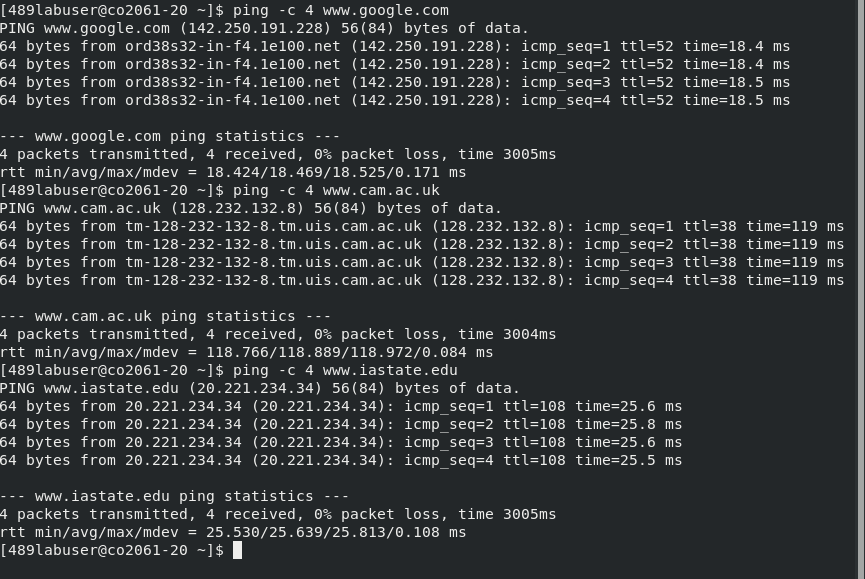
LAB 1

# Summary

This lab discusses basic and essential networking commands and their use cases in linux. For a lot of these, we require super user permissions, so we use su and change user to ‘489labuser’. Overall this lab provides a base for all the other labs.

# Switch User

# PING

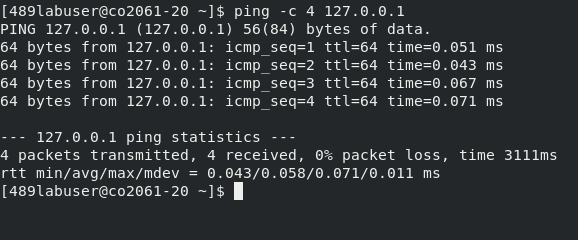
1) Average time:

Google – 18.5ms

cam.ac – 119ms

iastate - 25.6

2)

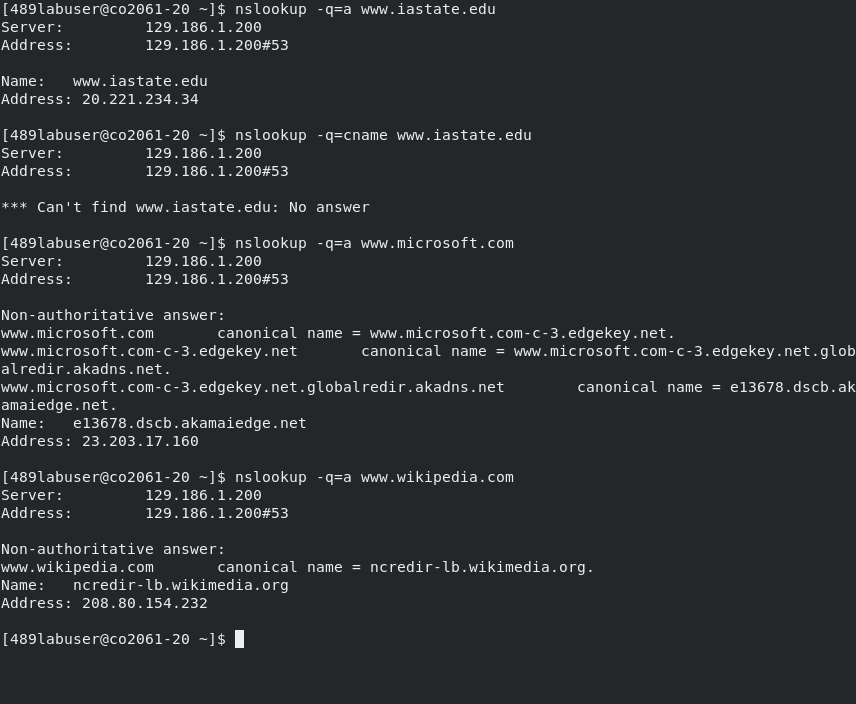


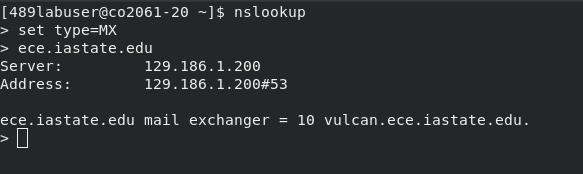
Average RTT: 0.065 ms

This is much lesser than the rest of it. The reason is pinging the localhost will return ICMP packages almost immediately since it is local to the system as compared to the other hosts which have to be accessed from a server somewhere on the internet.

# nslookup

3)



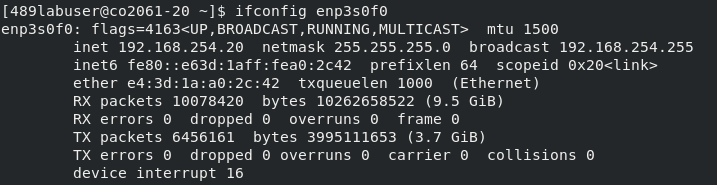
4)

5)



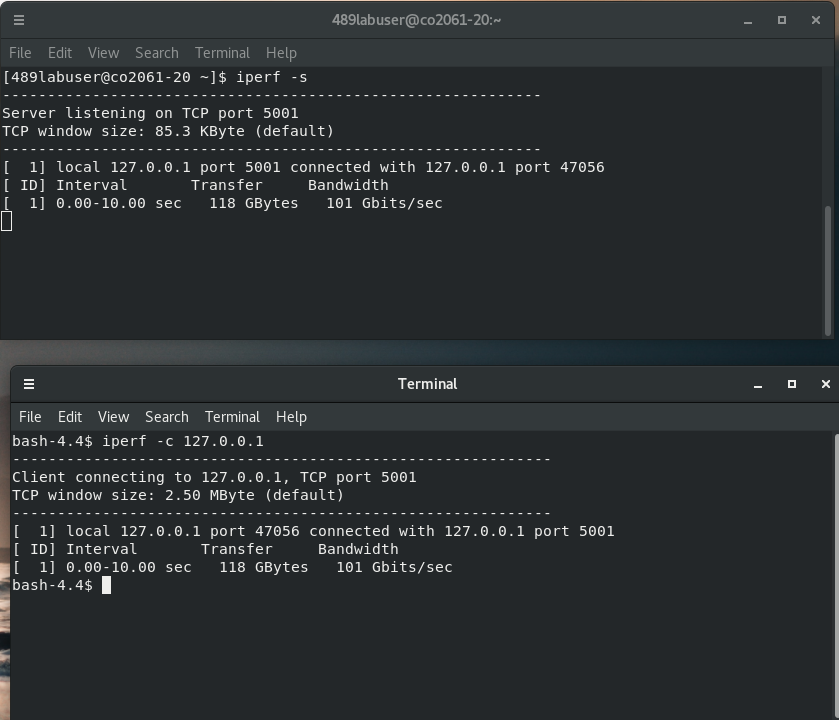
# ifconfig

6)



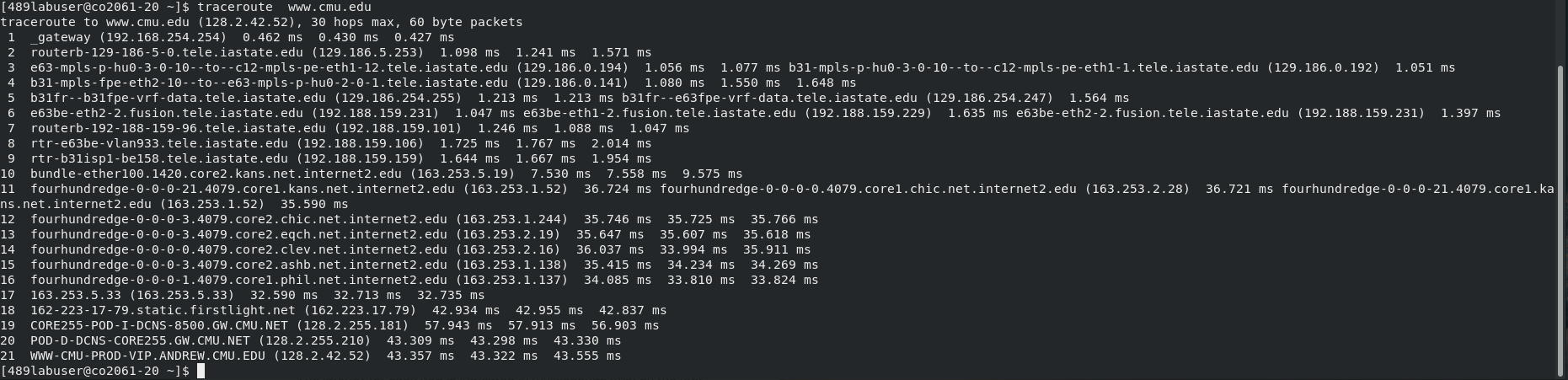
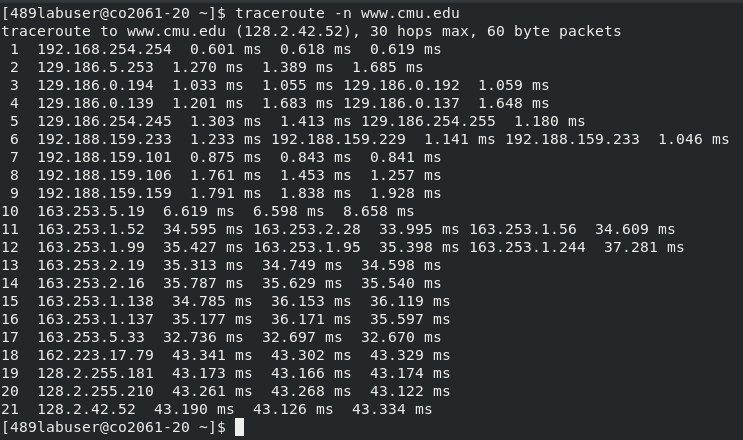
IP address: 192.168.254.20

# iperf

7)

1. Using iperf we can measure the bandwidth. Above we run iperf -s on the serve and iperf -c on the client. The bandwidth is 101 Gbps.

# traceroute

8)

Number of hops: 21

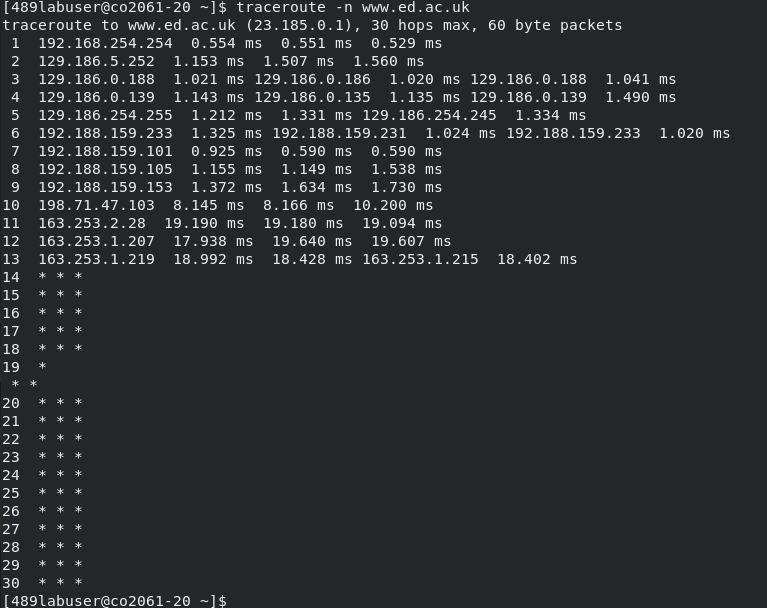
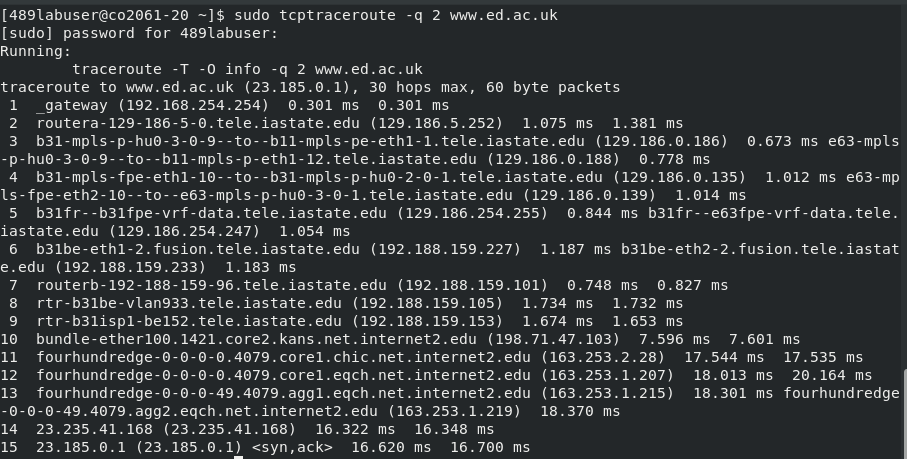
Routes/Gateway: 21 Routes. Gateways are the routers packet passes through

Latency: Latency is shown above in milliseconds, (43.190 + 43.190 + 43.126 + 43.334) ms

Reachability: Successfully reached destination 128.2.42.52

# tcptraceroute

9)



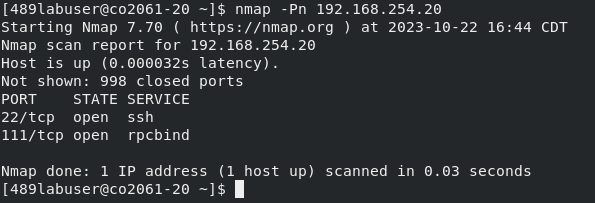
tcptraceroute uses TCP protocol rather than UDP or ICMP. Here we notice that TCP is more accessible. This is proved by having lesser number of hops compared to traceroute function.

We also notice that the latency is lesser in tcptraceroute. Both these functions call different protocols and it depends on choice of protocol to trace.

# Nmap

10)

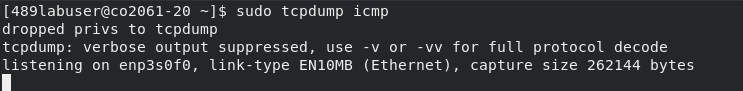
From ifconfig fucntion we found that the IP address of interface enp3s0f0 was 192.168.254.20.

This shows that ssh, port 22 is open.

# tcpdump

11)

At first, when we run tcpdump icmp (tcpdump for icmp packets coming in) we dont’ see anything.

But when we ping 192.168.254.20 (enp3s0f0) for my computer from attackers computer, we see this on my system.

A computer screen with white text

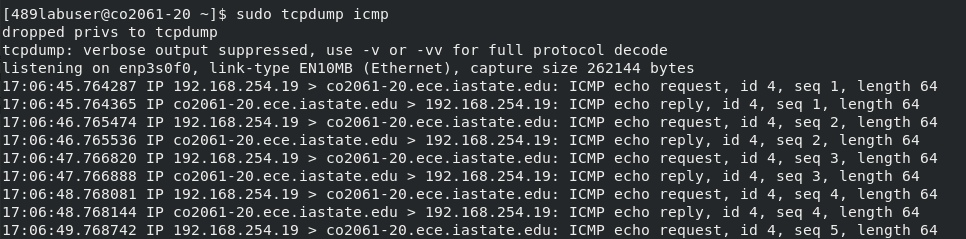
Description automatically generated

Above is the Ip for the attacker’s computer. From this computer we ping the IP of my computer. This is shown below.

A computer screen with a black and white text

Description automatically generated

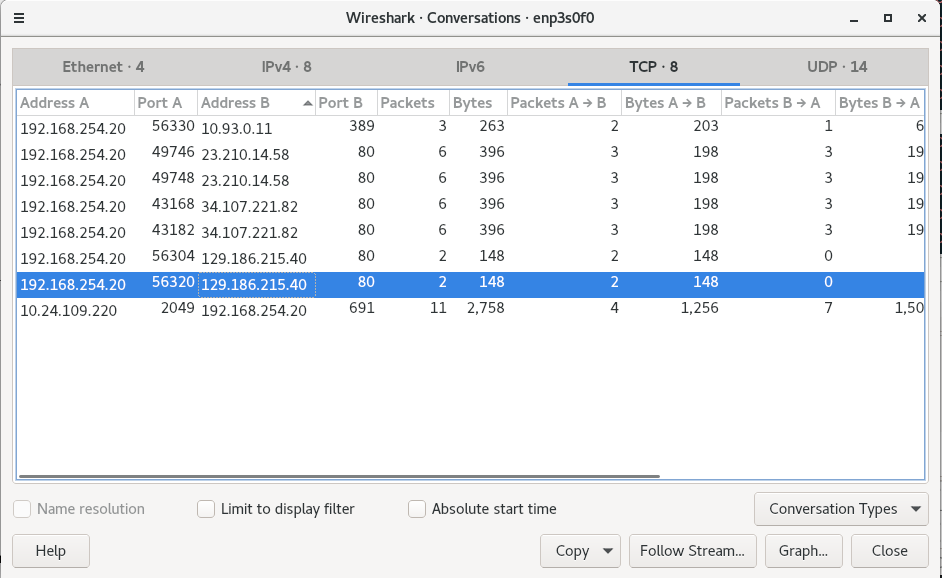
When the ping is started, we see that the ‘sudo tcpdump icmp’ command on our system starts printing data.

This shows the IP address of the device (192.168.254.19) pinging my device.

# Wireshark

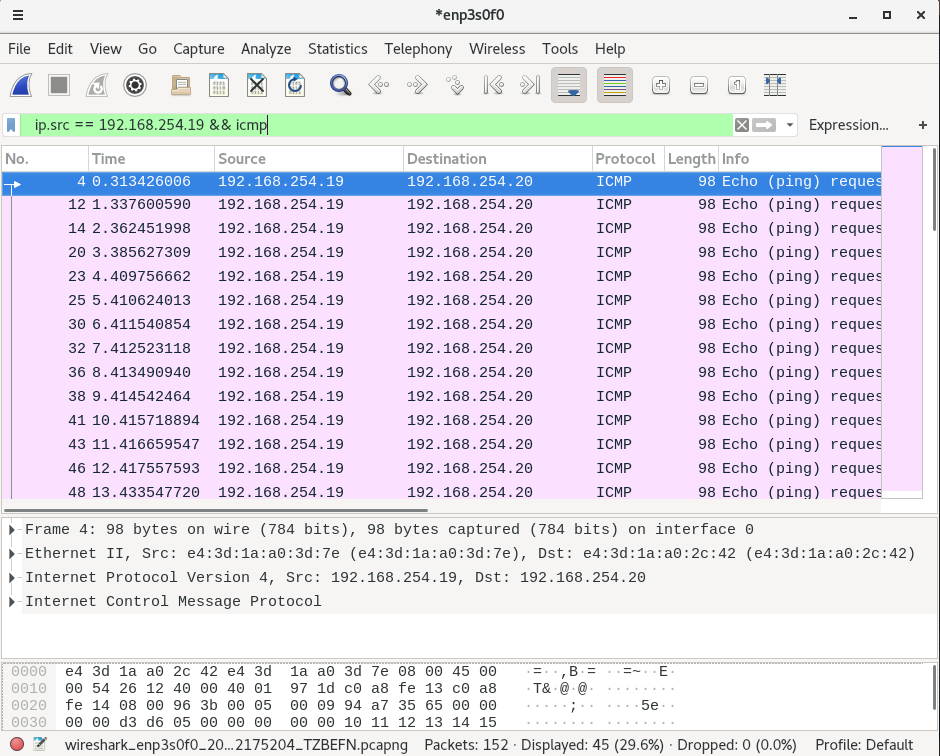
12)

We can use nslookup to find iastate.edu IP address, I used 129.168.215.40 from firefox and ran filtered tcp connections from wireshark. Below is the result I got.



13)

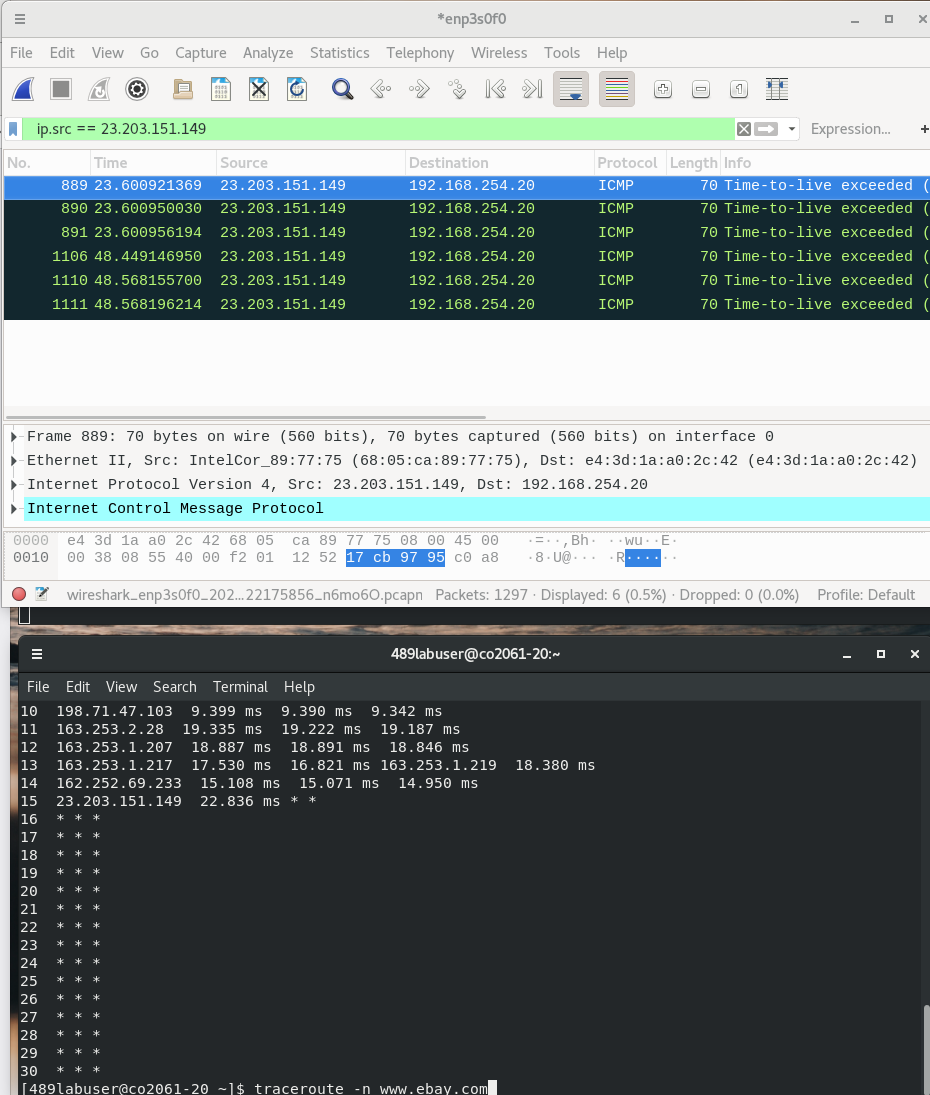
As I previosuly mentioned, running ifconfig on the other system, shows the IP to be, 192.168.254.19.

Using the custom filter we can check for the specific IP for ICMP protocol. This show that 784 bites were transmitted. Arrival time is displayed above

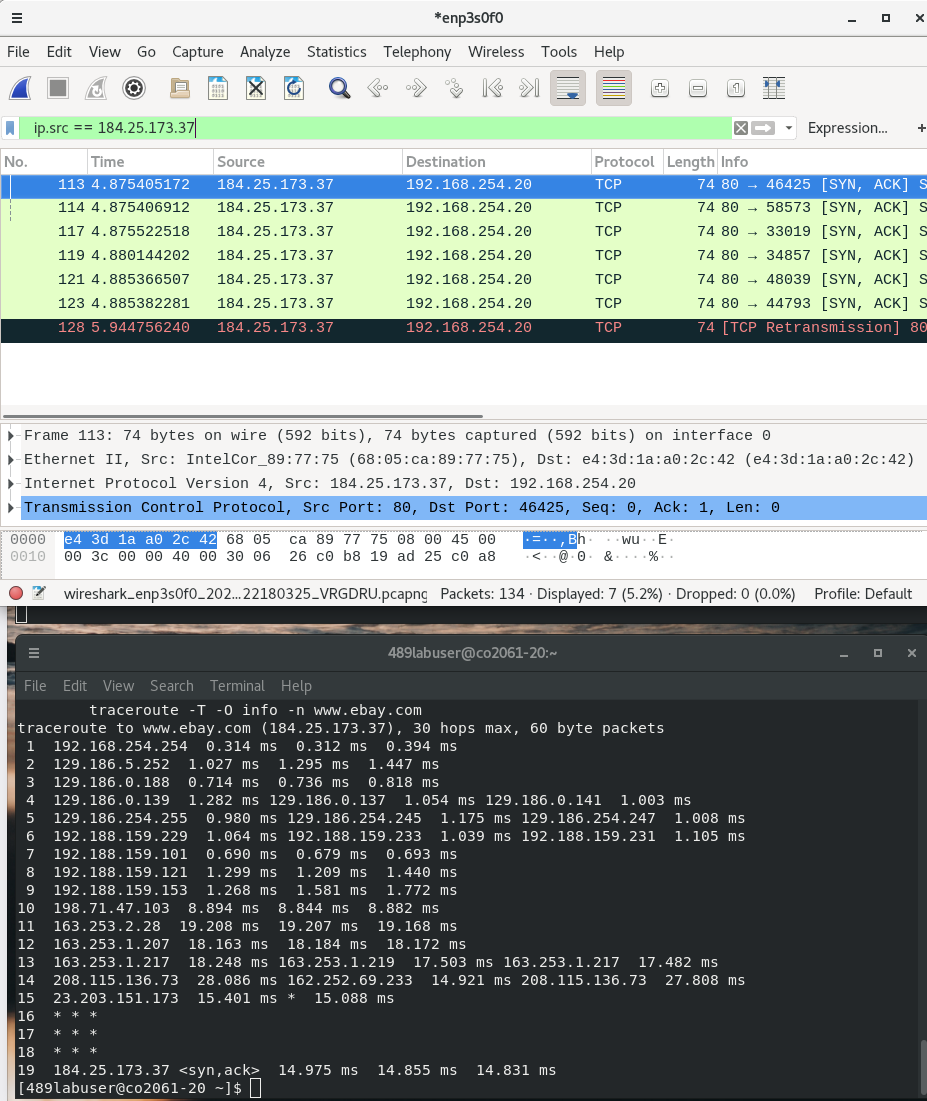
14)

traceroute:

Traceroute usually Pings the system, which usually uses the ICMP protocol.



tcptraceroute: TCP

Since tcptraceroute traces the tcp pipleine, after adding the filer of the destination IP of ebay, we find the type of packets by tcptraceroute is TCP