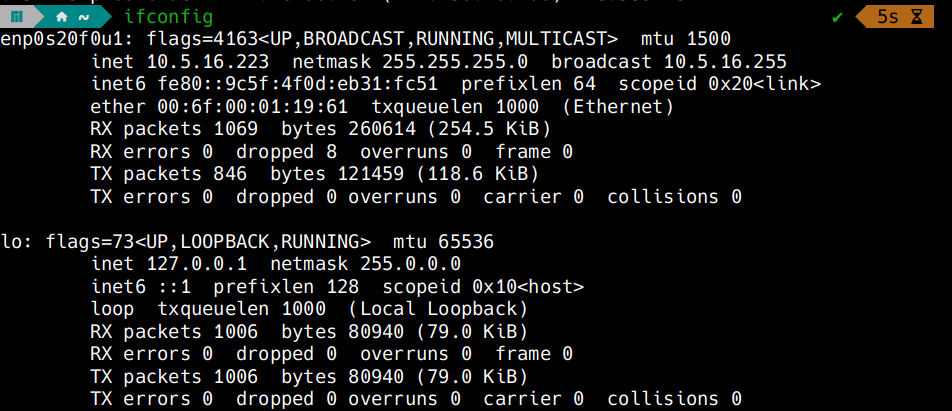
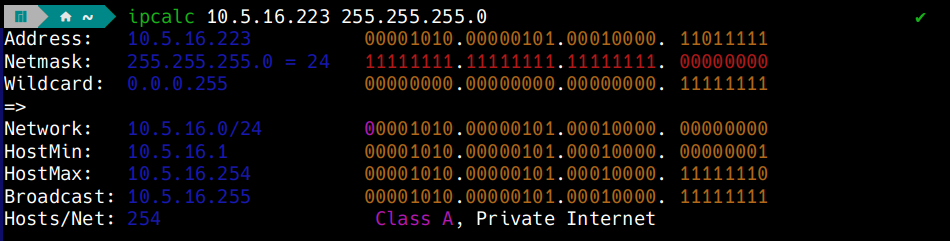
**Part 1**

1.

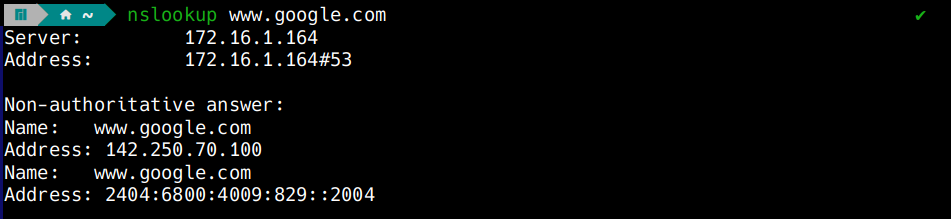


So my IP Address for the Ethernet connection is 10.5.16.223(enp0s20f0u1, the other is for the localhost).

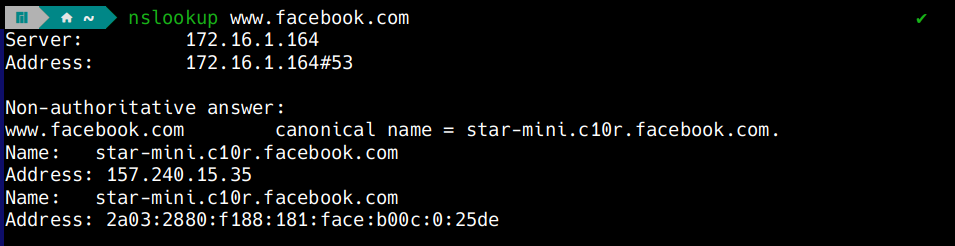
As in the screenshot, the subnet mask is 255.255.255.0.



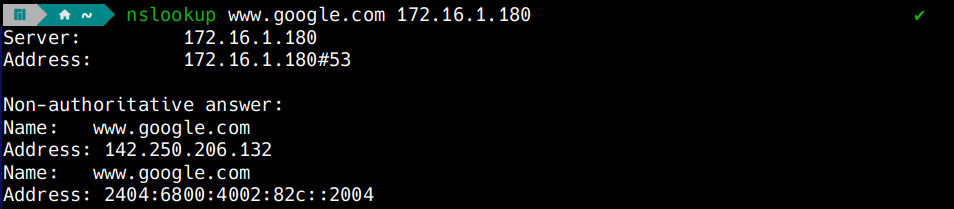
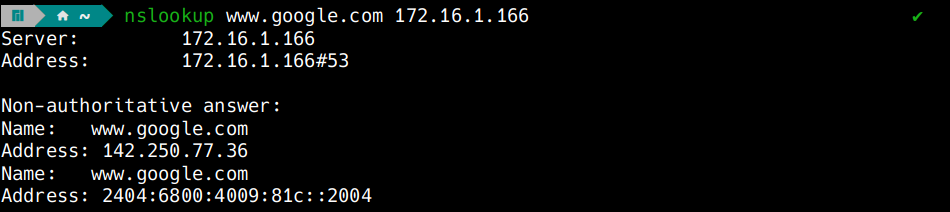
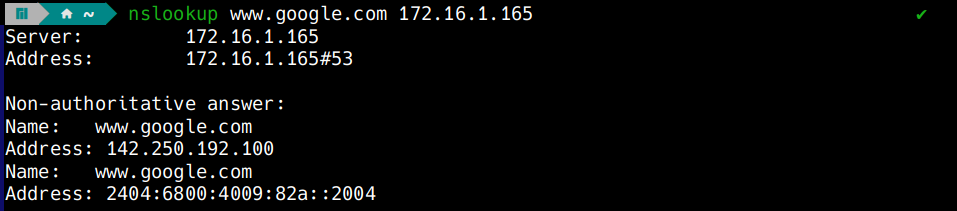
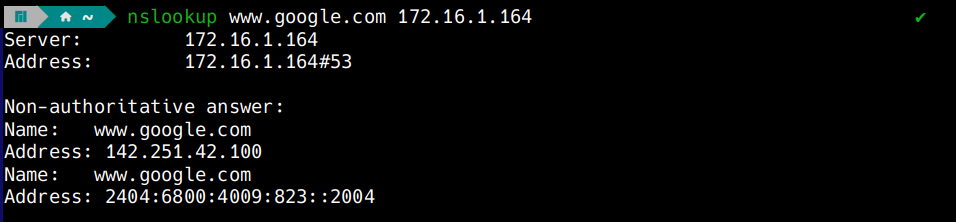
The Network ID is the AND of IP Address and Subnet Mask, we can see it using ipcalc. It is 10.5.16.0/24.



2. The IP Address associated with [www.google.com](http://www.google.com) is 142.250.70.100 (IPv4).



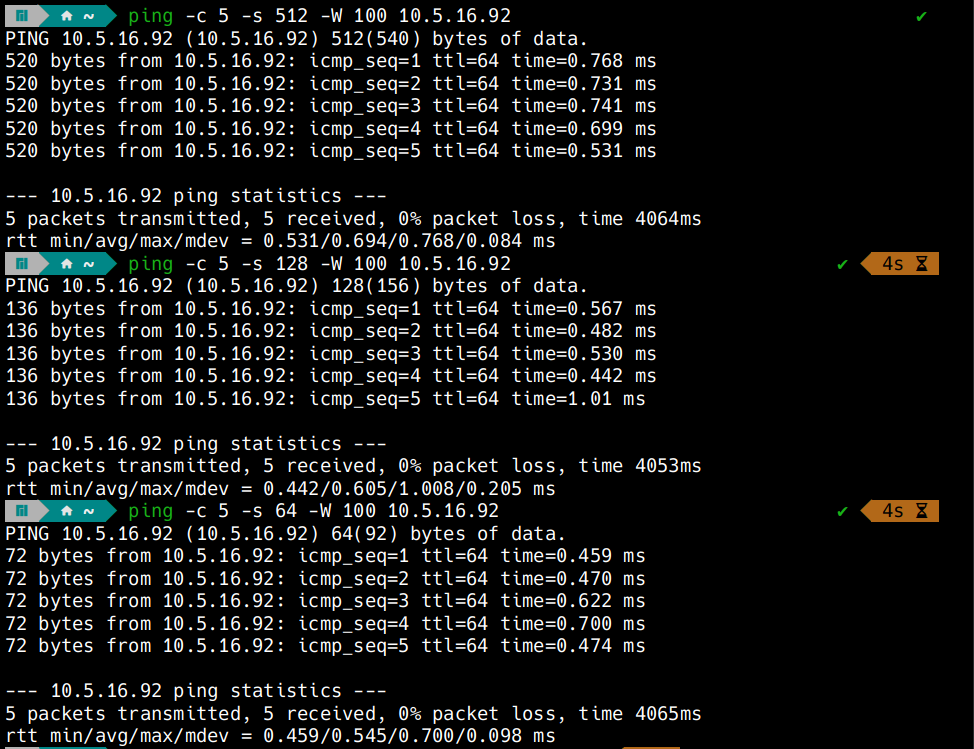
The IP Address associated with [www.facebook.com](http://www.facebook.com) is 157.240.15.35 (IPv4).



So yes, the IP Address indeed does change.

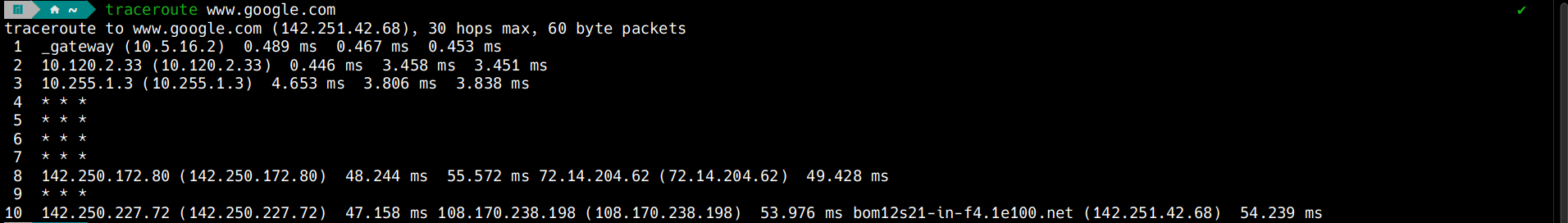
Google uses DNS Load Balancing to distribute traffic across multiple servers. This distributes the user traffic, reduces latency and provides fault tolerance if one of the servers is accidentally down. The different DNS Servers return different IP Addresses from Google’s pool of IP Addresses.

3.



Above is the result of pinging my friends IP Address with different packet sizes of 64, 128, 512 bytes and timeout 100. The terminal output shows the packet loss percentage, min, avg, max, and mdev/stddev of round-trip time.

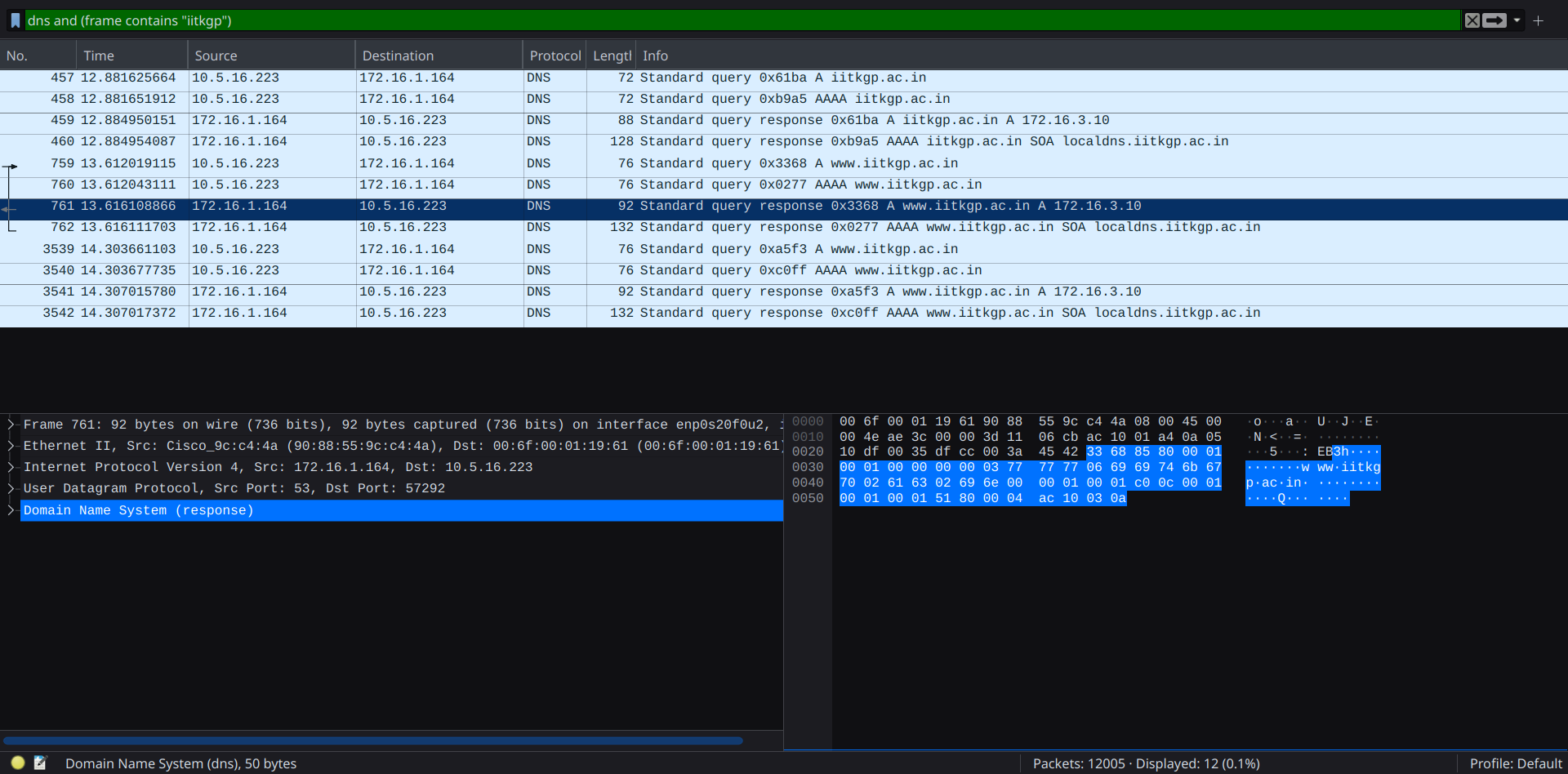
4.



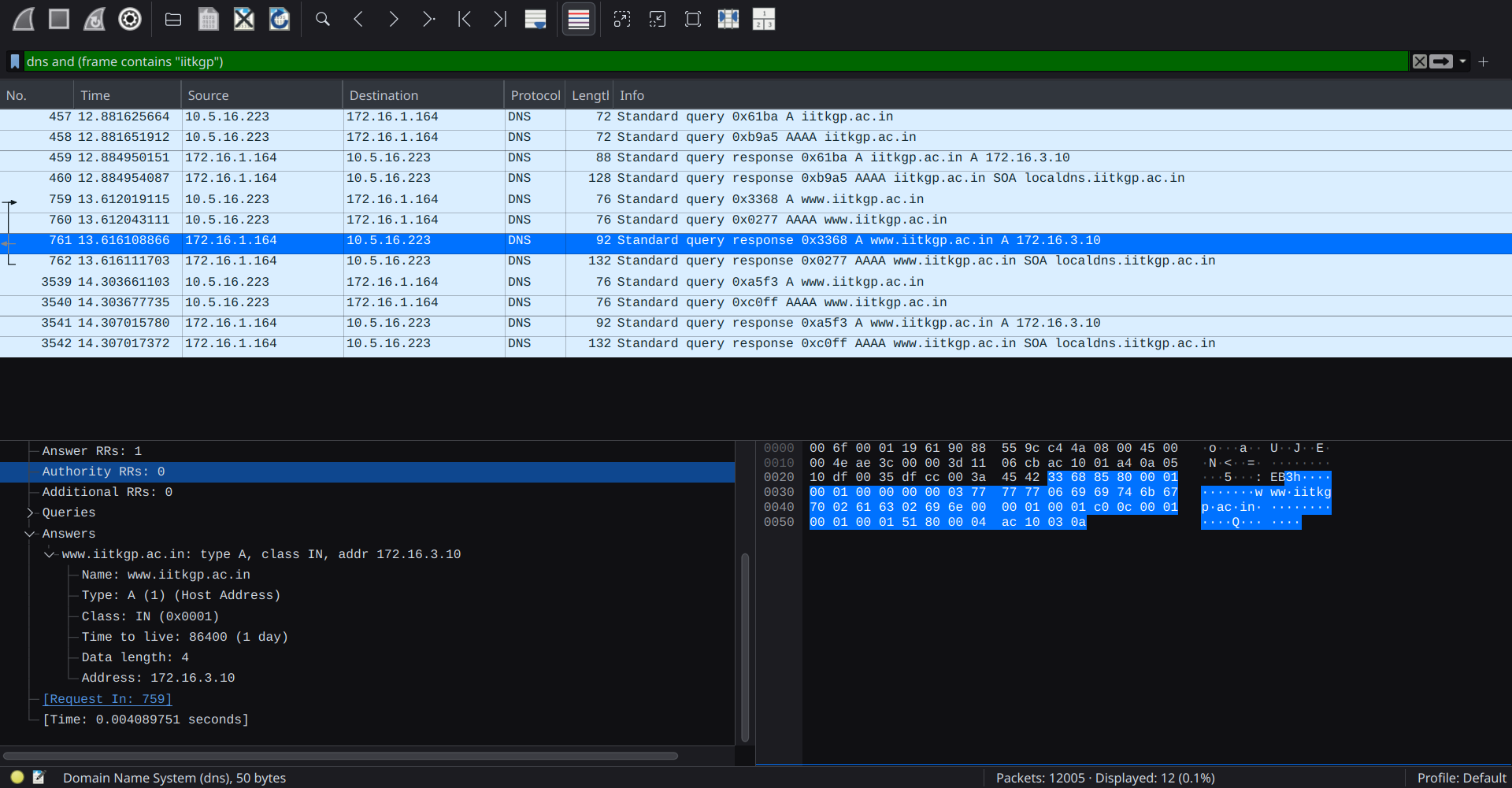
Above is the report of running traceroute for www.google.com. There are 10 lines, so 10 hosts.

The “\* \* \*” basically means that the hop did not respond, which can be due to various reasons like Firewall blocking ICMP, router not responding, packet loss etc

**Part 2**



1. From the screenshot, we can see that DNS is using UDP in the observed packets.



b) The source IP Address of the DNS Query is 10.5.16.223.

The destination IP Address of the DNS Query is 172.16.1.164.

c) As we see in the screenshot, 6 queries are sent from the machine to DNS server during name-to-IP resolution.

d) The DNS Server 172.16.1.164 replies with actual IP Addresses.

e) Only one DNS server is involved, and it does respond.

f) From the screenshot,

Name : iitkgp.ac.in

Type : A (1) (Host Address)

Class : IN (0x0001)

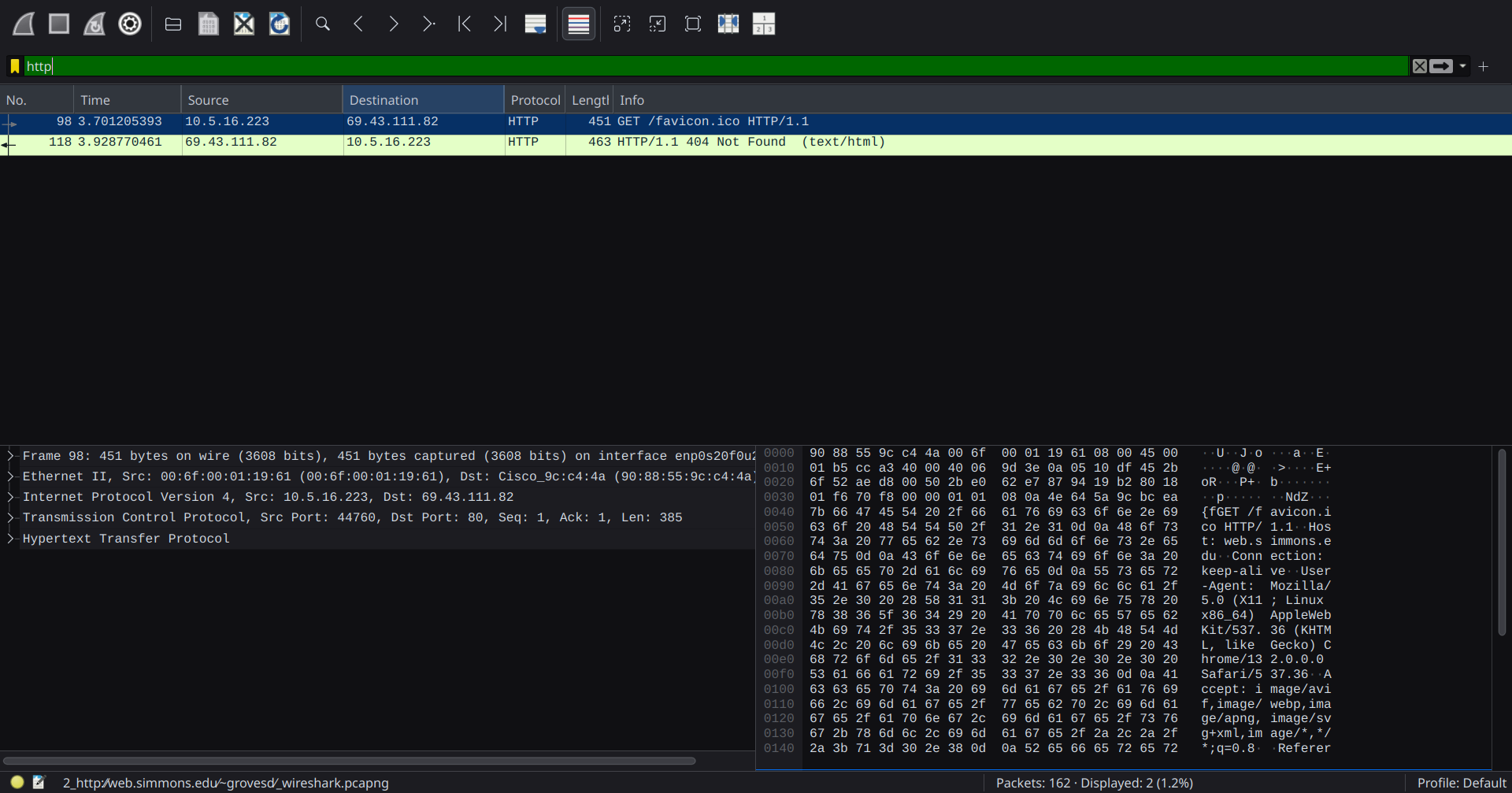
TTL : 86400 (1 day)

Resolved IP Address : 172.16.3.10

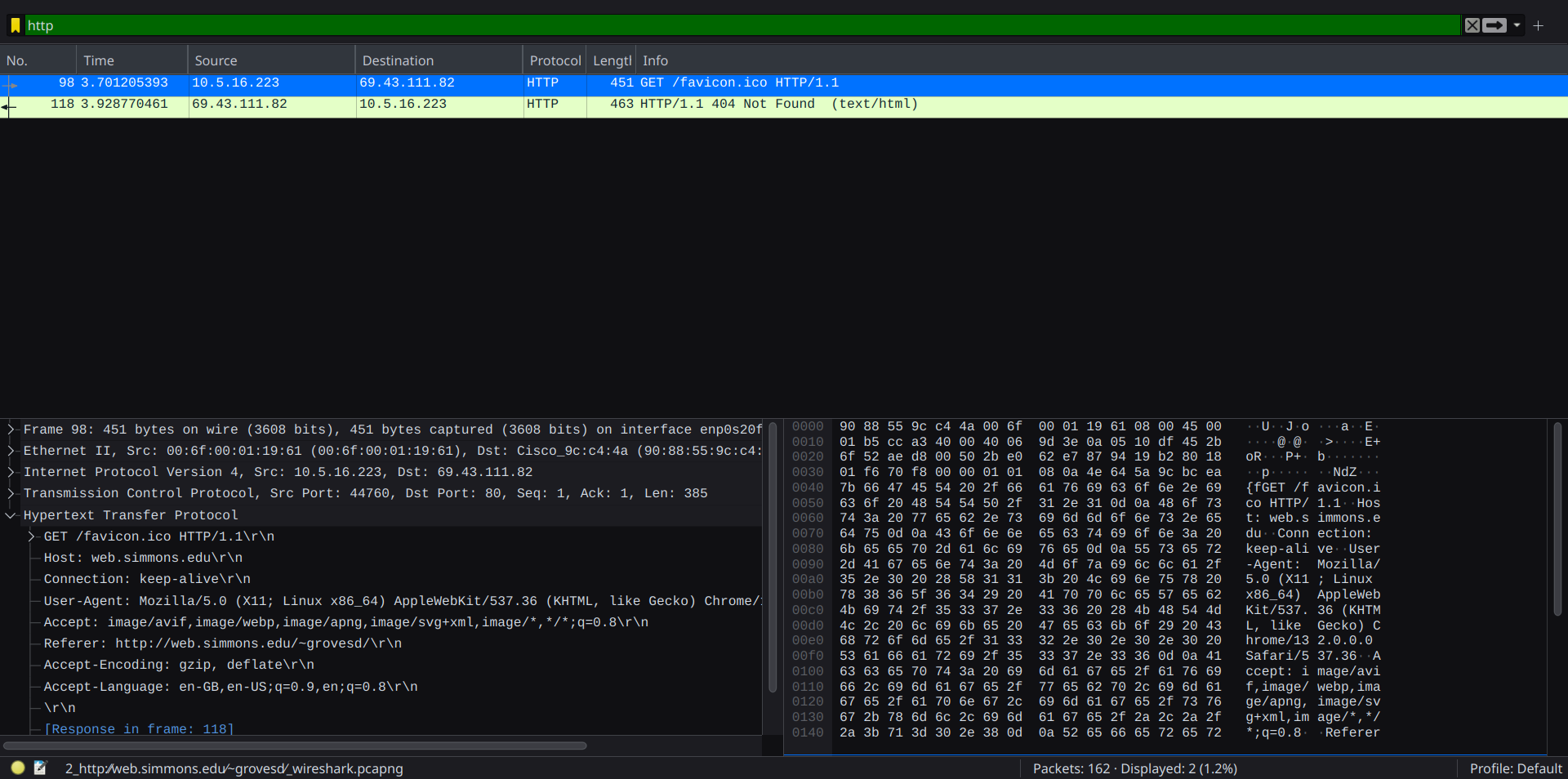
Data length : 4

2.

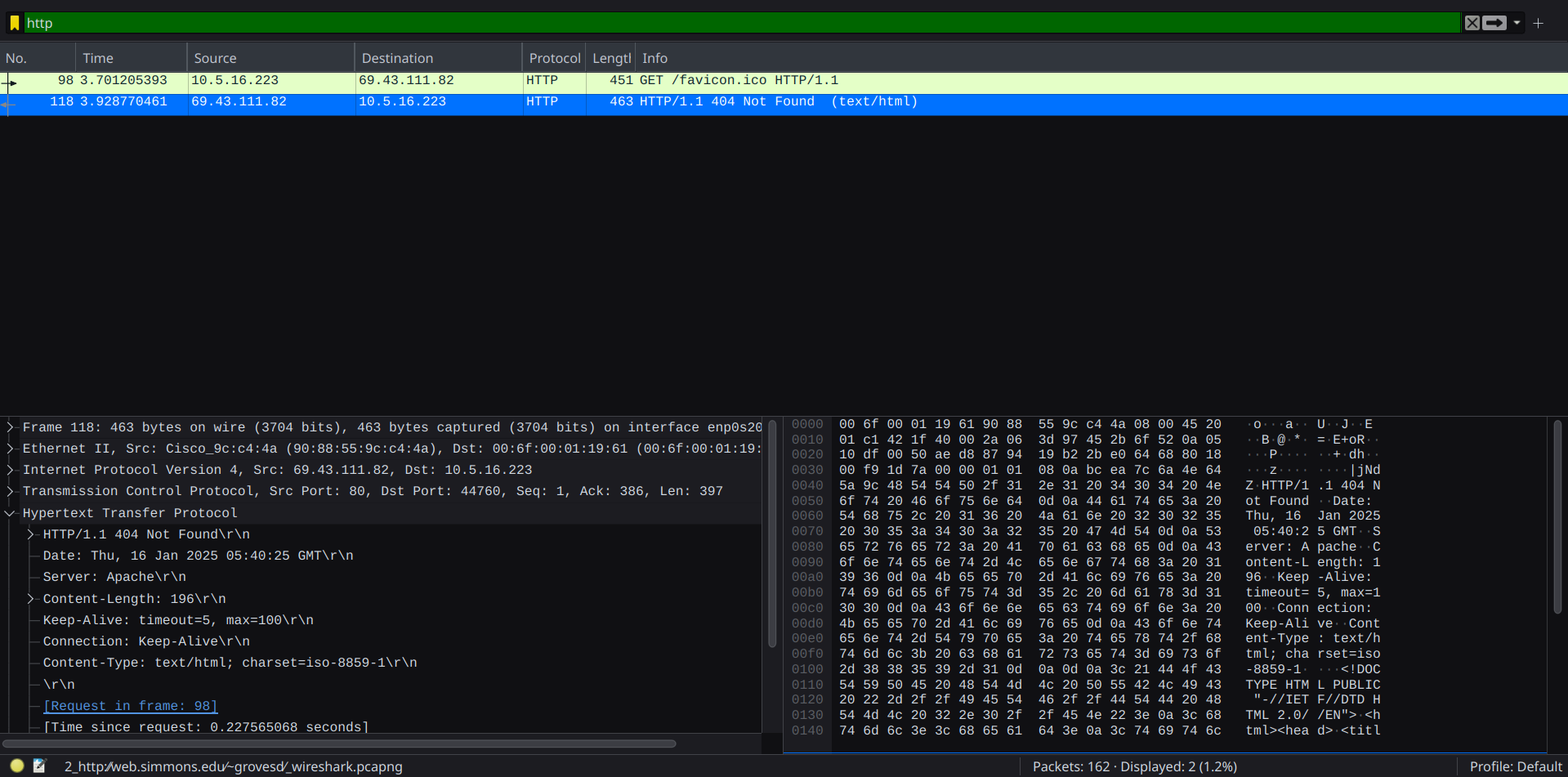
a)



Above is a screenshot of the result after initiating web traffic for the web server <http://web.simmons.edu/~grovesd/> and filtering for http in Wireshark.



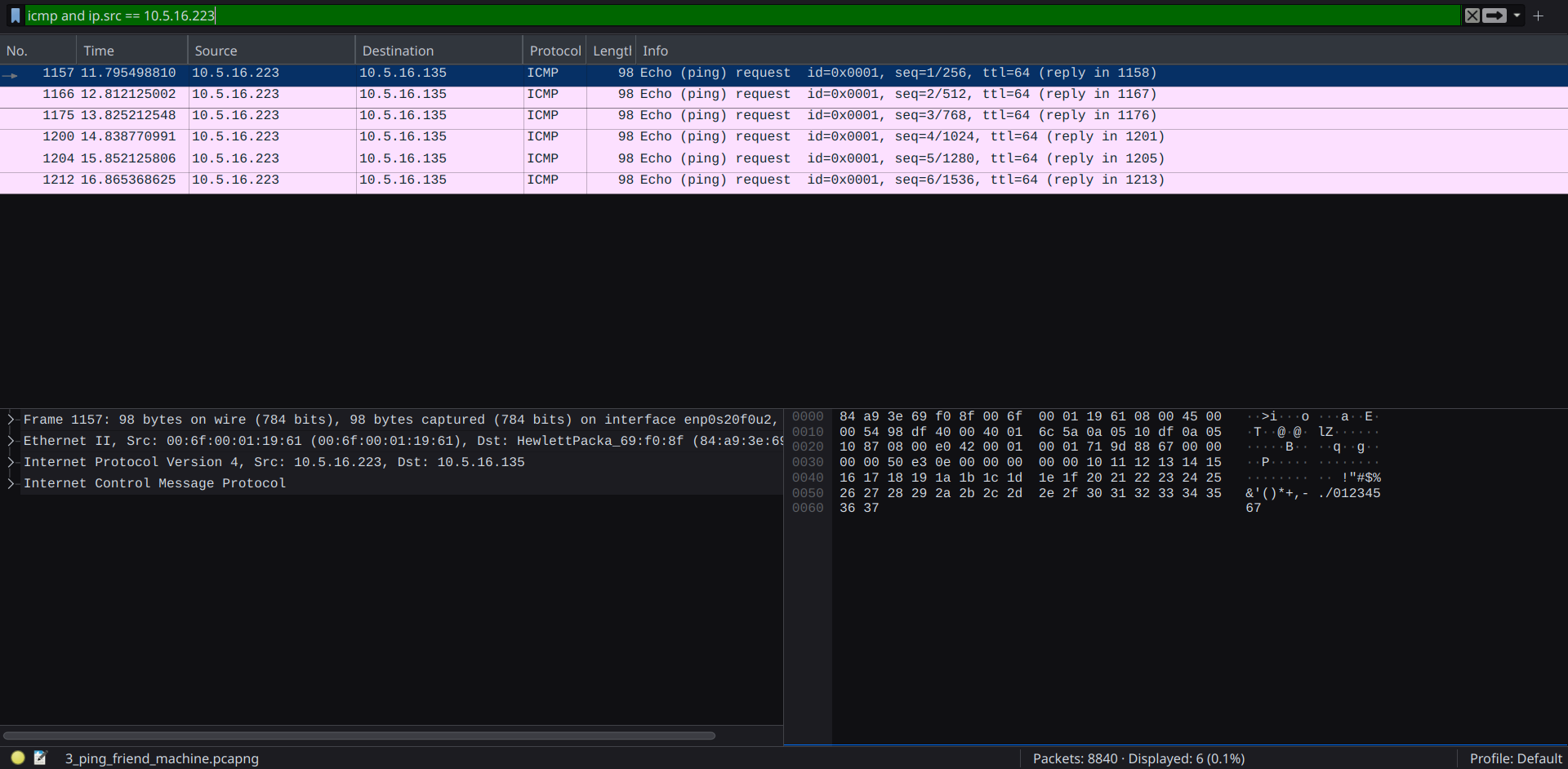
b) This is a screenshot of the above window, with the http request.



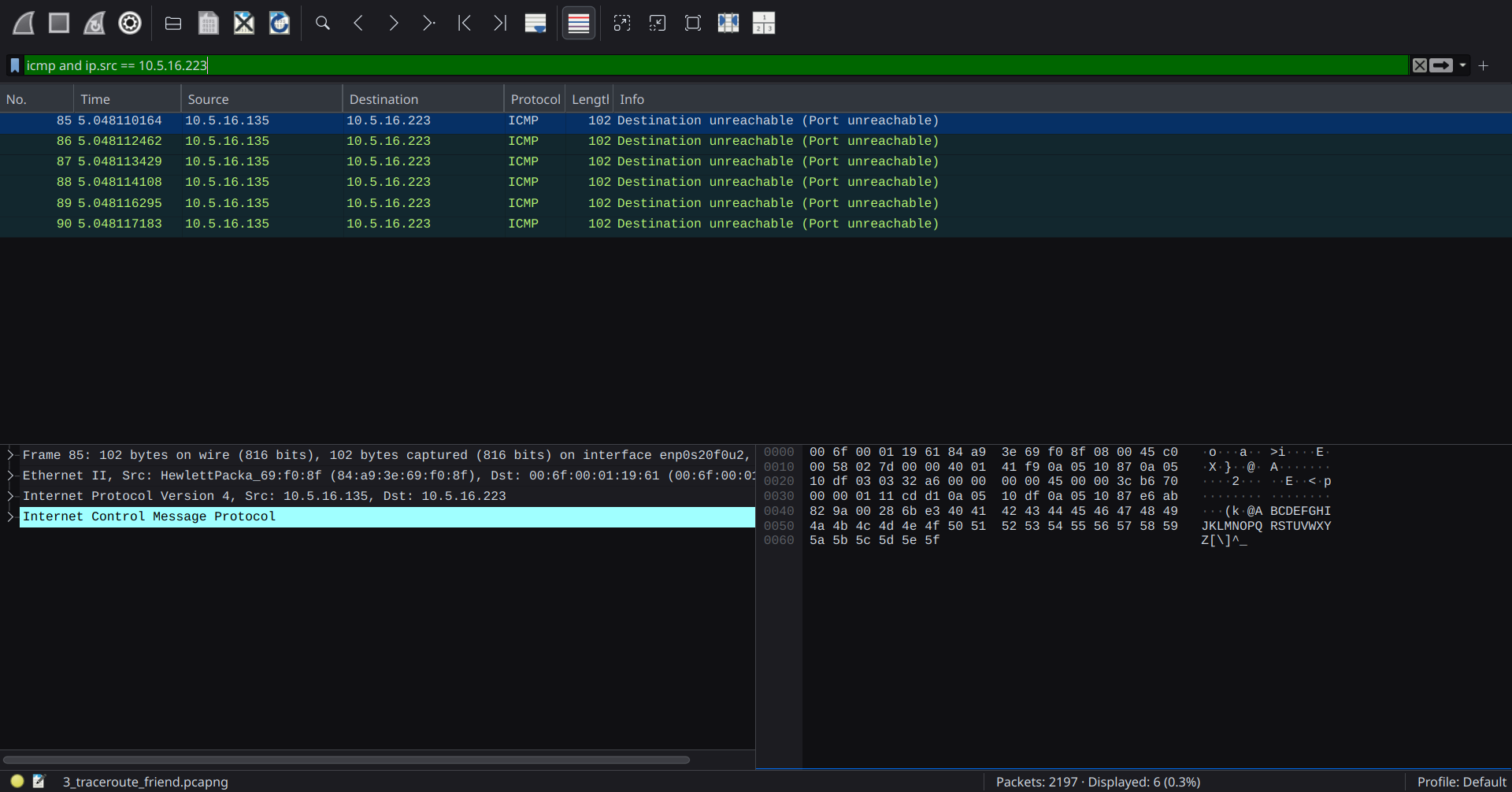
This is a screenshot of the above window, capturing the http response.

c) As we can see, 2 http packets have been exchange between the client and the server.

3.

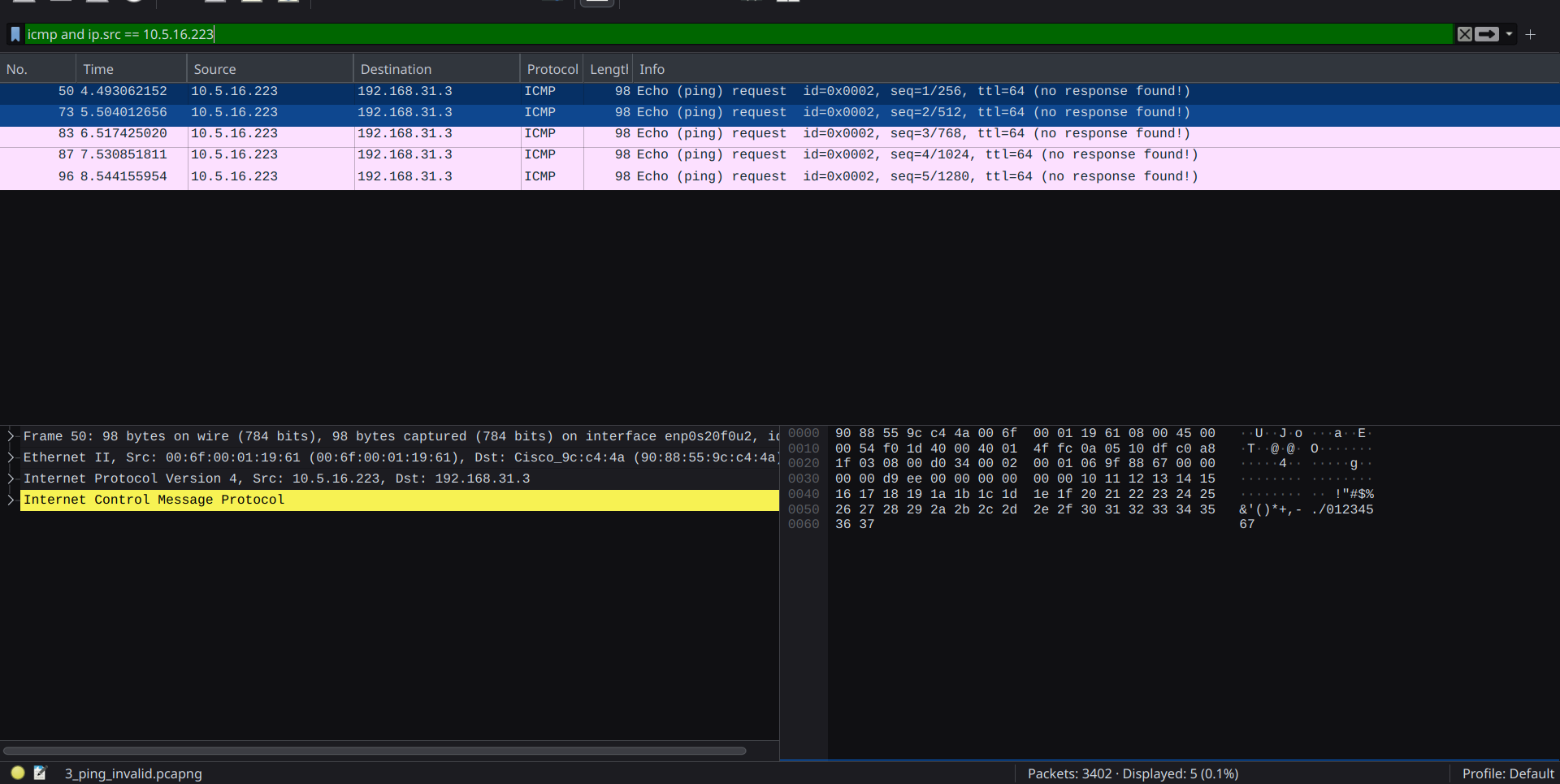


1. Above is a result of running ping command to generate ICMP traffic for my friends machine(10.5.16.135) and capturing it in Wireshark.



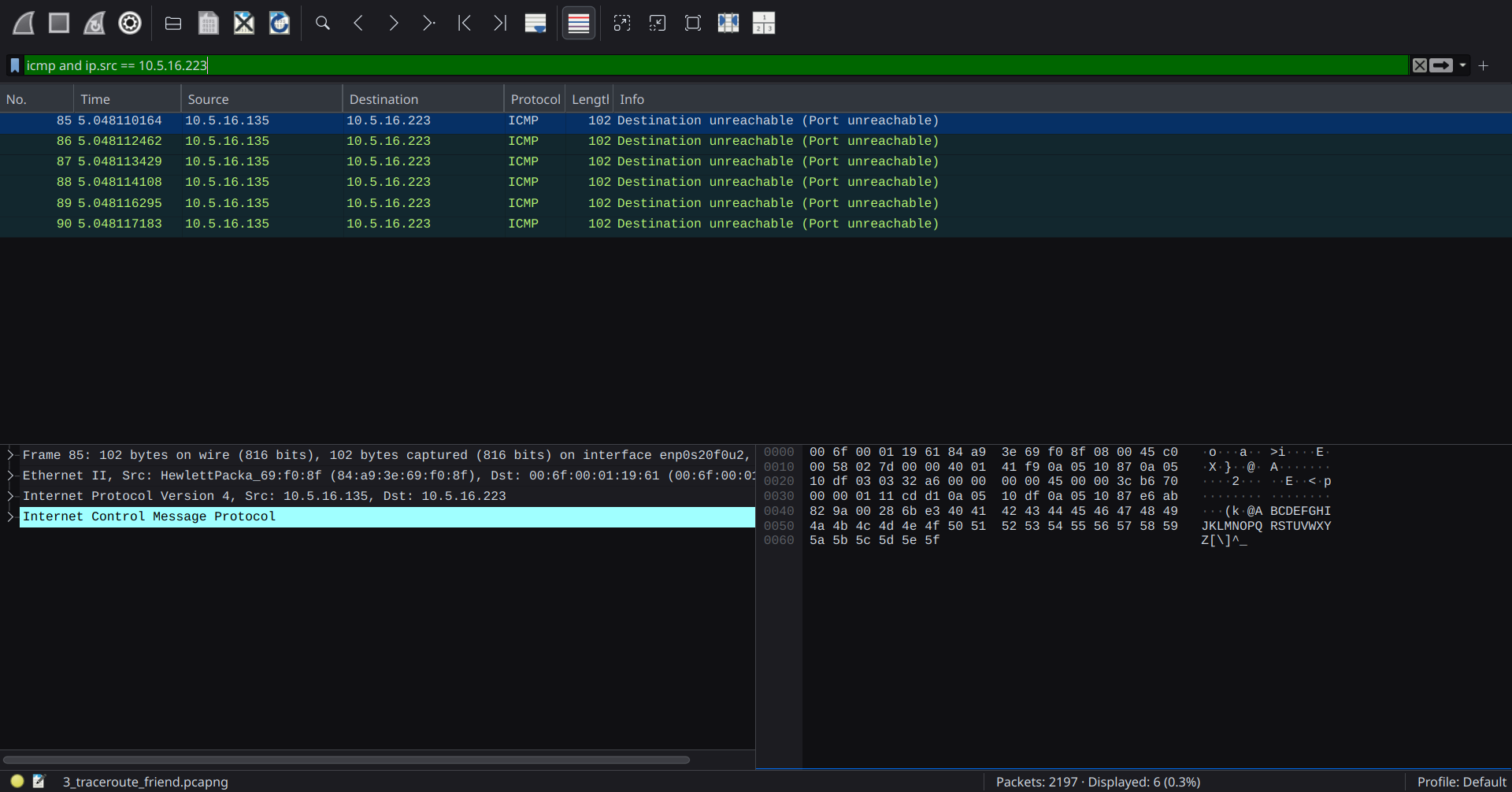
Above is a result of running traceroute command to generate ICMP traffic for my friends machine(10.5.16.135) and capturing it in Wireshark.I don’t kow the correct reason behind the “port unreachable” messages, but it seems to me that the Institute network uses NAT, which translates the internal IP addresses into a single external IP address.This is probably interfering with the normal operation of traceroute and leading to these messages.

b)

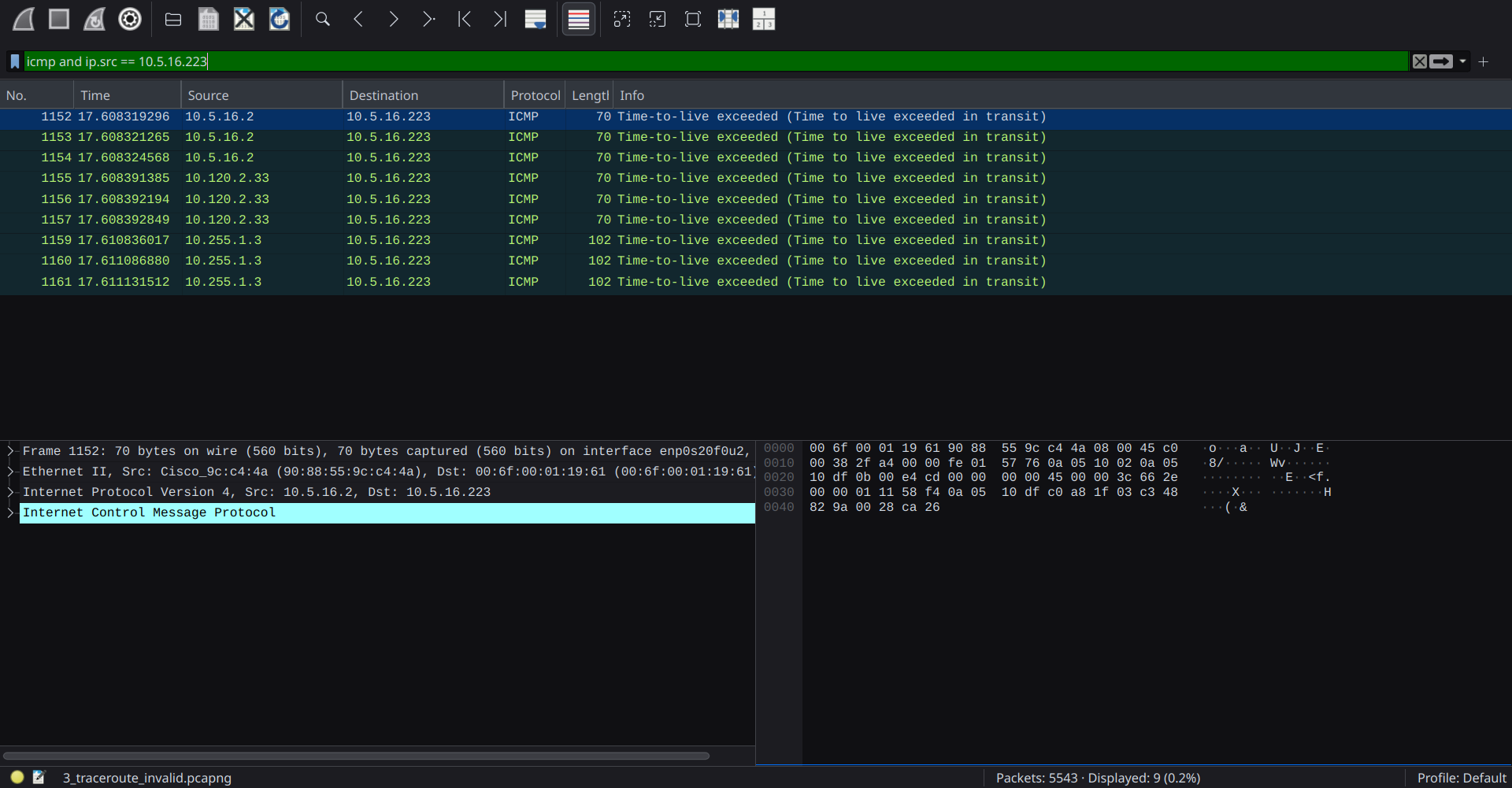


Above is the result of sending a ping to 192.168.31.3 and capturing the network traffic in Wireshark.When a ping (ICMP Echo Request) is sent to a host that is unreachable , there will be no ICMP Echo Reply. Wireshark will capture the outgoing ICMP Echo Request, but there won't be a corresponding ICMP Echo Reply. That’s why we can see in the brackets - “no response found”.

c)



Above is the result of running traceroute for my friend’s machine( reachable host ).



Above is the result of running traceroute for 192.168.31.3, an unreachable host.

When we run a traceroute to an unreachable host, the packets are sent out with increasing TTL values. Each router along the way decrements the TTL until it reaches zero. If the host is unreachable, the packets never reach their destination. Instead, an intermediate router will eventually send back an ICMP "time to live exceeded in transit" message, indicating that the packet was discarded because the TTL expired. This is the reason behind the “Time to live exceeded in transit” messages.