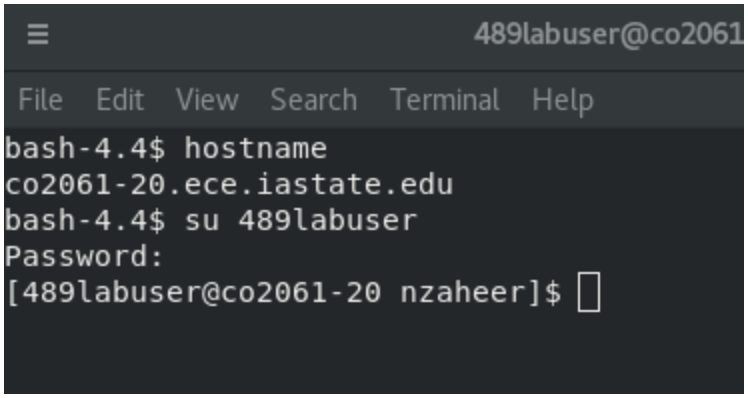
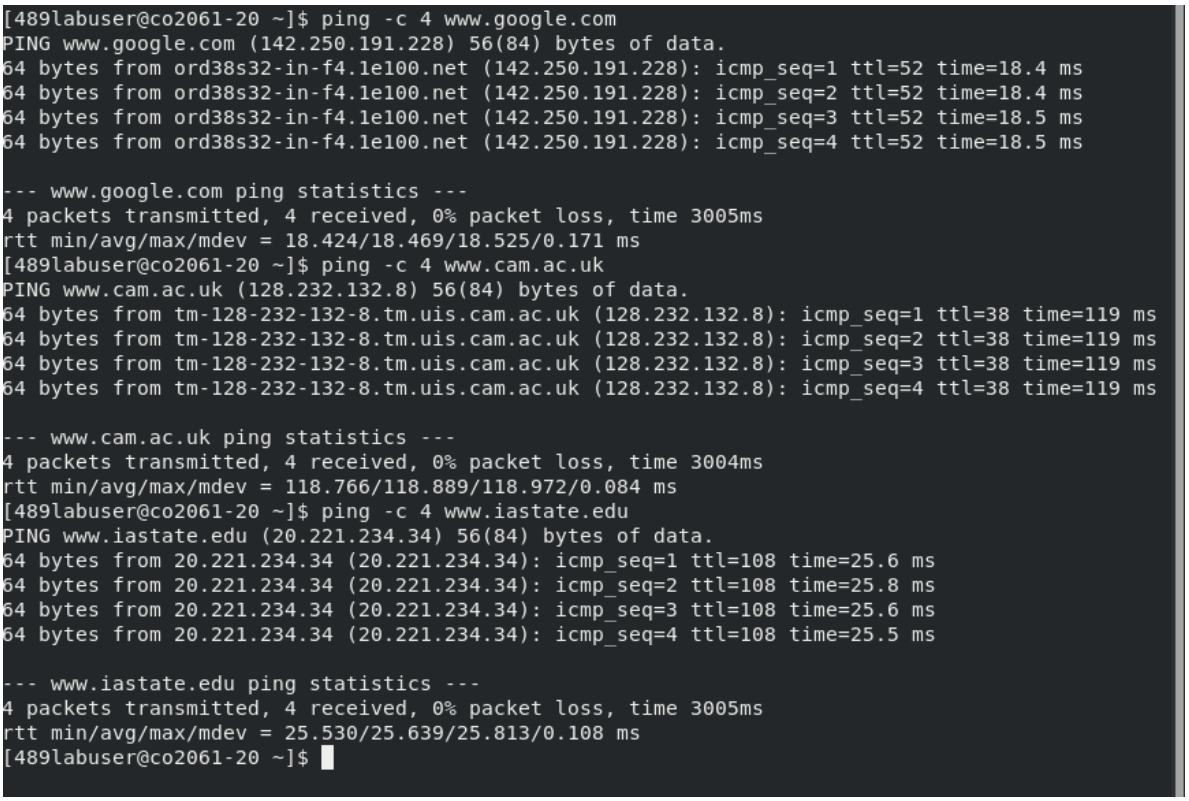
LAB 1

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)

```
[489labuser@co2061-20 ~]$ ping -c 4 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.051 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.043 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.067 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.071 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3111ms
rtt min/avg/max/mdev = 0.043/0.058/0.071/0.011 ms
[489labuser@co2061-20 ~]$
```

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)

```
[489labuser@co2061-20 ~]$ nslookup -q=a www.iastate.edu
Server:         129.186.1.200
Address:        129.186.1.200#53

Name:   www.iastate.edu
Address: 20.221.234.34

[489labuser@co2061-20 ~]$ nslookup -q=cname www.iastate.edu
Server:         129.186.1.200
Address:        129.186.1.200#53

*** Can't find www.iastate.edu: No answer

[489labuser@co2061-20 ~]$ nslookup -q=a www.microsoft.com
Server:         129.186.1.200
Address:        129.186.1.200#53

Non-authoritative answer:
www.microsoft.com       canonical name = www.microsoft.com-c-3.edgekey.net.
www.microsoft.com-c-3.edgekey.net       canonical name = www.microsoft.com-c-3.edgekey.net.glob
alredir.akadns.net.
www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net        canonical name = e13678.dscb.ak
amaiedge.net.
Name:   e13678.dscb.akamaiedge.net
Address: 23.203.17.160

[489labuser@co2061-20 ~]$ nslookup -q=a www.wikipedia.com
Server:         129.186.1.200
Address:        129.186.1.200#53

Non-authoritative answer:
www.wikipedia.com       canonical name = ncredir-lb.wikimedia.org.
Name:   ncredir-lb.wikimedia.org
Address: 208.80.154.232

[489labuser@co2061-20 ~]$
```

4)

```
[489labuser@co2061-20 ~]$ nslookup
> set type=MX
> ece.iastate.edu
Server:         129.186.1.200
Address:        129.186.1.200#53

ece.iastate.edu mail exchanger = 10 vulcan.ece.iastate.edu.
>
```

5)

```
[489labuser@co2061-20 ~]$ nslookup
> 129.186.215.40
40.215.186.129.in-addr.arpa     name = spock.ee.iastate.edu.
```

ifconfig

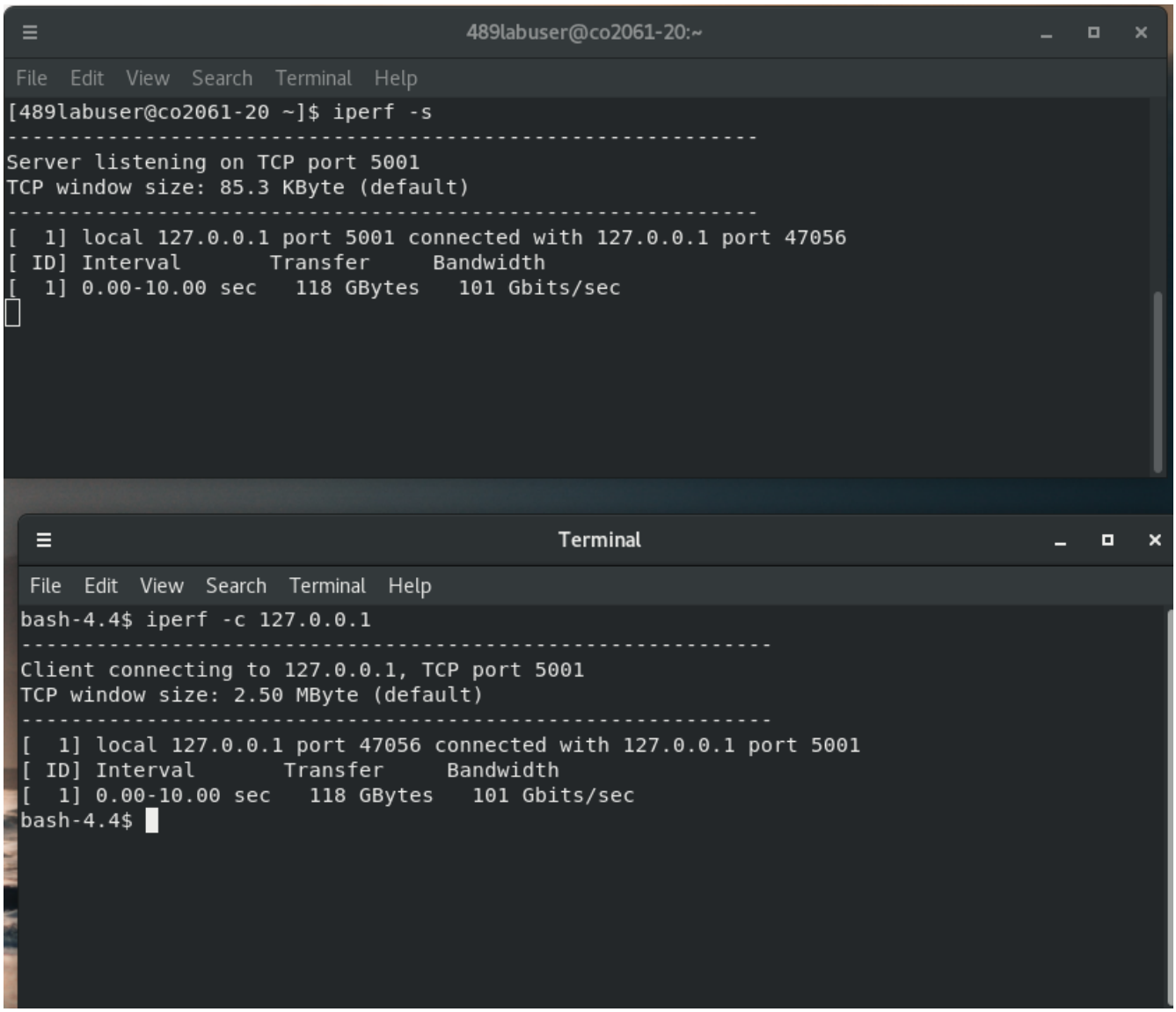
6)

```
[489labuser@co2061-20 ~]$ ifconfig enp3s0f0
enp3s0f0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.254.20  netmask 255.255.255.0  broadcast 192.168.254.255
        inet6 fe80::e63d:1aff:fea0:2c42  prefixlen 64  scopeid 0x20<link>
        ether e4:3d:1a:a0:2c:42  txqueuelen 1000  (Ethernet)
        RX packets 10078420  bytes 10262658522 (9.5 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6456161  bytes 3995111653 (3.7 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16
```

IP address: 192.168.254.20

iperf

7)



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

```
[489labuser@co2061-20 ~]$ traceroute -n www.cmu.edu
traceroute to www.cmu.edu (128.2.42.52), 30 hops max, 60 byte packets
 1  192.168.254.254  0.601 ms  0.618 ms  0.619 ms
 2  129.186.5.253  1.270 ms  1.389 ms  1.685 ms
 3  129.186.0.194  1.033 ms  1.055 ms 129.186.0.192  1.059 ms
 4  129.186.0.139  1.201 ms  1.683 ms 129.186.0.137  1.648 ms
 5  129.186.254.245  1.303 ms  1.413 ms 129.186.254.255  1.180 ms
 6  192.188.159.233  1.233 ms 192.188.159.229  1.141 ms 192.188.159.233  1.046 ms
 7  192.188.159.101  0.875 ms  0.843 ms  0.841 ms
 8  192.188.159.106  1.761 ms  1.453 ms  1.257 ms
 9  192.188.159.159  1.791 ms  1.838 ms  1.928 ms
10  163.253.5.19  6.619 ms  6.598 ms  8.658 ms
11  163.253.1.52  34.595 ms 163.253.2.28  33.995 ms 163.253.1.56  34.609 ms
12  163.253.1.99  35.427 ms 163.253.1.95  35.398 ms 163.253.1.244  37.281 ms
13  163.253.2.19  35.313 ms  34.749 ms  34.598 ms
14  163.253.2.16  35.787 ms  35.629 ms  35.540 ms
15  163.253.1.138  34.785 ms  36.153 ms  36.119 ms
16  163.253.1.137  35.177 ms  36.171 ms  35.597 ms
17  163.253.5.33  32.736 ms  32.697 ms  32.670 ms
18  162.223.17.79  43.341 ms  43.302 ms  43.329 ms
19  128.2.255.181  43.173 ms  43.166 ms  43.174 ms
20  128.2.255.210  43.261 ms  43.268 ms  43.122 ms
21  128.2.42.52  43.190 ms  43.126 ms  43.334 ms
[489labuser@co2061-20 ~]$
```

```
[489labuser@co2061-20 ~]$ traceroute  www.cmu.edu
traceroute to www.cmu.edu (128.2.42.52), 30 hops max, 60 byte packets
 1  _gateway (192.168.254.254)  0.462 ms  0.430 ms  0.427 ms
 2  routerb-129-186-5-0.tele.iastate.edu (129.186.5.253)  1.098 ms  1.241 ms  1.571 ms
 3  e63-mpls-p-hu0-3-0-10--to--c12-mpls-pe-eth1-12.tele.iastate.edu (129.186.0.194)  1.056 ms  1.077 ms b31-mpls-p-hu0-3-0-10--to--c12-mpls-pe-eth1-1.tele.iastate.edu (129.186.0.192)  1.051 ms
 4  b31-mpls-fpe-eth2-10--to--e63-mpls-p-hu0-2-0-1.tele.iastate.edu (129.186.0.141)  1.080 ms  1.550 ms  1.648 ms
 5  b31fr--b31fpe-vrf-data.tele.iastate.edu (129.186.254.255)  1.213 ms  1.213 ms b31fr--e63fpe-vrf-data.tele.iastate.edu (129.186.254.247)  1.564 ms
 6  e63be-eth2-2.fusion.tele.iastate.edu (192.188.159.231)  1.047 ms e63be-eth1-2.fusion.tele.iastate.edu (192.188.159.229)  1.635 ms e63be-eth2-2.fusion.tele.iastate.edu (192.188.159.231)  1.397 ms
 7  routerb-192-188-159-96.tele.iastate.edu (192.188.159.101)  1.246 ms  1.088 ms  1.047 ms
 8  rtr-e63be-vlan933.tele.iastate.edu (192.188.159.106)  1.725 ms  1.767 ms  2.014 ms
 9  rtr-b31isp1-be158.tele.iastate.edu (192.188.159.159)  1.644 ms  1.667 ms  1.954 ms
10  bundle-ether100.1420.core2.kans.net.internet2.edu (163.253.5.19)  7.530 ms  7.558 ms  9.575 ms
11  fourhundredge-0-0-0-21.4079.core1.kans.net.internet2.edu (163.253.1.52)  36.724 ms fourhundredge-0-0-0-0.4079.core1.chic.net.internet2.edu (163.253.2.28)  36.721 ms fourhundredge-0-0-0-21.4079.core1.ka
ns.net.internet2.edu (163.253.1.52)  35.590 ms
12  fourhundredge-0-0-0-3.4079.core2.chic.net.internet2.edu (163.253.1.244)  35.746 ms  35.725 ms  35.766 ms
13  fourhundredge-0-0-0-3.4079.core2.eqch.net.internet2.edu (163.253.2.19)  35.647 ms  35.607 ms  35.618 ms
14  fourhundredge-0-0-0-0.4079.core2.clev.net.internet2.edu (163.253.2.16)  36.037 ms  33.994 ms  35.911 ms
15  fourhundredge-0-0-0-3.4079.core2.ashb.net.internet2.edu (163.253.1.138)  35.415 ms  34.234 ms  34.269 ms
16  fourhundredge-0-0-0-1.4079.core1.phil.net.internet2.edu (163.253.1.137)  34.085 ms  33.810 ms  33.824 ms
17  163.253.5.33 (163.253.5.33)  32.590 ms  32.713 ms  32.735 ms
18  162-223-17-79.static.firstlight.net (162.223.17.79)  42.934 ms  42.955 ms  42.837 ms
19  CORE255-POD-I-DCNS-8500.GW.CMU.NET (128.2.255.181)  57.943 ms  57.913 ms  56.903 ms
20  POD-D-DCNS-CORE255.GW.CMU.NET (128.2.255.210)  43.309 ms  43.298 ms  43.330 ms
21  WWW-CMU-PROD-VIP.ANDREW.CMU.EDU (128.2.42.52)  43.357 ms  43.322 ms  43.555 ms
[489labuser@co2061-20 ~]$
```

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)

```
[489labuser@co2061-20 ~]$ sudo tcptraceroute -q 2 www.ed.ac.uk
[sudo] password for 489labuser:
Running:
        traceroute -T -O info -q 2 www.ed.ac.uk
traceroute to www.ed.ac.uk (23.185.0.1), 30 hops max, 60 byte packets
 1  _gateway (192.168.254.254)  0.301 ms  0.301 ms
 2  routera-129-186-5-0.tele.iastate.edu (129.186.5.252)  1.075 ms  1.381 ms
 3  b31-mpls-p-hu0-3-0-9--to--b11-mpls-pe-eth1-1.tele.iastate.edu (129.186.0.186)  0.673 ms e63-mpls
-p-hu0-3-0-9--to--b11-mpls-p-eth1-12.tele.iastate.edu (129.186.0.188)  0.778 ms
 4  b31-mpls-fpe-eth1-10--to--b31-mpls-p-hu0-2-0-1.tele.iastate.edu (129.186.0.135)  1.012 ms e63-mp
ls-fpe-eth2-10--to--e63-mpls-p-hu0-3-0-1.tele.iastate.edu (129.186.0.139)  1.014 ms
 5  b31fr--b31fpe-vrf-data.tele.iastate.edu (129.186.254.255)  0.844 ms b31fr--e63fpe-vrf-data.tele.
iastate.edu (129.186.254.247)  1.054 ms
 6  b31be-eth1-2.fusion.tele.iastate.edu (192.188.159.227)  1.187 ms b31be-eth2-2.fusion.tele.iastat
e.edu (192.188.159.233)  1.183 ms
 7  routerb-192-188-159-96.tele.iastate.edu (192.188.159.101)  0.748 ms  0.827 ms
 8  rtr-b31be-vlan933.tele.iastate.edu (192.188.159.105)  1.734 ms  1.732 ms
 9  rtr-b31isp1-be152.tele.iastate.edu (192.188.159.153)  1.674 ms  1.653 ms
10  bundle-ether100.1421.core2.kans.net.internet2.edu (198.71.47.103)  7.596 ms  7.601 ms
11  fourhundredge-0-0-0-0.4079.core1.chic.net.internet2.edu (163.253.2.28)  17.544 ms  17.535 ms
12  fourhundredge-0-0-0-0.4079.core1.eqch.net.internet2.edu (163.253.1.207)  18.013 ms  20.164 ms
13  fourhundredge-0-0-0-49.4079.agg1.eqch.net.internet2.edu (163.253.1.215)  18.301 ms fourhundredge
-0-0-0-49.4079.agg2.eqch.net.internet2.edu (163.253.1.219)  18.370 ms
14  23.235.41.168 (23.235.41.168)  16.322 ms  16.348 ms
15  23.185.0.1 (23.185.0.1) <syn,ack>  16.620 ms  16.700 ms
```

```
[489labuser@co2061-20 ~]$ traceroute -n www.ed.ac.uk
traceroute to www.ed.ac.uk (23.185.0.1), 30 hops max, 60 byte packets
 1  192.168.254.254  0.554 ms  0.551 ms  0.529 ms
 2  129.186.5.252  1.153 ms  1.507 ms  1.560 ms
 3  129.186.0.188  1.021 ms 129.186.0.186  1.020 ms 129.186.0.188  1.041 ms
 4  129.186.0.139  1.143 ms 129.186.0.135  1.135 ms 129.186.0.139  1.490 ms
 5  129.186.254.255  1.212 ms  1.331 ms 129.186.254.245  1.334 ms
 6  192.188.159.233  1.325 ms 192.188.159.231  1.024 ms 192.188.159.233  1.020 ms
 7  192.188.159.101  0.925 ms  0.590 ms  0.590 ms
 8  192.188.159.105  1.155 ms  1.149 ms  1.538 ms
 9  192.188.159.153  1.372 ms  1.634 ms  1.730 ms
10  198.71.47.103  8.145 ms  8.166 ms  10.200 ms
11  163.253.2.28  19.190 ms  19.180 ms  19.094 ms
12  163.253.1.207  17.938 ms  19.640 ms  19.607 ms
13  163.253.1.219  18.992 ms  18.428 ms 163.253.1.215  18.402 ms
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  *
 * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
[489labuser@co2061-20 ~]$
```

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.

```
[489labuser@co2061-20 ~]$ nmap -Pn 192.168.254.20
Starting Nmap 7.70 ( https://nmap.org ) at 2023-10-22 16:44 CDT
Nmap scan report for 192.168.254.20
Host is up (0.000032s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
[489labuser@co2061-20 ~]$
```

This shows that ssh, port 22 is open.

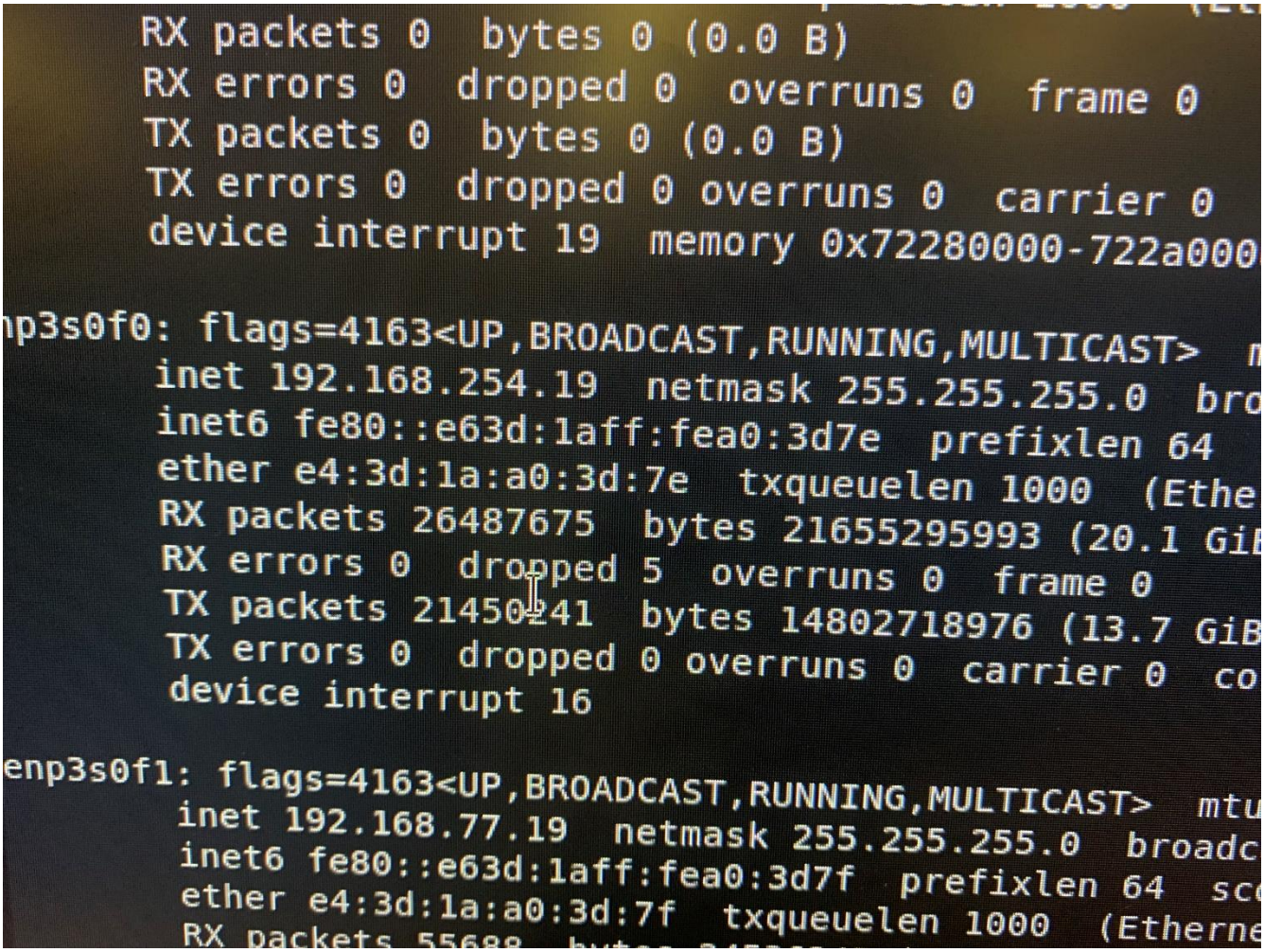
tcpdump

11)

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

```
[489labuser@co2061-20 ~]$ sudo tcpdump icmp
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0f0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

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

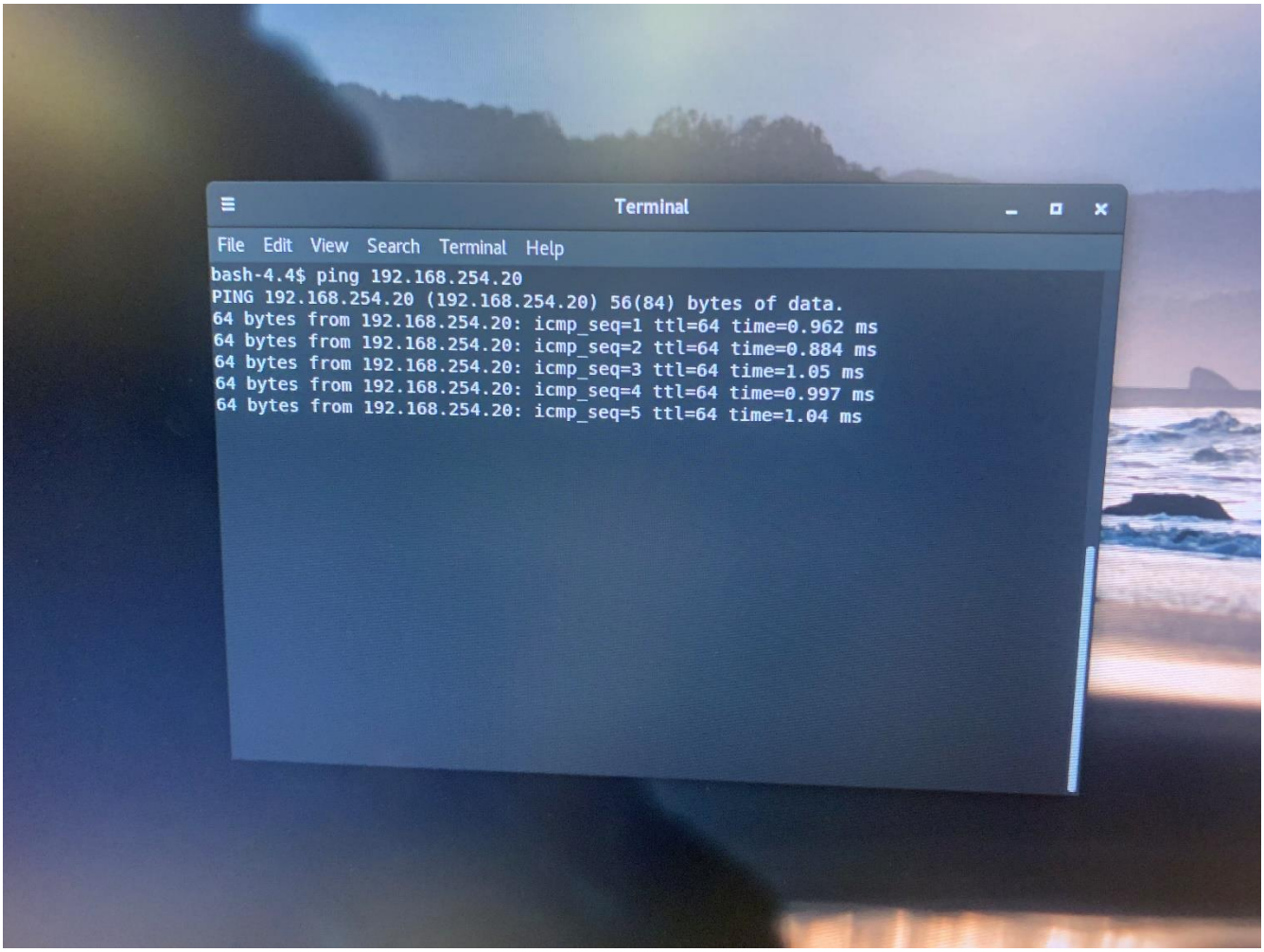


```
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0
        device interrupt 19  memory 0x72280000-722a000

np3s0f0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  m
        inet 192.168.254.19  netmask 255.255.255.0  bro
        inet6 fe80::e63d:1aff:fea0:3d7e  prefixlen 64
        ether e4:3d:1a:a0:3d:7e  txqueuelen 1000  (Ethe
        RX packets 26487675  bytes 21655295993 (20.1 GiB
        RX errors 0  dropped 5  overruns 0  frame 0
        TX packets 21450241  bytes 14802718976 (13.7 GiB
        TX errors 0  dropped 0 overruns 0  carrier 0  co
        device interrupt 16

enp3s0f1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu
        inet 192.168.77.19  netmask 255.255.255.0  broadc
        inet6 fe80::e63d:1aff:fea0:3d7f  prefixlen 64  sc
        ether e4:3d:1a:a0:3d:7f  txqueuelen 1000  (Etherne
        RX packets 55688
```

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



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

```
[489labuser@co2061-20 ~]$ sudo tcpdump icmp
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0f0, link-type EN10MB (Ethernet), capture size 262144 bytes
17:06:45.764287 IP 192.168.254.19 > co2061-20.ece.iastate.edu: ICMP echo request, id 4, seq 1, length 64
17:06:45.764365 IP co2061-20.ece.iastate.edu > 192.168.254.19: ICMP echo reply, id 4, seq 1, length 64
17:06:46.765474 IP 192.168.254.19 > co2061-20.ece.iastate.edu: ICMP echo request, id 4, seq 2, length 64
17:06:46.765536 IP co2061-20.ece.iastate.edu > 192.168.254.19: ICMP echo reply, id 4, seq 2, length 64
17:06:47.766820 IP 192.168.254.19 > co2061-20.ece.iastate.edu: ICMP echo request, id 4, seq 3, length 64
17:06:47.766888 IP co2061-20.ece.iastate.edu > 192.168.254.19: ICMP echo reply, id 4, seq 3, length 64
17:06:48.768081 IP 192.168.254.19 > co2061-20.ece.iastate.edu: ICMP echo request, id 4, seq 4, length 64
17:06:48.768144 IP co2061-20.ece.iastate.edu > 192.168.254.19: ICMP echo reply, id 4, seq 4, length 64
17:06:49.768742 IP 192.168.254.19 > co2061-20.ece.iastate.edu: ICMP echo request, id 4, seq 5, length 64
```

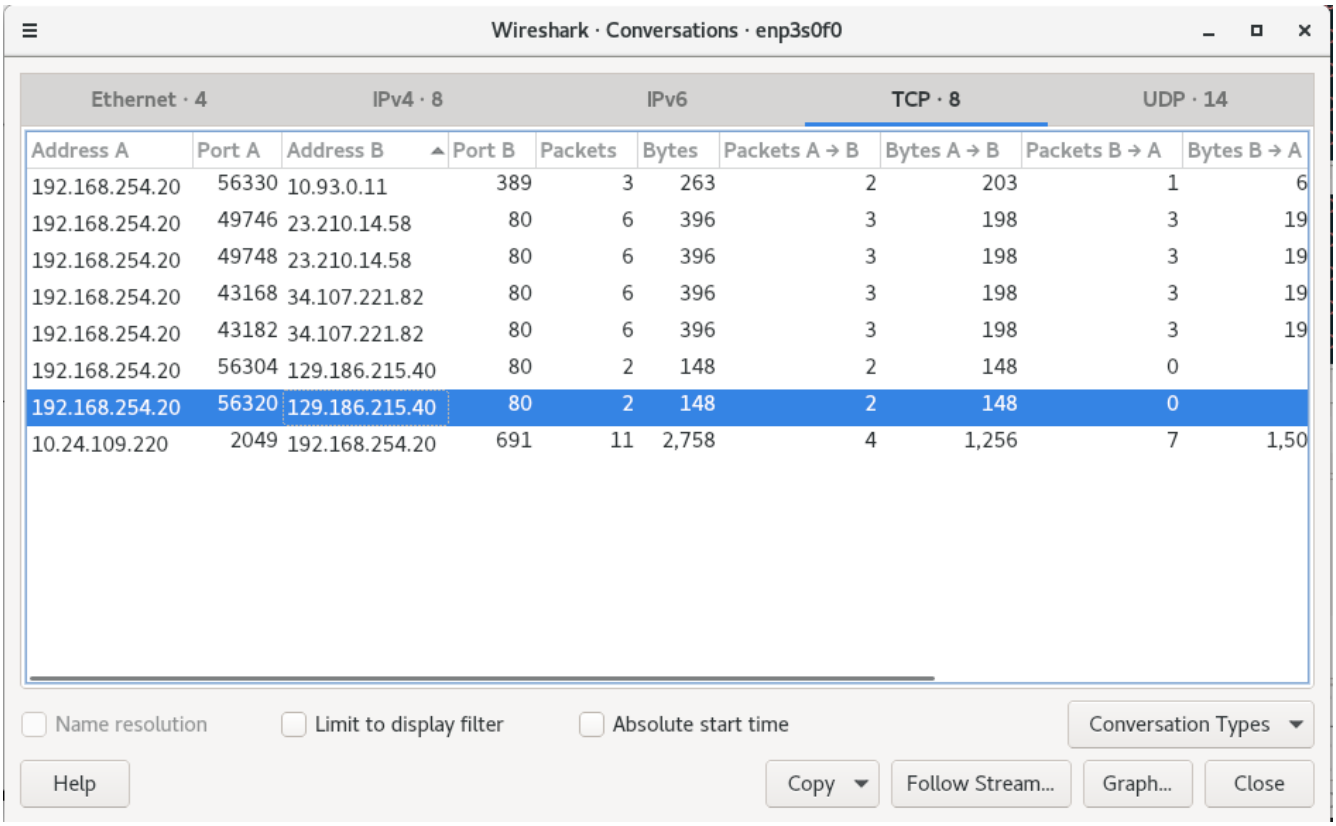
This shows the IP address of the device (192.168.254.19) pinging my device.

Wireshark

12)

```
30  20.221.234.34 (20.221.234.34) <syn,ack>  26.538 ms  29.630 ms
[489labuser@co2061-20 nzaheer]$ sudo tcptraceroute -q 2 www.iastate.edu
```

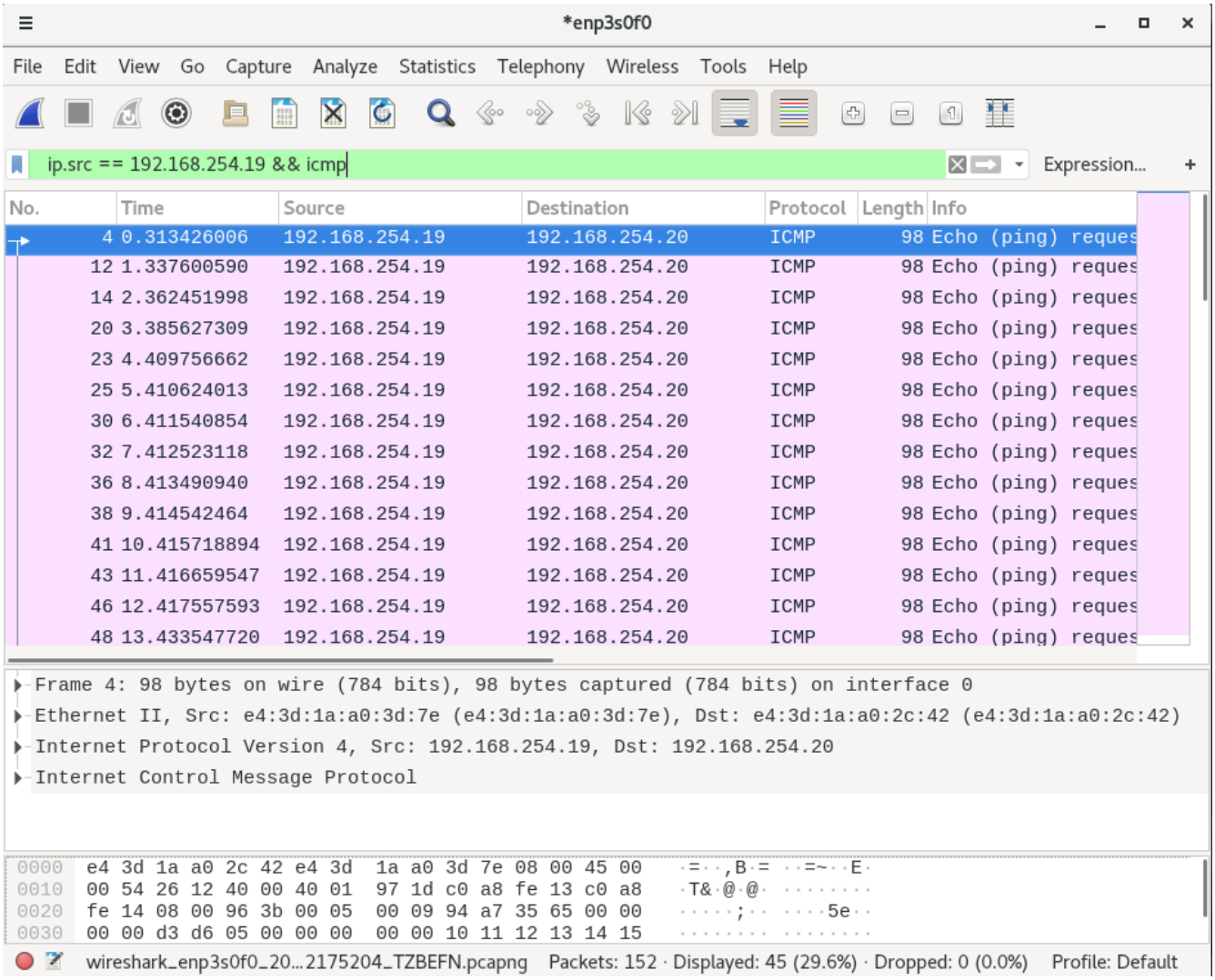
We can use nslookup to find iastate.edu IP address, I used 129.168.215.40 from firefox and ran filtered tcp connections from wireshark. Below is the result I got.



Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
192.168.254.20	56330	10.93.0.11	389	3	263	2	203	1	6
192.168.254.20	49746	23.210.14.58	80	6	396	3	198	3	19
192.168.254.20	49748	23.210.14.58	80	6	396	3	198	3	19
192.168.254.20	43168	34.107.221.82	80	6	396	3	198	3	19
192.168.254.20	43182	34.107.221.82	80	6	396	3	198	3	19
192.168.254.20	56304	129.186.215.40	80	2	148	2	148	0	
192.168.254.20	56320	129.186.215.40	80	2	148	2	148	0	
10.24.109.220	2049	192.168.254.20	691	11	2,758	4	1,256	7	1,50

13)

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

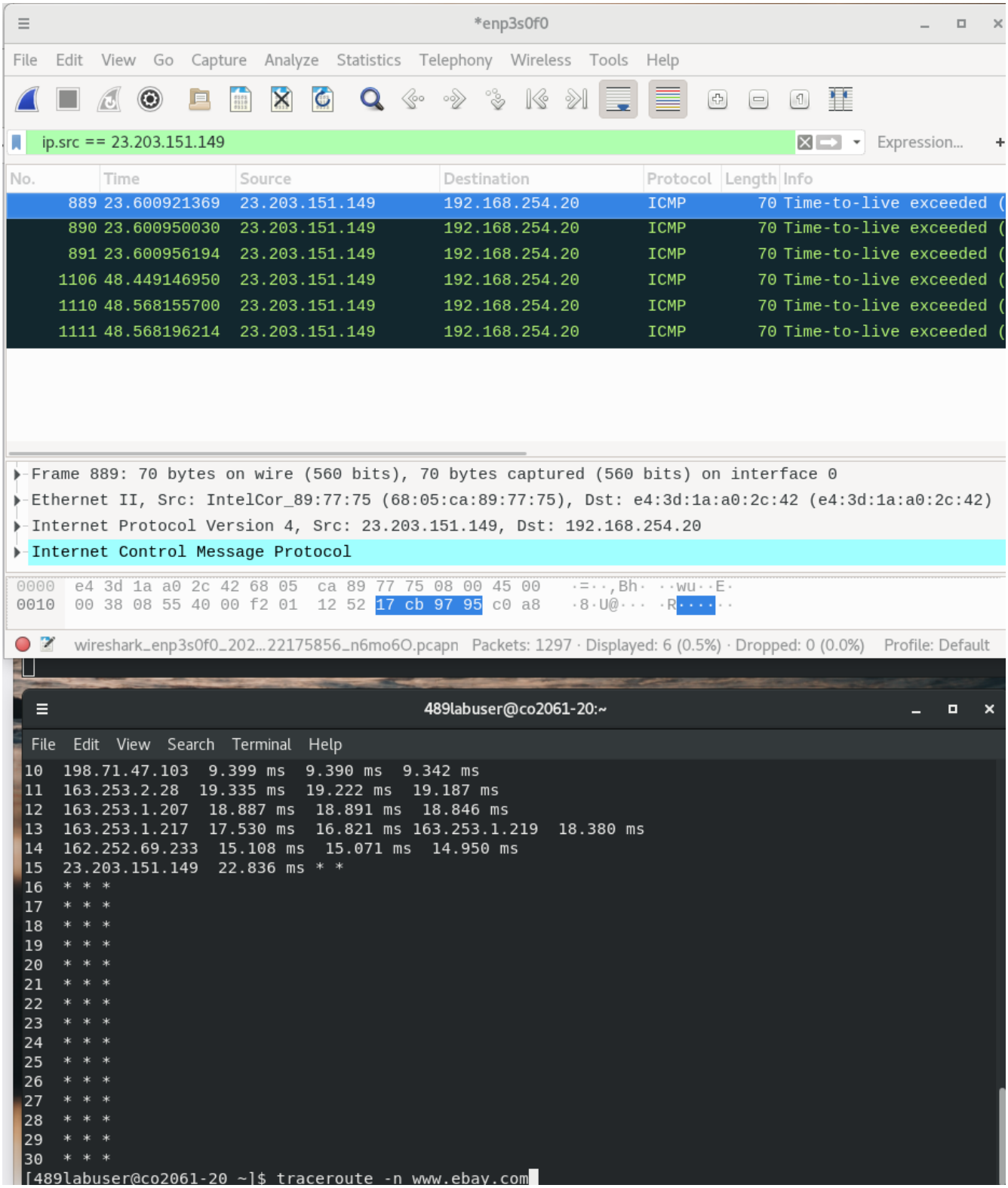


Using the custom filter we can check for the specific IP for ICMP protocol. This show that 784 bites were transmitted. Arrival time is displayed above

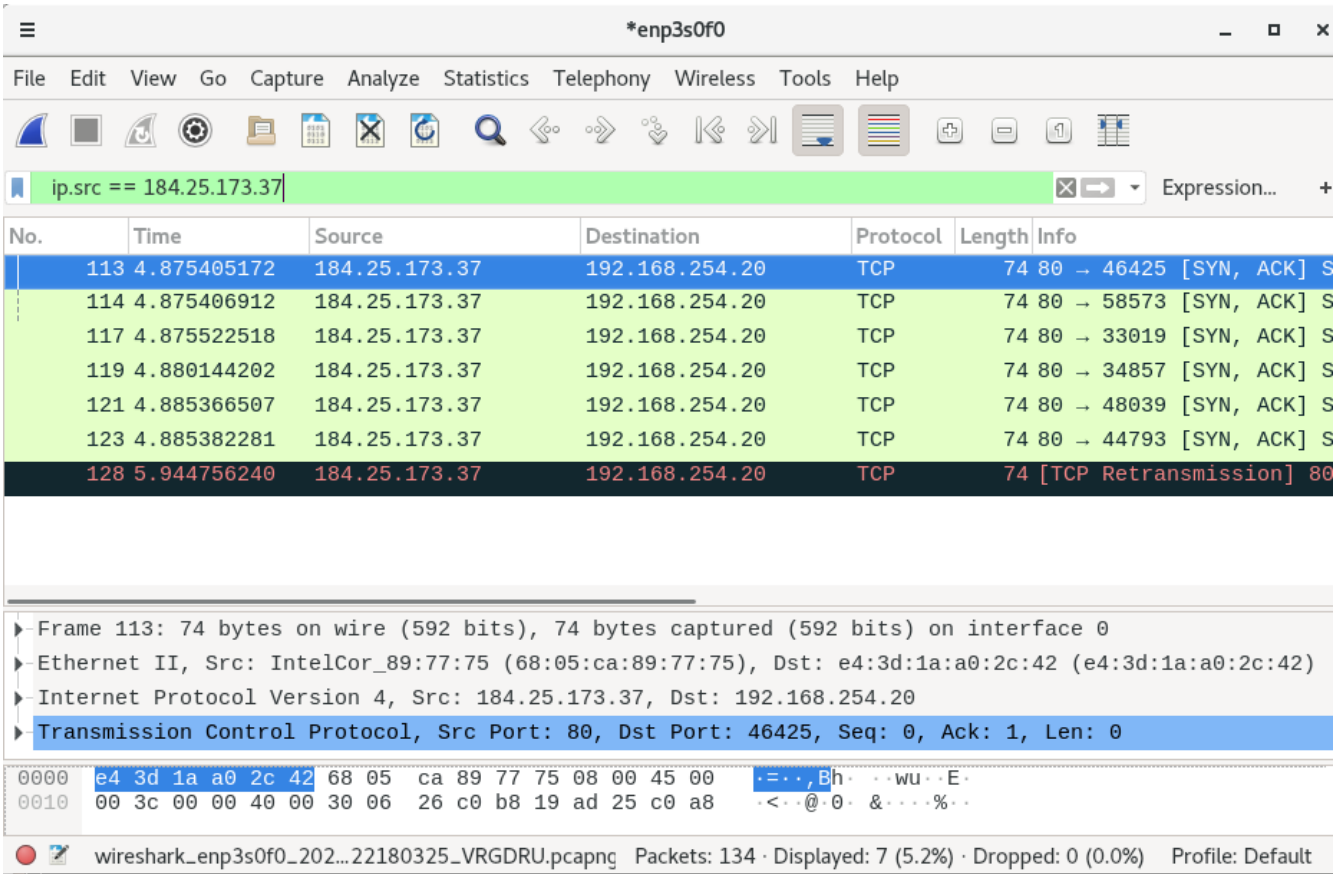
14)

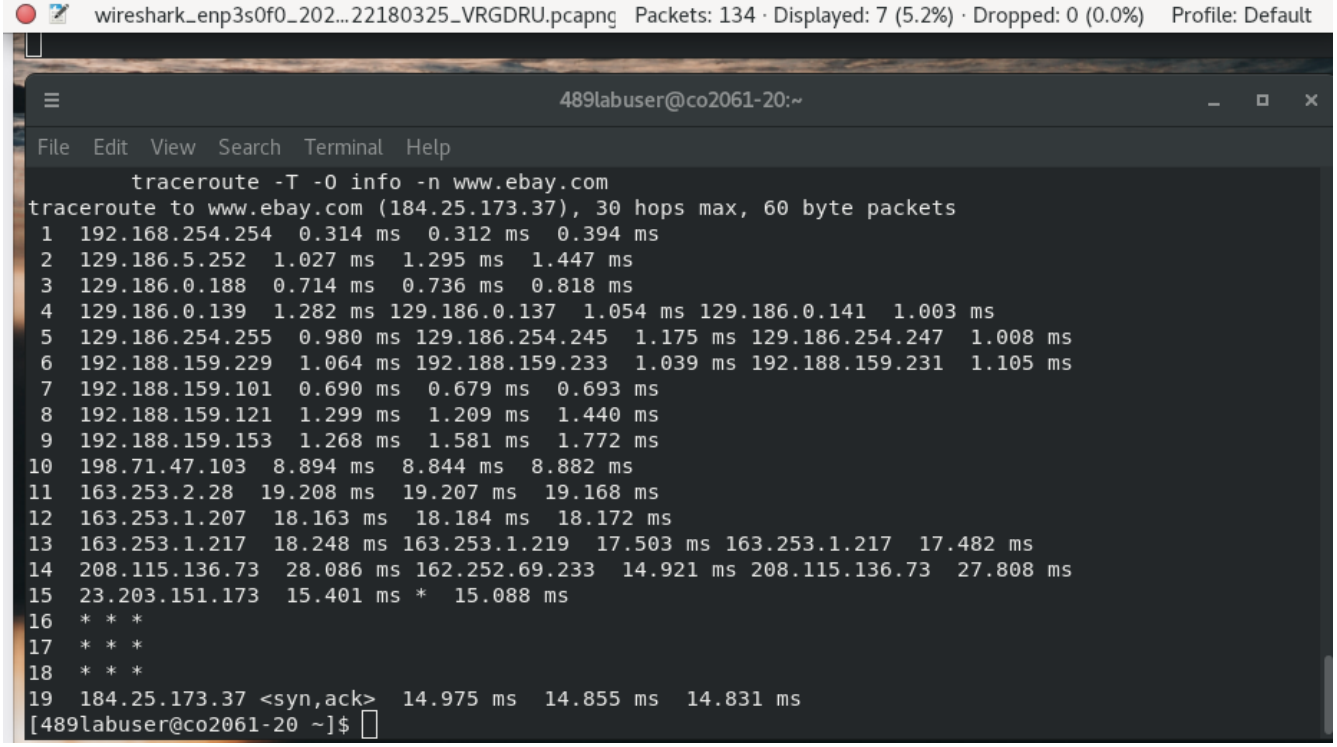
traceroute:

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