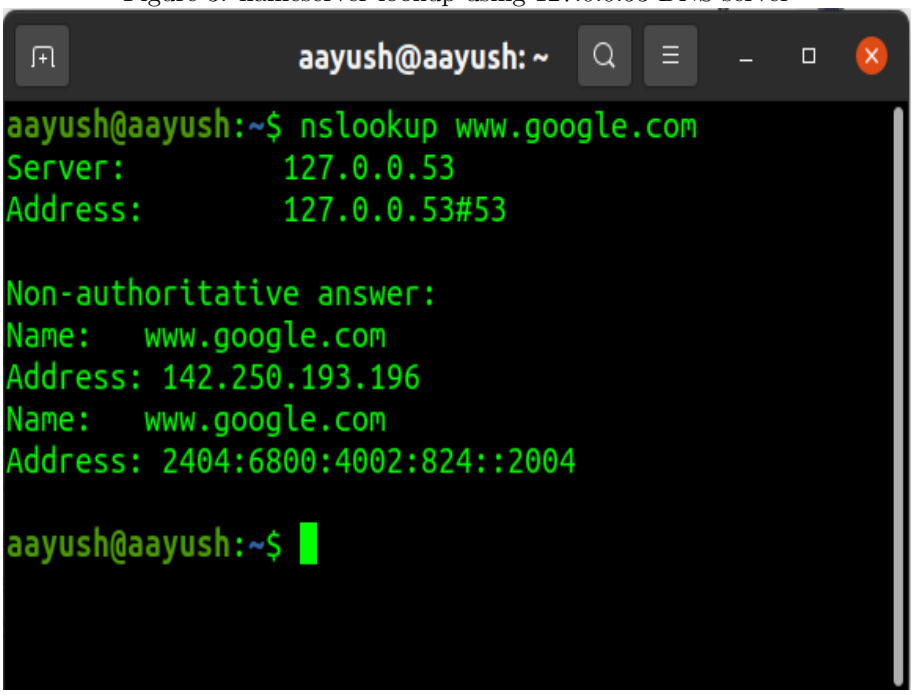
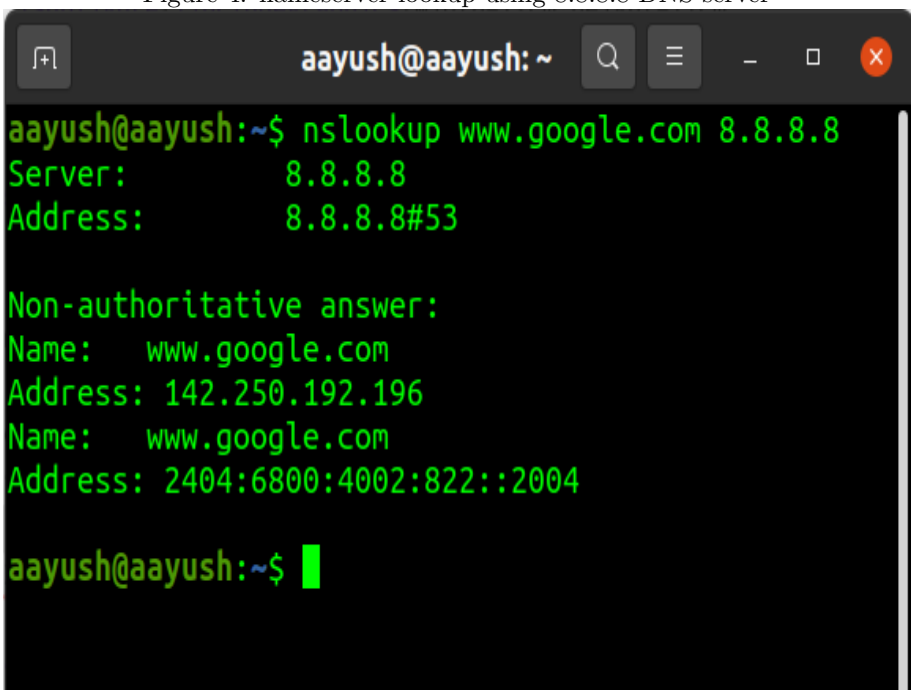


Figure 4: nameserver lookup using 8.8.8.8 DNS server



1.3 ping

The ping command is used to check whether a particular host is reachable across an IP network, by sending an ICMP packet and checking the response. This can be used to communicate with various IPs.

To find the maximum packet size for which the domain responds, binary search on the final possible value can be done. For this we send the domain some packets of a size and based on the response we can determine whether the it is the optimal value or the actual value is smaller or bigger.

For this I made a python script which will ping the domain and by doing a binary search found the maximum size for which we can get back a response.

The maximum data packet size that we can send turned out to be 65399. The maximum data packet size that we can receive a response for is same for both www.facebook.com and www.google.com and the value turned out to be 1472. Whereas for www.iitd.ac.in, since I am connected on the IITD WiFi, that is the Local Network, I was able to receive a response for the maximum packet size that we can send ie 65399.

Figure 5: Binary search for www.google.com

Figure 6: Binary search for www.facebook.com

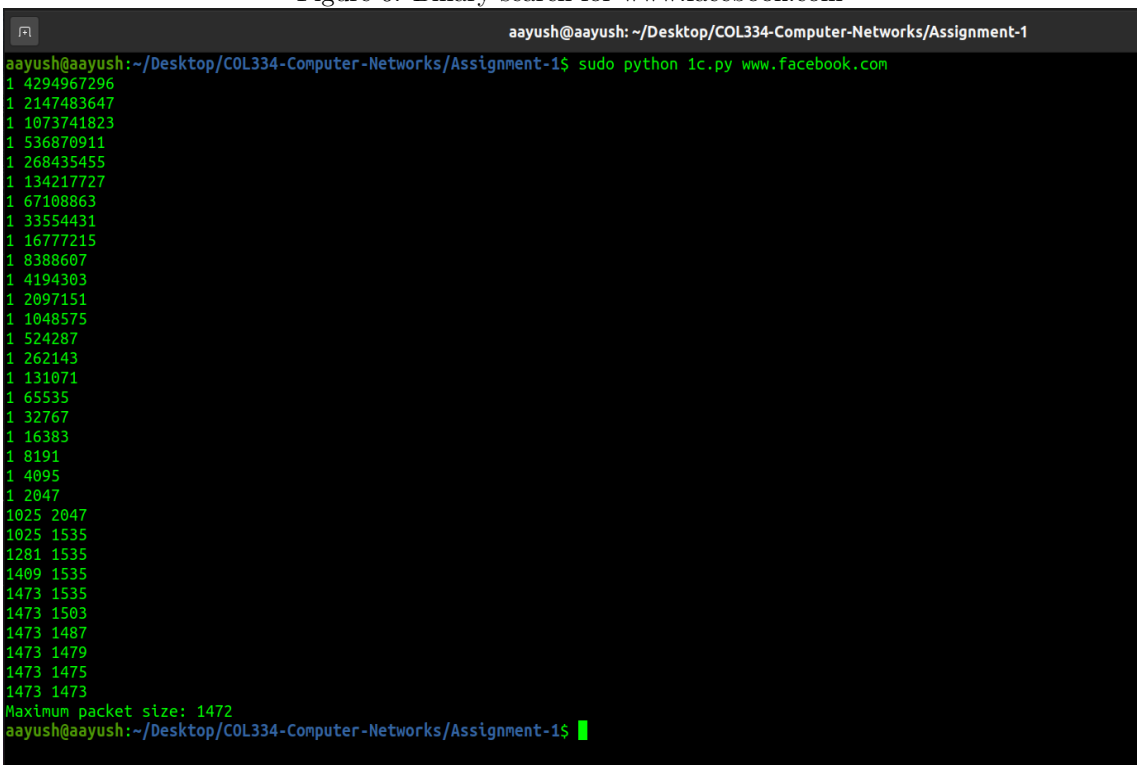
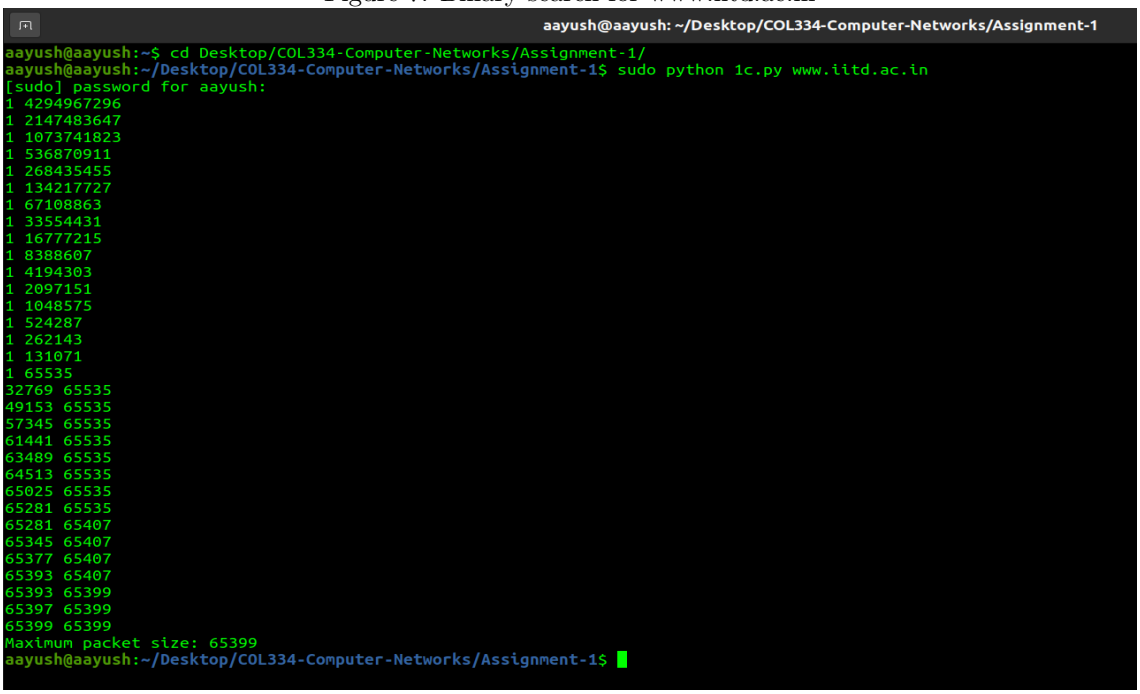


Figure 7: Binary search for www.iitd.ac.in



1.4 traceroute

When the packet is sent from the source to the destination IP address, it goes through a number of routers on the way. Traceroute command helps us to identify the the IPs of the routers we have encountered on the way. -4 flag can be used to print the IPv4 address forcibly. With this we can determine the IP of a router 'x' hops away from the source and also the Round trip time from the source to that router. The route taken to reach the final destination address is different with different ISPs, like say when we are reaching www.iitd.ac.in using "Jio" the routers are different from the routers we get when we reach wwww.iitd.ac.in using Local Area Network.

Figure 8: Trace route using IITD WiFi

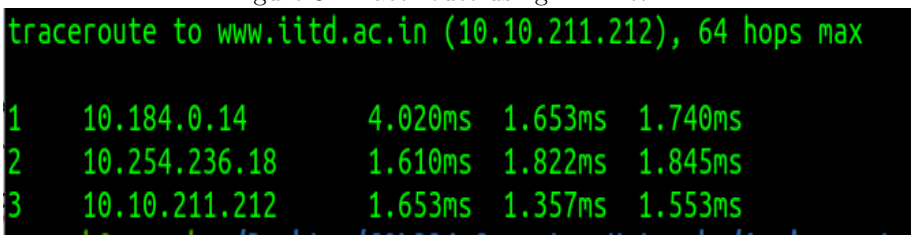
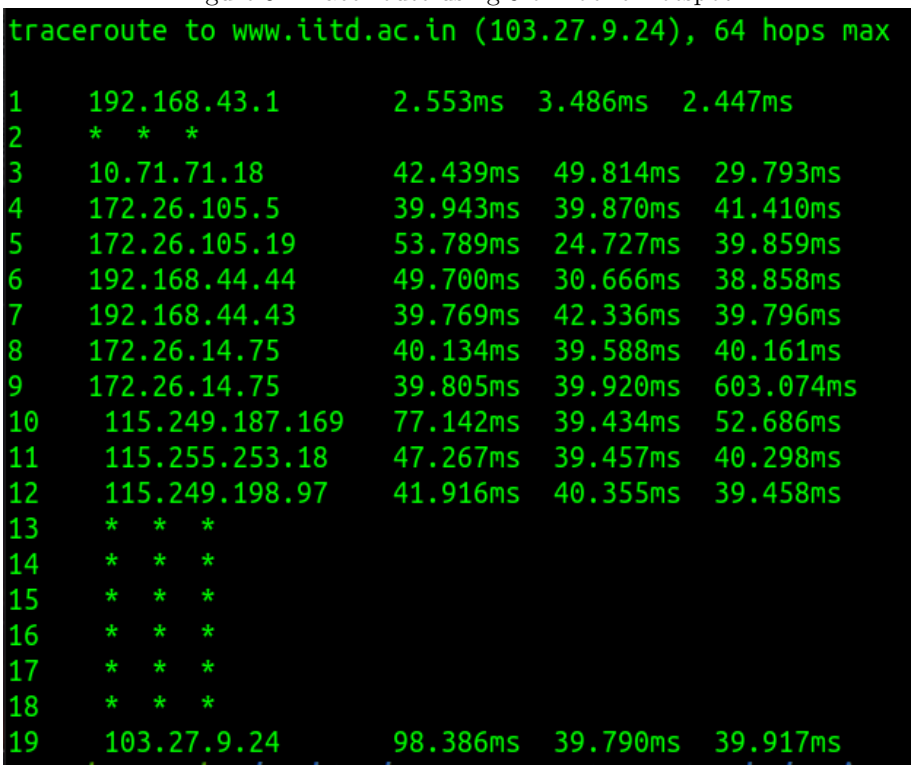


Figure 9: Trace route using Jio Mobile Hotspot



2 Packet Analysis

2.1

The time taken for DNS request-response to complete was around 3.2ms

2.2

Number of http requests were around 27. This shows that the whole web page is not loaded at once. Parts of the webpage load and we can't tell what the web page is going to be. Also the requests were going to different servers and thus we can see that all the data is not stored on the same server, and thus we have to send http requests to the servers where data is present. For images, gifs we have to send additional requests.

2.3

Time to download the web page is:
Start time (first DNS request): 23:00:02.822
End time (Time at which last content object was received): 23:00:04.257
Total time: 1.435s

2.4

There was no http traffic. There was only one http request. When this request is made to the server, the server responds with the code "website moved permanently" and the objects are moved to the https server as cse.iitd.ac.in deals only with encrypted data. The client then converses with the location using TLS encryption.

3 Implementing Traceroute using Ping

3.1 Approach used

The time to live value of the packet that is sent reduces by 1 everytime it hits a router on the route. Thus by making the TTL value of the packet as 'x' we can determine the the IP of the router that is 'x' hops away from the source (here 'x' is less than the minimum ttl value required to successfully reach the final destination).

I used a ICMP socket and created ICMP packets which will be the send to the final destination. Everytime the packet dies we get the response back and the IP address of the router where it died. Using this we have obtained the IP address of the Router on the route. And within the code, by starting the clock just before sending the packet and stopping the clock just after we have received the packet, we can know the Round trip time value. This way RTT value can be determined for every Hop number.

Sometimes the router doesn't respond back and in that case, code might be stuck at the line where we are waiting for the response. For that we can set the timeout value for the socket. So if we are not able to get the response in some "TIMEOUT" time, then raise the exception for that packet and report the RTT value for that packet to be 0.

3.2 Hop number and their RTT values

3.2.1 www.google.com

Figure 10: Routers on route to www.google.com

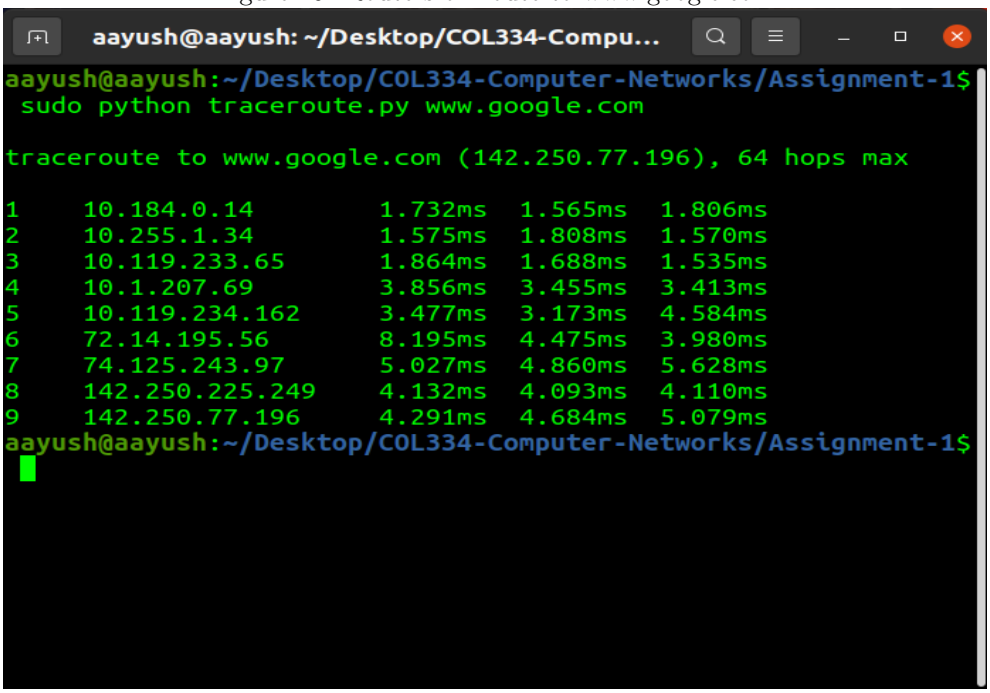
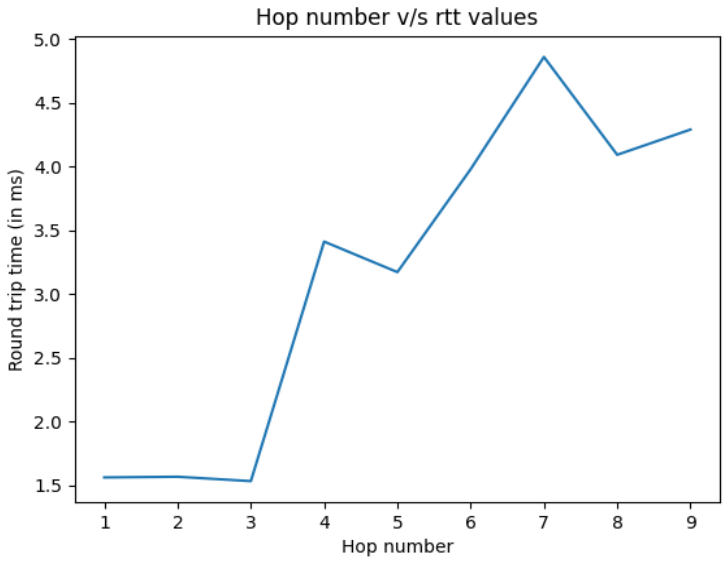


Figure 11: Hop number v/s RTT graph for www.google.com



3.2.2 www.facebook.com

Figure 12: Routers on route to www.facebook.com

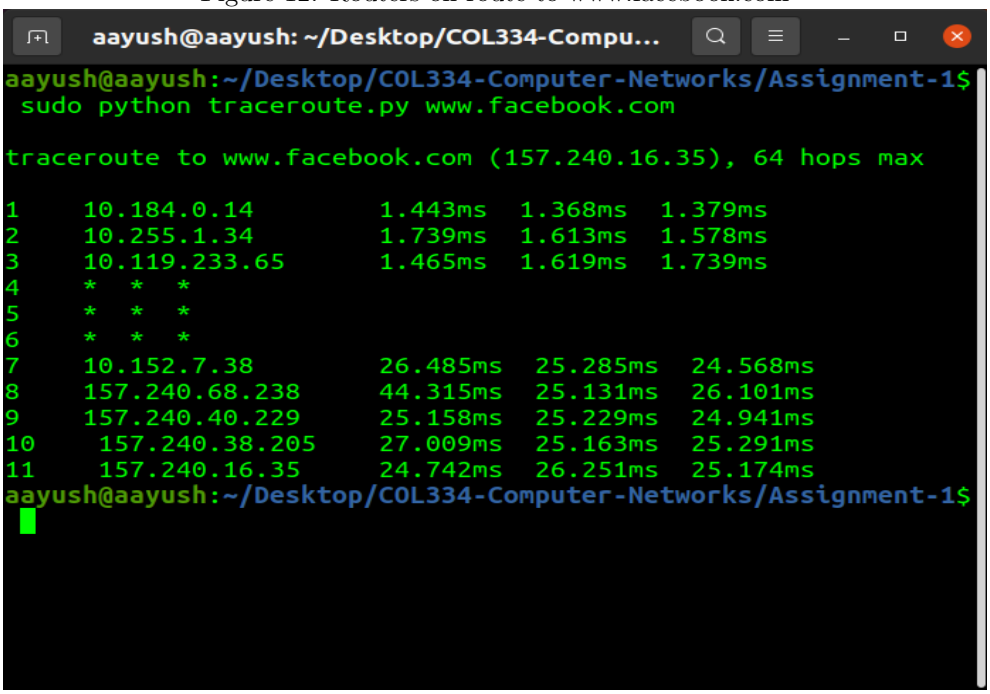
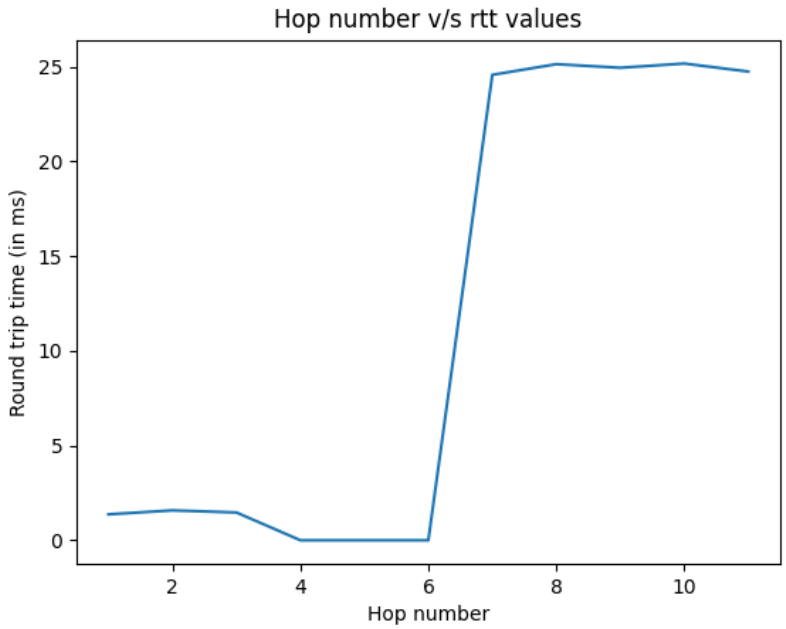


Figure 13: Hop number v/s RTT graph for www.facebook.com



3.2.3 www.iitd.ac.in

Figure 14: Routers on route to www.iitd.ac.in

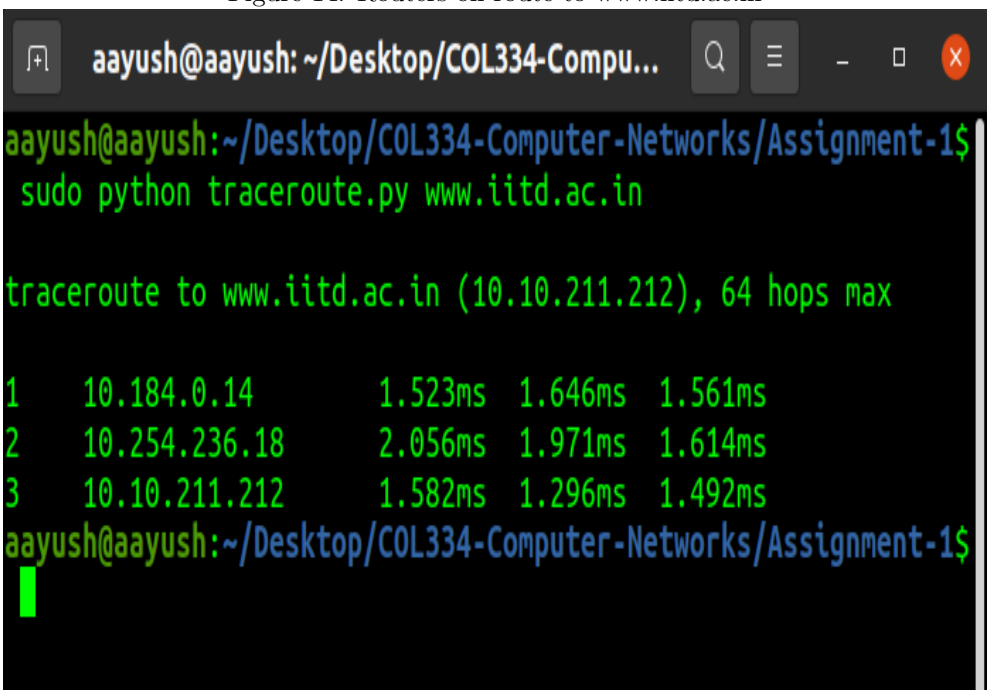


Figure 15: Hop number v/s RTT graph for www.iitd.ac.in