```
489labuser@co2061-06:~
File  Edit  View  Search  Terminal  Help
[489labuser@co2061-06 ~]$ ping www.iastate.edu
PING www.iastate.edu (20.221.234.34) 56(84) bytes of data.
64 bytes from 20.221.234.34 (20.221.234.34): icmp_seq=1 ttl=106 time=25.1 ms
64 bytes from 20.221.234.34 (20.221.234.34): icmp_seq=2 ttl=106 time=25.4 ms
64 bytes from 20.221.234.34 (20.221.234.34): icmp_seq=3 ttl=106 time=25.5 ms
^C
--- www.iastate.edu ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 25.060/25.333/25.548/0.203 ms
[489labuser@co2061-06 ~]$ ping 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=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.074 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.074 ms
^C
--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2086ms
rtt min/avg/max/mdev = 0.039/0.062/0.074/0.017 ms
[489labuser@co2061-06 ~]$
```

1. and 2. This is the screen shot for pinging www.iastate.edu and 127.0.0.1 ip. The time is at the end of the line is the round trip time. Between the two you can see that the time was a significantly smaller for 127.0.0.1 compared to www.iastate.edu.

```
489labuser@co2061-06:~
File  Edit  View  Search  Terminal  Help
[489labuser@co2061-06 ~]$ www.google.com
bash: www.google.com: command not found...
ping [489labuser@co2061-06 ~]$ ping www.google.com
PING www.google.com (142.250.69.228) 56(84) bytes of data.
64 bytes from den08s05-in-f4.1e100.net (142.250.69.228): icmp_seq=1 ttl=111 time
=25.8 ms
64 bytes from den08s05-in-f4.1e100.net (142.250.69.228): icmp_seq=2 ttl=111 time
=26.2 ms
64 bytes from den08s05-in-f4.1e100.net (142.250.69.228): icmp_seq=3 ttl=111 time
=26.0 ms
^C
--- www.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 25.847/26.004/26.160/0.225 ms
[489labuser@co2061-06 ~]$ ping www.cam.ac.uk
PING www.cam.ac.uk (128.232.132.8) 56(84) bytes of data.
64 bytes from tm-128-232-132-8.tm.uis.cam.ac.uk (128.232.132.8): icmp_seq=1 ttl=
38 time=119 ms
64 bytes from tm-128-232-132-8.tm.uis.cam.ac.uk (128.232.132.8): icmp_seq=2 ttl=
38 time=119 ms
64 bytes from tm-128-232-132-8.tm.uis.cam.ac.uk (128.232.132.8): icmp_seq=3 ttl=
38 time=119 ms
^C
--- www.cam.ac.uk ping statistics ---
```

These are the screen caps for pinging
This is the screen shot from google and cam.ac.uk. The response times are different by around 100 ms.

```
489labuser@co2061-06:~
File  Edit  View  Search  Terminal  Help
** server can't find www.istate.edu: NXDOMAIN

[489labuser@co2061-06 ~]$ nslookup
> set type=A
> www.iastate.edu
Server:         129.186.1.200
Address:        129.186.1.200#53

Name:   www.iastate.edu
Address: 20.221.234.34
> ^C[489labuser@co2061-06 ~]$
[489labuser@co2061-06 ~]$ nslookup www.iastate.edu
Server:         129.186.1.200
Address:        129.186.1.200#53

Name:   www.iastate.edu
Address: 20.221.234.34

[489labuser@co2061-06 ~]$ nslookup microsoft.com
Server:         129.186.1.200
Address:        129.186.1.200#53

Non-authoritative answer:
Name:   microsoft.com
```

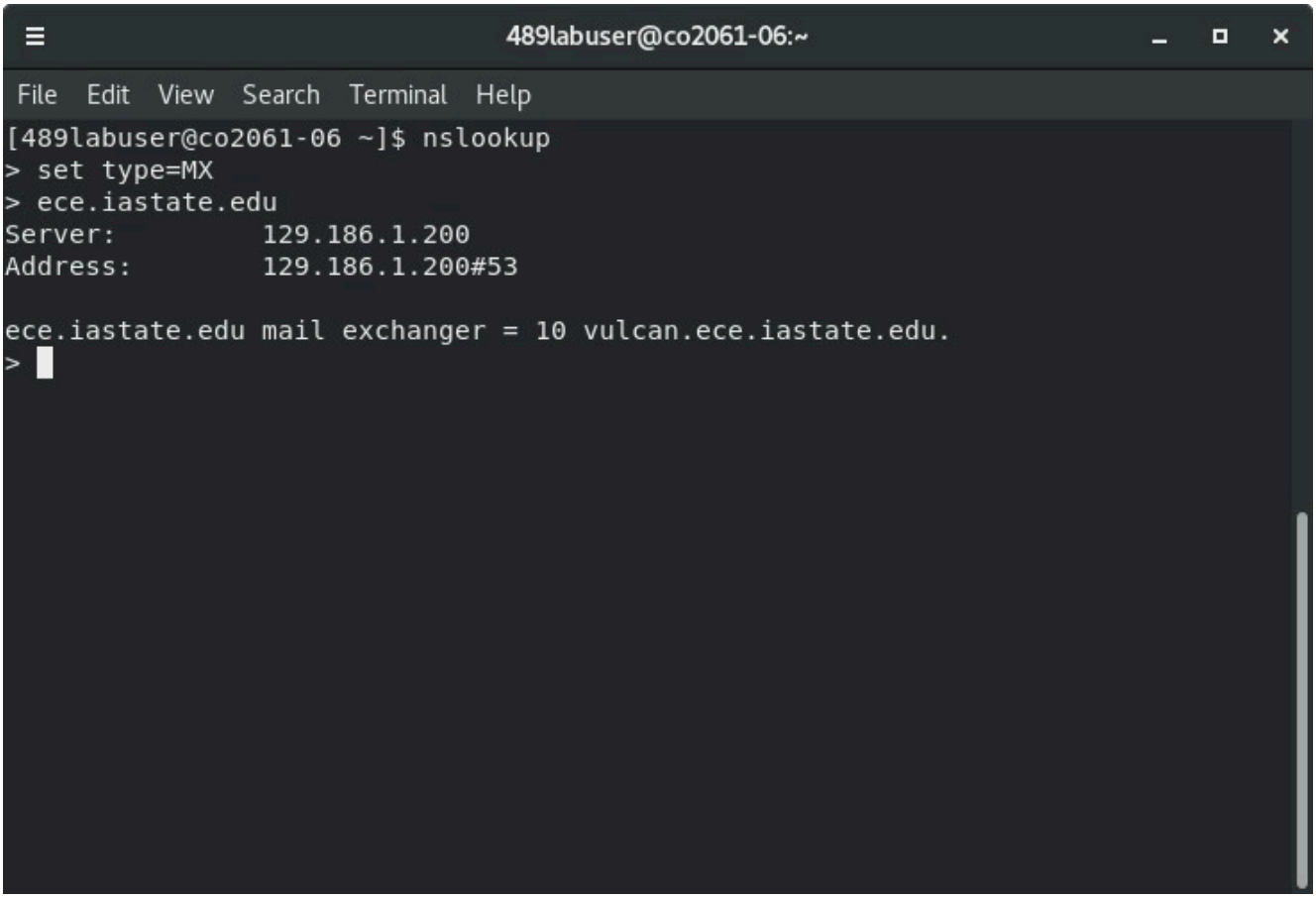
3. This is screen shot of using nslookup with www.iastate.edu

```
489labuser@co2061-06:~
File  Edit  View  Search  Terminal  Help
[489labuser@co2061-06 ~]$ nslookup 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.e
dgekey.net.globalredir.akadns.net.
www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net        canonical name =
 e13678.dscb.akamaiedge.net.
Name:   e13678.dscb.akamaiedge.net
Address: 69.192.209.170
Name:   e13678.dscb.akamaiedge.net
Address: 2600:1404:9400:183::356e
Name:   e13678.dscb.akamaiedge.net
Address: 2600:1404:9400:189::356e
Name:   e13678.dscb.akamaiedge.net
Address: 2600:1404:9400:19a::356e
Name:   e13678.dscb.akamaiedge.net
Address: 2600:1404:9400:18b::356e
Name:   e13678.dscb.akamaiedge.net
Address: 2600:1404:9400:1a3::356e

[489labuser@co2061-06 ~]$
```

3. This is the screenshot for nslookup on www.microsoft.com

```
489labuser@co2061-06:~
File  Edit  View  Search  Terminal  Help
Address: 69.192.209.170
Name:   e13678.dscb.akamaiedge.net
Address: 2600:1404:9400:183::356e
Name:   e13678.dscb.akamaiedge.net
Address: 2600:1404:9400:189::356e
Name:   e13678.dscb.akamaiedge.net
Address: 2600:1404:9400:19a::356e
Name:   e13678.dscb.akamaiedge.net
Address: 2600:1404:9400:18b::356e
Name:   e13678.dscb.akamaiedge.net
Address: 2600:1404:9400:1a3::356e

[489labuser@co2061-06 ~]$ nslookup 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
Name:   ncredir-lb.wikimedia.org
Address: 2620:0:861:ed1a::9

[489labuser@co2061-06 ~]$
```

3. This is the nslookup for www.wikipedia.com



4. This is the interactive lookup for the mail exchanger for ece.iastate.edu

```
489labuser@co2061-06:~
File  Edit  View  Search  Terminal  Help
[489labuser@co2061-06 ~]$ nslookup
> set type=PTR
> 129.186.215.40
Server:         129.186.1.200
Address:        129.186.1.200#53

Non-authoritative answer:
40.215.186.129.in-addr.arpa     name = spock.ee.iastate.edu.

Authoritative answers can be found from:
>
```

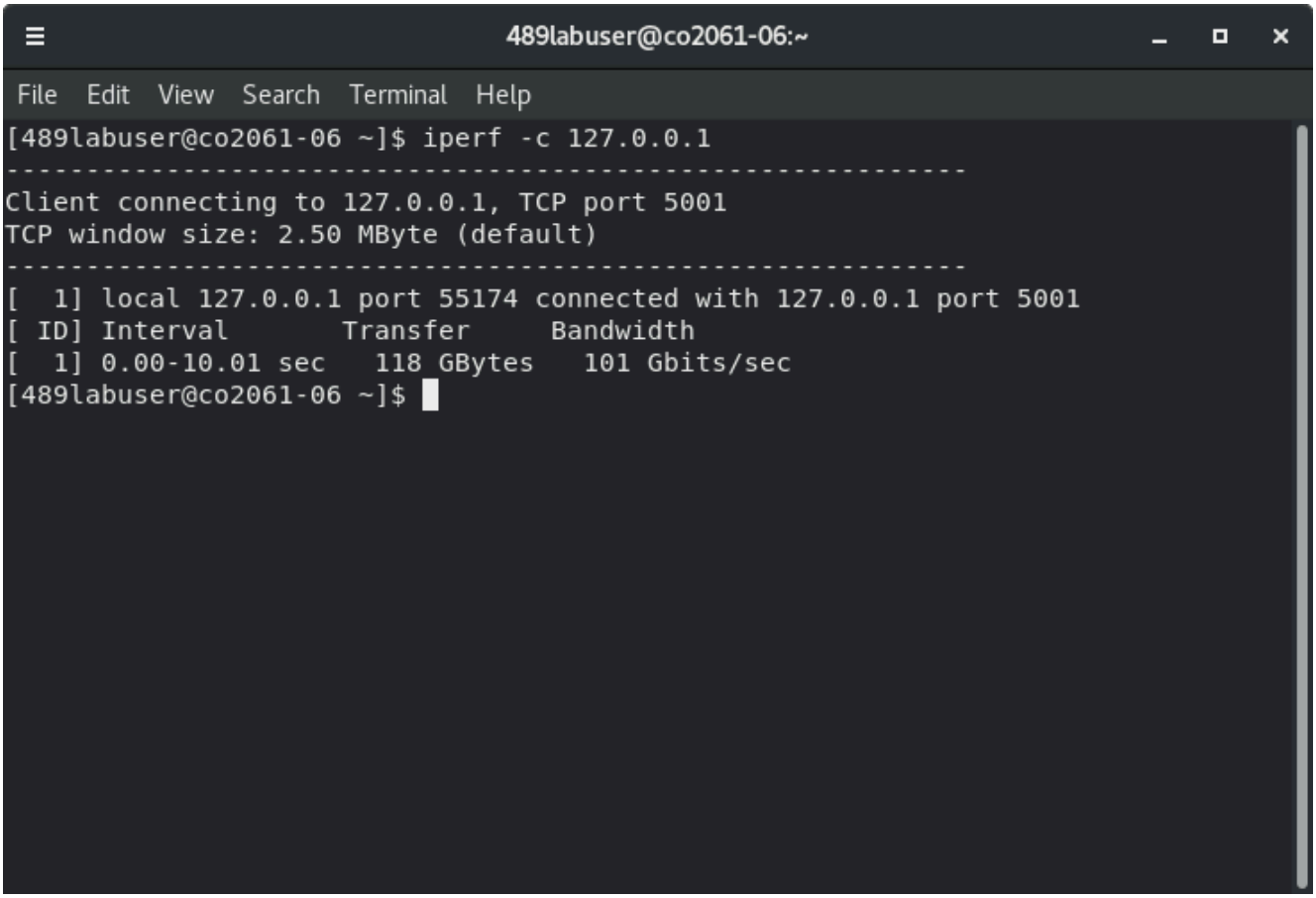
5. This is the nslookup for the hostname for 129.186.215.40. The name is spock.ee.iastate.edu.

```
489labuser@co2061-06:~
File  Edit  View  Search  Terminal  Help
        ether 74:86:e2:28:9c:dd  txqueuelen 1000  (Ethernet)
        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  collisions 0
        device interrupt 19  memory 0x72280000-722a0000

enp3s0f0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.254.6  netmask 255.255.255.0  broadcast 192.168.254.255
        inet6 fe80::e63d:1aff:fea0:29be  prefixlen 64  scopeid 0x20<link>
        ether e4:3d:1a:a0:29:be  txqueuelen 1000  (Ethernet)
        RX packets 2387888  bytes 1554000752 (1.4 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 657743  bytes 313699637 (299.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16

enp3s0f1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.75.6  netmask 255.255.255.0  broadcast 192.168.75.255
        inet6 fe80::e63d:1aff:fea0:29bf  prefixlen 64  scopeid 0x20<link>
        ether e4:3d:1a:a0:29:bf  txqueuelen 1000  (Ethernet)
        RX packets 1010140  bytes 77062216 (73.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 584  bytes 47778 (46.6 KiB)
```

6. Here are some of the results from running ifconfig. We are specifically looking at “en3s0f0” at we can see the inet field to find the ip: 192.168.254.6

```
489labuser@co2061-06:~
File  Edit  View  Search  Terminal  Help
[489labuser@co2061-06 ~]$ iperf -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
------------------------------------------------------------
[  1] local 127.0.0.1 port 5001 connected with 127.0.0.1 port 55174
[ ID] Interval       Transfer     Bandwidth
[  1] 0.00-10.00 sec   118 GBytes   101 Gbits/sec
```

This is the first terminal with iperf being the server.



7. This is the second tereminal it is acting as the client. The measured bandwidth is 101 Gbits/sec

```
489labuser@co2061-06:~
File  Edit  View  Search  Terminal  Help
        TX packets 4531501  bytes 126841292687 (118.1 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
        ether 52:54:00:36:a5:56  txqueuelen 1000  (Ethernet)
        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  collisions 0

[489labuser@co2061-06 ~]$ tcpdump
tcpdump: enp3s0f0: You don't have permission to capture on that device
(socket: Operation not permitted)
[489labuser@co2061-06 ~]$ sudo /usr/sbin/tcp -i enp3s0f0
[sudo] password for 489labuser:
[sudo] password for 489labuser:
Sorry, try again.
[sudo] password for 489labuser:
Sorry, try again.
[sudo] password for 489labuser:
sudo: /usr/sbin/tcp: command not found
[489labuser@co2061-06 ~]$ clear

[489labuser@co2061-06 ~]$ traceroute www.google.com
traceroute to www.google.com (142.250.72.36), 30 hops max, 60 byte packets
 1  _gateway (192.168.254.254)  0.522 ms  0.521 ms  0.519 ms
 2  routerb-129-186-5-0.tele.iastate.edu (129.186.5.253)  1.383 ms  1.554 ms  1.851 ms
 3  e63-mpls-p-hu0-3-0-10--to--c12-mpls-pe-eth1-12.tele.iastate.edu (129.186.0.194)  1.017 ms  1.038 ms b31-mpls-p-hu0-3-0-10--to--c12-mpls-pe-eth1-1.tele.iastate.edu (129.186.0.192)  1.176 ms
 4  b31-mpls-fpe-eth2-10--to--e63-mpls-p-hu0-2-0-1.tele.iastate.edu (129.186.0.141)  1.506 ms b31-mpls-fpe-eth1-10--to--b31-mpls-p-hu0-2-0-1.tele.iastate.edu (129.186.0.135)  1.166 ms e63-mpls-fpe-eth2-10--to--e
63-mpls-p-hu0-3-0-1.tele.iastate.edu (129.186.0.139)  1.285 ms
 5  e63fr--e63fpe-vrf-data.tele.iastate.edu (129.186.254.253)  1.306 ms e63fr--b31fpe-vrf-data.tele.iastate.edu (129.186.254.245)  1.521 ms e63fr--e63fpe-vrf-data.tele.iastate.edu (129.186.254.253)  1.340 ms
 6  b31be-eth2-2.fusion.tele.iastate.edu (192.188.159.233)  1.409 ms e63be-eth1-2.fusion.tele.iastate.edu (192.188.159.229)  1.240 ms e63be-eth2-2.fusion.tele.iastate.edu (192.188.159.231)  1.136 ms
 7  routerb-192-188-159-96.tele.iastate.edu (192.188.159.101)  1.106 ms  0.932 ms  0.909 ms
 8  rtr-e63be-vlan934.tele.iastate.edu (192.188.159.122)  1.438 ms  1.829 ms  1.745 ms
 9  rtr-b31isp1-be158.tele.iastate.edu (192.188.159.159)  1.423 ms  1.745 ms  3.671 ms
10  bundle-ether100.1421.core2.kans.net.internet2.edu (198.71.47.103)  7.477 ms  7.482 ms  7.524 ms
11  fourhundredge-0-0-0-0.4079.core1.chic.net.internet2.edu (163.253.2.28)  18.776 ms  18.803 ms  18.026 ms
12  fourhundredge-0-0-0-0.4079.core1.eqch.net.internet2.edu (163.253.1.207)  18.465 ms  18.454 ms  18.518 ms
13  fourhundredge-0-0-0-49.4079.agg2.eqch.net.internet2.edu (163.253.1.219)  28.040 ms fourhundredge-0-0-0-48.4079.agg2.eqch.net.internet2.edu (163.253.1.217)  28.037 ms fourhundredge-0-0-0-49.4079.agg2.eqch.net
.internet2.edu (163.253.1.219)  28.060 ms
14  72.14.216.92 (72.14.216.92)  15.465 ms  14.965 ms  15.079 ms
15  * * *
16  108.170.243.225 (108.170.243.225)  15.887 ms 142.251.60.202 (142.251.60.202)  14.989 ms 142.251.61.40 (142.251.61.40)  15.089 ms
17  108.170.243.165 (108.170.243.165)  15.432 ms 108.170.243.233 (108.170.243.233)  41.514 ms 108.170.244.15 (108.170.244.15)  14.888 ms
18  * 142.251.234.40 (142.251.234.40)  60.486 ms  16.111 ms
19  192.178.72.201 (192.178.72.201)  73.606 ms 192.178.72.199 (192.178.72.199)  27.200 ms 192.178.72.204 (192.178.72.204)  95.609 ms
20  172.253.77.137 (172.253.77.137)  28.120 ms 209.85.248.175 (209.85.248.175)  26.333 ms 142.251.250.181 (142.251.250.181)  27.926 ms
21  172.253.74.23 (172.253.74.23)  26.863 ms 209.85.247.43 (209.85.247.43)  26.275 ms 172.253.74.23 (172.253.74.23)  26.826 ms
22  172.253.51.83 (172.253.51.83)  25.909 ms  25.877 ms  25.948 ms
23  108.170.228.25 (108.170.228.25)  25.920 ms 192.178.96.201 (192.178.96.201)  26.835 ms 192.178.96.191 (192.178.96.191)  26.474 ms
24  172.253.75.177 (172.253.75.177)  25.860 ms  25.564 ms 209.85.142.171 (209.85.142.171)  25.549 ms
25  den16s08-in-f4.1e100.net (142.250.72.36)  25.809 ms  25.908 ms  25.723 ms
[489labuser@co2061-06 ~]$
```

8. This is result of running traceroute to www.google.com. There was a lot of hops as we can see. It recorded 25 hops to different routers and ips. There are two things that are interesting. The first, is that from 9 to 10 the latency jumps up and stay high for the following routes. The other is that 15 is blocked. That means there is a firewall that is blocking source UDP files that it has to send back which causes us to not receive any information back about the packets.

```
489labuser@co2061-06:~
File  Edit  View  Search  Terminal  Help
64 bytes from 192.168.254.5: icmp_seq=12 ttl=64 time=0.815 ms
64 bytes from 192.168.254.5: icmp_seq=13 ttl=64 time=0.804 ms
64 bytes from 192.168.254.5: icmp_seq=14 ttl=64 time=0.835 ms
64 bytes from 192.168.254.5: icmp_seq=15 ttl=64 time=1.16 ms
64 bytes from 192.168.254.5: icmp_seq=16 ttl=64 time=0.814 ms
64 bytes from 192.168.254.5: icmp_seq=17 ttl=64 time=1.18 ms
64 bytes from 192.168.254.5: icmp_seq=18 ttl=64 time=1.05 ms
64 bytes from 192.168.254.5: icmp_seq=19 ttl=64 time=1.02 ms
64 bytes from 192.168.254.5: icmp_seq=20 ttl=64 time=1.03 ms
64 bytes from 192.168.254.5: icmp_seq=21 ttl=64 time=1.01 ms
64 bytes from 192.168.254.5: icmp_seq=22 ttl=64 time=0.969 ms
64 bytes from 192.168.254.5: icmp_seq=23 ttl=64 time=0.890 ms
64 bytes from 192.168.254.5: icmp_seq=24 ttl=64 time=0.627 ms
64 bytes from 192.168.254.5: icmp_seq=25 ttl=64 time=0.793 ms
64 bytes from 192.168.254.5: icmp_seq=26 ttl=64 time=0.651 ms
64 bytes from 192.168.254.5: icmp_seq=27 ttl=64 time=0.796 ms
64 bytes from 192.168.254.5: icmp_seq=28 ttl=64 time=0.736 ms
64 bytes from 192.168.254.5: icmp_seq=29 ttl=64 time=1.02 ms
64 bytes from 192.168.254.5: icmp_seq=30 ttl=64 time=0.830 ms
64 bytes from 192.168.254.5: icmp_seq=31 ttl=64 time=1.06 ms
64 bytes from 192.168.254.5: icmp_seq=32 ttl=64 time=0.910 ms
64 bytes from 192.168.254.5: icmp_seq=33 ttl=64 time=0.769 ms
^C
--- 192.168.254.5 ping statistics ---
33 packets transmitted, 33 received, 0% packet loss, time 32198ms
rtt min/avg/max/mdev = 0.627/0.951/1.365/0.157 ms
[489labuser@co2061-06 ~]$ tcptraceroute -q 2 google.com
Running:
        traceroute -T -O info -q 2 google.com
You do not have enough privileges to use this traceroute method.
socket: Operation not permitted
[489labuser@co2061-06 ~]$ sudo tcptraceroute -q 2 google.com
[sudo] password for 489labuser:
Running:
        traceroute -T -O info -q 2 google.com
traceroute to google.com (142.250.72.14), 30 hops max, 60 byte packets
 1  _gateway (192.168.254.254)  0.529 ms  0.552 ms
 2  routerb-129-186-5-0.tele.iastate.edu (129.186.5.253)  1.056 ms  1.324 ms
 3  b31-mpls-p-hu0-3-0-10--to--c12-mpls-pe-eth1-1.tele.iastate.edu (129.186.0.192)  0.873 ms  0.898 ms
 4  b31-mpls-fpe-eth2-10--to--e63-mpls-p-hu0-2-0-1.tele.iastate.edu (129.186.0.141)  1.316 ms e63-mpls-fpe-eth1-10--to--b31-mpls-p-hu0-3-0-1.tele.iastate.edu (129.186.0.137)  1.222 ms
 5  e63fr--b31fpe-vrf-data.tele.iastate.edu (129.186.254.245)  1.037 ms e63fr--e63fpe-vrf-data.tele.iastate.edu (129.186.254.253)  1.216 ms
 6  b31be-eth1-2.fusion.tele.iastate.edu (192.188.159.227)  1.031 ms  1.301 ms
 7  routerb-192-188-159-96.tele.iastate.edu (192.188.159.101)  0.893 ms  0.875 ms
 8  rtr-e63be-vlan934.tele.iastate.edu (192.188.159.122)  1.500 ms  1.786 ms
 9  rtr-b31isp1-be158.tele.iastate.edu (192.188.159.159)  1.568 ms  1.567 ms
10  bundle-ether100.1421.core2.kans.net.internet2.edu (198.71.47.103)  8.256 ms  8.254 ms
11  fourhundredge-0-0-0-0.4079.core1.chic.net.internet2.edu (163.253.2.28)  18.283 ms  18.265 ms
12  fourhundredge-0-0-0-0.4079.core1.eqch.net.internet2.edu (163.253.1.207)  19.741 ms  19.723 ms
13  fourhundredge-0-0-0-48.4079.agg2.eqch.net.internet2.edu (163.253.1.217)  19.550 ms  19.538 ms
14  72.14.216.92 (72.14.216.92)  16.040 ms  15.166 ms
15  74.125.251.183 (74.125.251.183)  15.168 ms 108.170.243.225 (108.170.243.225)  16.529 ms
16  108.170.243.254 (108.170.243.254)  16.340 ms 108.170.243.197 (108.170.243.197)  17.239 ms
17  142.251.234.163 (142.251.234.163)  16.240 ms 142.251.234.40 (142.251.234.40)  16.506 ms
18  192.178.72.204 (192.178.72.204)  33.126 ms 192.178.72.199 (192.178.72.199)  25.804 ms
19  209.85.142.165 (209.85.142.165)  27.036 ms 209.85.246.165 (209.85.246.165)  26.045 ms
20  209.85.247.43 (209.85.247.43)  25.843 ms 142.250.236.43 (142.250.236.43)  25.796 ms
21  172.253.51.117 (172.253.51.117)  25.670 ms 172.253.51.77 (172.253.51.77)  25.633 ms
22  216.239.58.179 (216.239.58.179)  25.422 ms 209.85.143.67 (209.85.143.67)  25.501 ms
23  142.251.51.221 (142.251.51.221)  25.616 ms  25.668 ms
24  den08s06-in-f14.1e100.net (142.250.72.14) <syn,ack>  25.481 ms  25.468 ms
[489labuser@co2061-06 ~]$
```

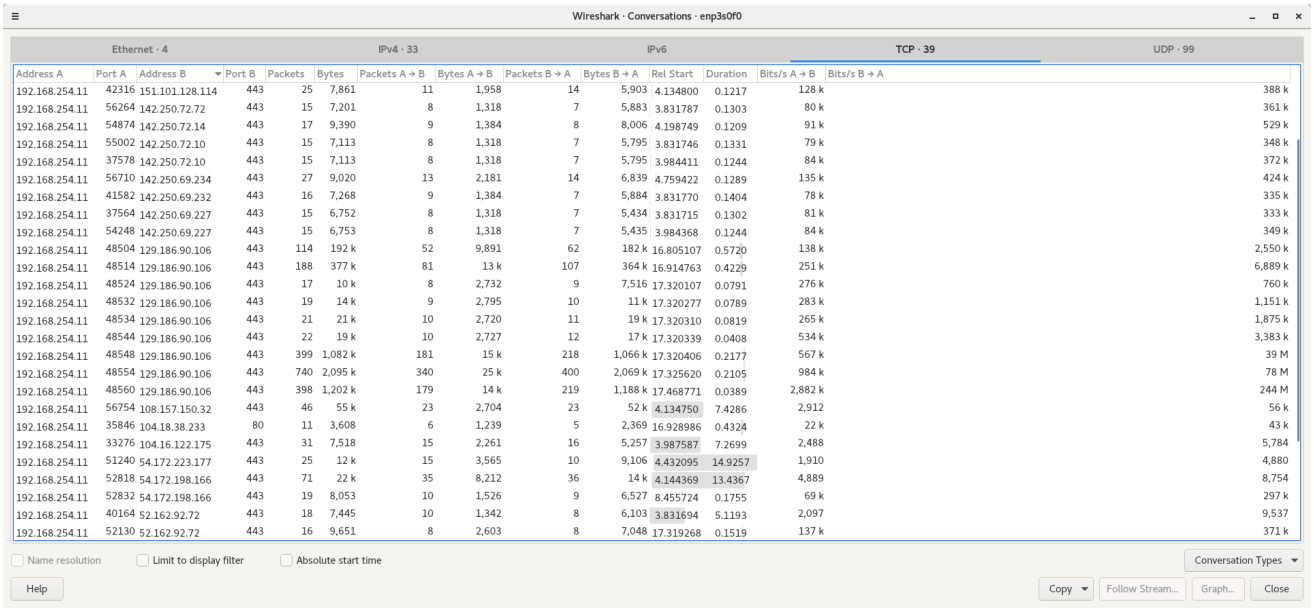
9. This is the result of running tcptraceroute on google. In this case opposed to the UDP version we are able to receive information about 15. This means it must not be blocking TCP packets? Another interesting thing was that running multiple tests it went through the same network route when running multiple tests.

```
489labuser@co2061-06:~
File  Edit  View  Search  Terminal  Help
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
[489labuser@co2061-06 ~]$ nmap -Pn 192.168.254.6
Starting Nmap 7.70 ( https://nmap.org ) at 2024-01-23 15:35 CST
Nmap scan report for 192.168.254.6
Host is up (0.000034s 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 0.02 seconds
[489labuser@co2061-06 ~]$
```

10. This is the nmap results. We can see that 22/tcp is open which is the SSH service

```
489labuser@co2061-06:~
File  Edit  View  Search  Terminal  Help
15:44:09.016049 IP co2061-06.ece.iastate.edu.45317 > den08s05-in-f14.1e100.net.https: UDP, length 113
15:44:09.016141 IP co2061-06.ece.iastate.edu.45317 > den08s05-in-f14.1e100.net.https: UDP, length 1357
15:44:09.016146 IP co2061-06.ece.iastate.edu.45317 > den08s05-in-f14.1e100.net.https: UDP, length 1028
15:44:09.031547 IP den08s05-in-f14.1e100.net.https > co2061-06.ece.iastate.edu.45317: UDP, length 27
15:44:09.055979 IP den08s05-in-f14.1e100.net.https > co2061-06.ece.iastate.edu.45317: UDP, length 123
15:44:09.061752 IP den08s05-in-f14.1e100.net.https > co2061-06.ece.iastate.edu.45317: UDP, length 30
15:44:09.061850 IP co2061-06.ece.iastate.edu.45317 > den08s05-in-f14.1e100.net.https: UDP, length 31
15:44:09.072901 IP den08s05-in-f14.1e100.net.https > co2061-06.ece.iastate.edu.45317: UDP, length 1353
15:44:09.072945 IP den08s05-in-f14.1e100.net.https > co2061-06.ece.iastate.edu.45317: UDP, length 605
15:44:09.073269 IP co2061-06.ece.iastate.edu.45317 > den08s05-in-f14.1e100.net.https: UDP, length 36
15:44:09.124576 IP den08s05-in-f14.1e100.net.https > co2061-06.ece.iastate.edu.45317: UDP, length 27
15:44:10.504131 STP 802.1w, Rapid STP, Flags [Learn, Forward, Agreement], bridge-id 8000.4c:60:de:68:88:4c.800e, length 43
15:44:12.503449 STP 802.1w, Rapid STP, Flags [Learn, Forward, Agreement], bridge-id 8000.4c:60:de:68:88:4c.800e, length 43
15:44:14.502481 STP 802.1w, Rapid STP, Flags [Learn, Forward, Agreement], bridge-id 8000.4c:60:de:68:88:4c.800e, length 43
15:44:14.842407 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 4c:60:de:68:88:4c (oui Unknown), length 280
15:44:14.842674 IP co2061-06.ece.iastate.edu.58316 > ns-1.iastate.edu.domain: 15949+ PTR? 255.255.255.255.in-addr.arpa. (46)
15:44:14.844023 IP ns-1.iastate.edu.domain > co2061-06.ece.iastate.edu.58316: 15949 NXDomain 0/1/0 (114)
15:44:14.844263 IP co2061-06.ece.iastate.edu.55912 > ns-1.iastate.edu.domain: 35051+ PTR? 0.0.0.0.in-addr.arpa. (38)
15:44:14.845191 IP ns-1.iastate.edu.domain > co2061-06.ece.iastate.edu.55912: 35051 NXDomain 0/1/0 (106)
15:44:16.501993 STP 802.1w, Rapid STP, Flags [Learn, Forward, Agreement], bridge-id 8000.4c:60:de:68:88:4c.800e, length 43
15:44:18.501337 STP 802.1w, Rapid STP, Flags [Learn, Forward, Agreement], bridge-id 8000.4c:60:de:68:88:4c.800e, length 43
15:44:19.347999 IP 192.168.254.5 > co2061-06.ece.iastate.edu: ICMP echo request, id 8, seq 1, length 64
15:44:19.348083 IP co2061-06.ece.iastate.edu > 192.168.254.5: ICMP echo reply, id 8, seq 1, length 64
15:44:19.348268 IP co2061-06.ece.iastate.edu.42151 > ns-1.iastate.edu.domain: 64328+ PTR? 5.254.168.192.in-addr.arpa. (44)
15:44:19.349544 IP ns-1.iastate.edu.domain > co2061-06.ece.iastate.edu.42151: 64328 NXDomain 0/1/0 (121)
15:44:20.349105 IP 192.168.254.5 > co2061-06.ece.iastate.edu: ICMP echo request, id 8, seq 2, length 64
15:44:20.349140 IP co2061-06.ece.iastate.edu > 192.168.254.5: ICMP echo reply, id 8, seq 2, length 64
15:44:20.500616 STP 802.1w, Rapid STP, Flags [Learn, Forward, Agreement], bridge-id 8000.4c:60:de:68:88:4c.800e, length 43
15:44:21.392442 IP 192.168.254.5 > co2061-06.ece.iastate.edu: ICMP echo request, id 8, seq 3, length 64
15:44:21.392510 IP co2061-06.ece.iastate.edu > 192.168.254.5: ICMP echo reply, id 8, seq 3, length 64
15:44:22.393900 IP 192.168.254.5 > co2061-06.ece.iastate.edu: ICMP echo request, id 8, seq 4, length 64
15:44:22.393964 IP co2061-06.ece.iastate.edu > 192.168.254.5: ICMP echo reply, id 8, seq 4, length 64
15:44:22.499876 STP 802.1w, Rapid STP, Flags [Learn, Forward, Agreement], bridge-id 8000.4c:60:de:68:88:4c.800e, length 43
15:44:23.440428 IP 192.168.254.5 > co2061-06.ece.iastate.edu: ICMP echo request, id 8, seq 5, length 64
15:44:23.440496 IP co2061-06.ece.iastate.edu > 192.168.254.5: ICMP echo reply, id 8, seq 5, length 64
15:44:24.441694 IP 192.168.254.5 > co2061-06.ece.iastate.edu: ICMP echo request, id 8, seq 6, length 64
15:44:24.441758 IP co2061-06.ece.iastate.edu > 192.168.254.5: ICMP echo reply, id 8, seq 6, length 64
15:44:24.499268 STP 802.1w, Rapid STP, Flags [Learn, Forward, Agreement], bridge-id 8000.4c:60:de:68:88:4c.800e, length 43
15:44:24.719694 ARP, Request who-has 192.168.254.5 tell co2061-06.ece.iastate.edu, length 28
15:44:24.720353 ARP, Reply 192.168.254.5 is-at e4:3d:1a:a0:35:36 (oui Unknown), length 46
15:44:24.792083 IP co2061-06.ece.iastate.edu.33449 > ns-1.iastate.edu.domain: 59612+ A? play.google.com. (33)
15:44:24.792088 IP co2061-06.ece.iastate.edu.33449 > ns-1.iastate.edu.domain: 43485+ AAAA? play.google.com. (33)
15:44:24.792547 IP co2061-06.ece.iastate.edu.45317 > den08s05-in-f14.1e100.net.https: UDP, length 1357
15:44:24.792558 IP co2061-06.ece.iastate.edu.45317 > den08s05-in-f14.1e100.net.https: UDP, length 940
15:44:24.793141 IP ns-1.iastate.edu.domain > co2061-06.ece.iastate.edu.33449: 43485 1/0/0 AAAA 2607:f8b0:400f:802::200e (61)
15:44:24.793177 IP ns-1.iastate.edu.domain > co2061-06.ece.iastate.edu.33449: 59612 1/0/0 A 142.250.69.238 (49)
15:44:24.818459 IP den08s05-in-f14.1e100.net.https > co2061-06.ece.iastate.edu.45317: UDP, length 30
15:44:24.831354 IP den08s05-in-f14.1e100.net.https > co2061-06.ece.iastate.edu.45317: UDP, length 1353
15:44:24.831404 IP den08s05-in-f14.1e100.net.https > co2061-06.ece.iastate.edu.45317: UDP, length 372
15:44:24.831761 IP den08s05-in-f14.1e100.net.https > co2061-06.ece.iastate.edu.45317: UDP, length 25
15:44:24.831796 IP co2061-06.ece.iastate.edu.45317 > den08s05-in-f14.1e100.net.https: UDP, length 41
15:44:24.848149 ARP, Request who-has co2061-06.ece.iastate.edu tell 192.168.254.5, length 46
15:44:24.848176 ARP, Reply co2061-06.ece.iastate.edu is-at e4:3d:1a:a0:29:be (oui Unknown), length 28
15:44:24.852343 IP co2061-06.ece.iastate.edu.45317 > den08s05-in-f14.1e100.net.https: UDP, length 32
15:44:24.865023 IP co2061-06.ece.iastate.edu.48490 > ns-1.iastate.edu.domain: 35435+ A? play.google.com. (33)
15:44:24.865026 IP co2061-06.ece.iastate.edu.48490 > ns-1.iastate.edu.domain: 1901+ AAAA? play.google.com. (33)
15:44:24.865595 IP co2061-06.ece.iastate.edu.45317 > den08s05-in-f14.1e100.net.https: UDP, length 1357
15:44:24.865604 IP co2061-06.ece.iastate.edu.45317 > den08s05-in-f14.1e100.net.https: UDP, length 403
15:44:24.866180 IP ns-1.iastate.edu.domain > co2061-06.ece.iastate.edu.48490: 35435 1/0/0 A 142.250.72.78 (49)
15:44:24.866198 IP ns-1.iastate.edu.domain > co2061-06.ece.iastate.edu.48490: 1901 1/0/0 AAAA 2607:f8b0:400f:804::200e (61)
15:44:24.882785 IP den08s05-in-f14.1e100.net.https > co2061-06.ece.iastate.edu.45317: UDP, length 27
```

11. This is showing tcpdump. Here my friend Yi is sending packets to me. I found his ip to be 192.168.254.5 which he confirmed to be right.



Wireshark · Conversations · enp3s0f0

Ethernet · 4 | IPv4 · 33 | IPv6 | TCP · 39 | UDP · 99

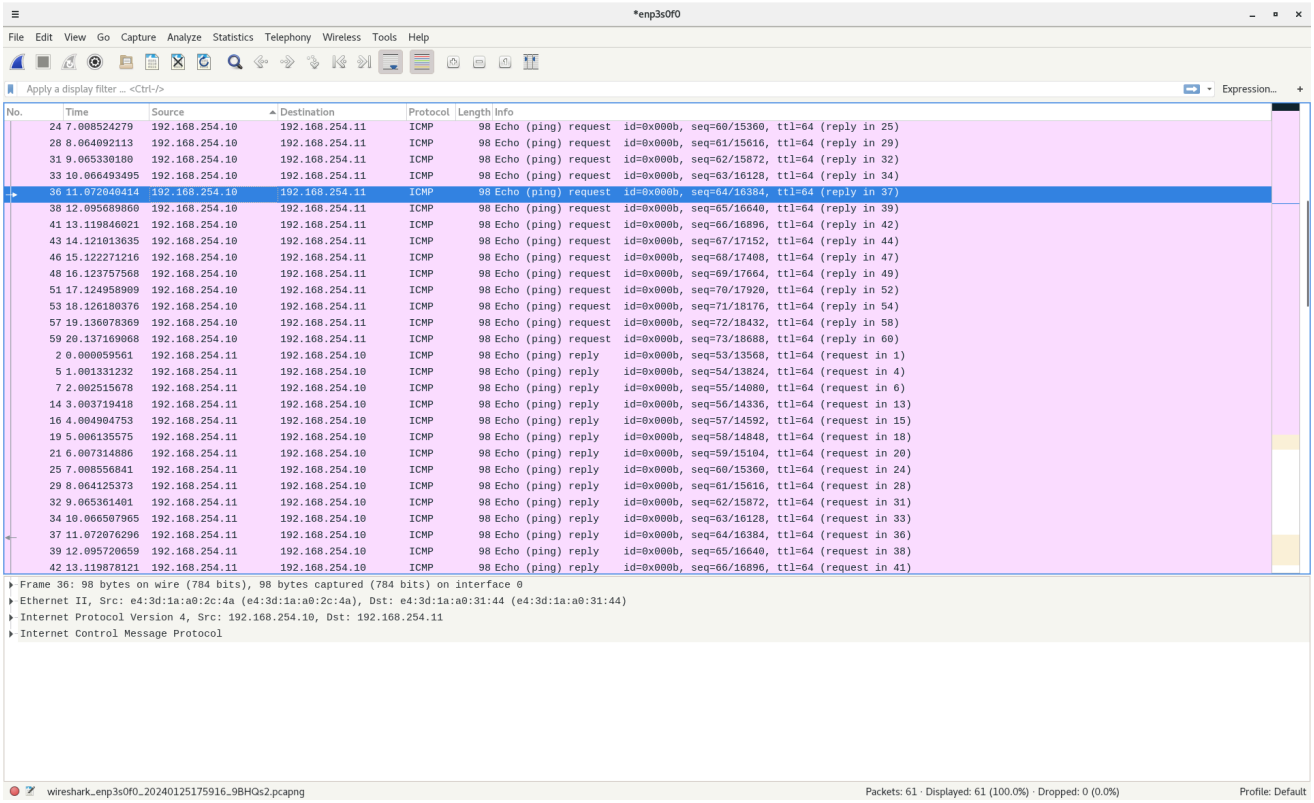
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.254.11	42316	151.101.128.114	443	25	7,861	11	1,958	14	5,903	4.134800	0.1217	128 k	388 k
192.168.254.11	56264	142.250.72.72	443	15	7,201	8	1,318	7	5,883	3.831787	0.1303	80 k	361 k
192.168.254.11	54874	142.250.72.14	443	17	9,390	9	1,384	8	8,006	4.198749	0.1209	91 k	529 k
192.168.254.11	55002	142.250.72.10	443	15	7,113	8	1,318	7	5,795	3.831746	0.1331	79 k	348 k
192.168.254.11	37578	142.250.72.10	443	15	7,113	8	1,318	7	5,795	3.984411	0.1244	84 k	372 k
192.168.254.11	56710	142.250.69.234	443	27	9,020	13	2,181	14	6,839	4.759422	0.1289	135 k	424 k
192.168.254.11	41582	142.250.69.232	443	16	7,268	9	1,384	7	5,884	3.831770	0.1404	78 k	335 k
192.168.254.11	37564	142.250.69.227	443	15	6,752	8	1,318	7	5,434	3.831715	0.1302	81 k	333 k
192.168.254.11	54248	142.250.69.227	443	15	6,753	8	1,318	7	5,435	3.984368	0.1244	84 k	349 k
192.168.254.11	48504	129.186.90.106	443	114	192 k	52	9,891	62	182 k	16.805107	0.5720	138 k	2,550 k
192.168.254.11	48514	129.186.90.106	443	188	377 k	81	13 k	107	364 k	16.914763	0.4229	251 k	6,889 k
192.168.254.11	48524	129.186.90.106	443	17	10 k	8	2,732	9	7,516	17.320107	0.0791	276 k	760 k
192.168.254.11	48532	129.186.90.106	443	19	14 k	9	2,795	10	11 k	17.320277	0.0789	283 k	1,151 k
192.168.254.11	48534	129.186.90.106	443	21	21 k	10	2,720	11	19 k	17.320310	0.0819	265 k	1,875 k
192.168.254.11	48544	129.186.90.106	443	22	19 k	10	2,727	12	17 k	17.320339	0.0408	534 k	3,383 k
192.168.254.11	48548	129.186.90.106	443	399	1,082 k	181	15 k	218	1,066 k	17.320406	0.2177	567 k	39 M
192.168.254.11	48554	129.186.90.106	443	740	2,095 k	340	25 k	400	2,069 k	17.325620	0.2105	984 k	78 M
192.168.254.11	48560	129.186.90.106	443	398	1,202 k	179	14 k	219	1,188 k	17.468771	0.0389	2,882 k	244 M
192.168.254.11	56754	108.157.150.32	443	46	55 k	23	2,704	23	52 k	4.134750	7.4286	2,912	56 k
192.168.254.11	35846	104.18.38.233	80	11	3,608	6	1,239	5	2,369	16.928986	0.4324	22 k	43 k
192.168.254.11	33276	104.16.122.175	443	31	7,518	15	2,261	16	5,257	3.987587	7.2699	2,488	5,784
192.168.254.11	51240	54.172.223.177	443	25	12 k	15	3,565	10	9,106	4.432095	14.9257	1,910	4,880
192.168.254.11	52818	54.172.198.166	443	71	22 k	35	8,212	36	14 k	4.144369	13.4367	4,889	8,754
192.168.254.11	52832	54.172.198.166	443	19	8,053	10	1,526	9	6,527	8.455724	0.1755	69 k	297 k
192.168.254.11	40164	52.162.92.72	443	18	7,445	10	1,342	8	6,103	3.831694	5.1193	2,097	9,537
192.168.254.11	52130	52.162.92.72	443	16	9,651	8	2,603	8	7,048	17.319268	0.1519	137 k	371 k

Name resolution | Limit to display filter | Absolute start time | Conversation Types

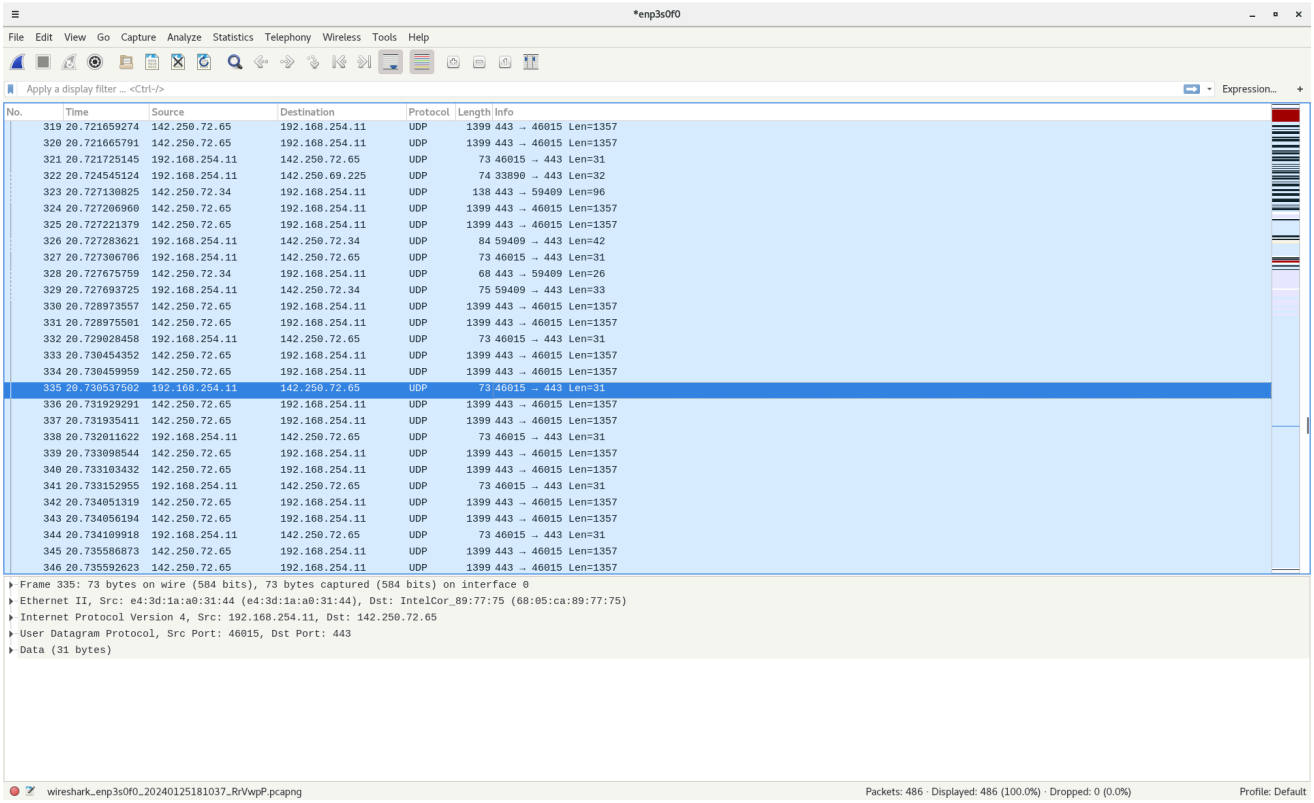
Help | Copy | Follow Stream... | Graph... | Close

12. This is to show the different TCP conversaions I am having. The IP is different between TCP and UDP for www.iastate.edu. I can tell 129.186.90.106 is iastate.edu because it was the most high traffic conversation.

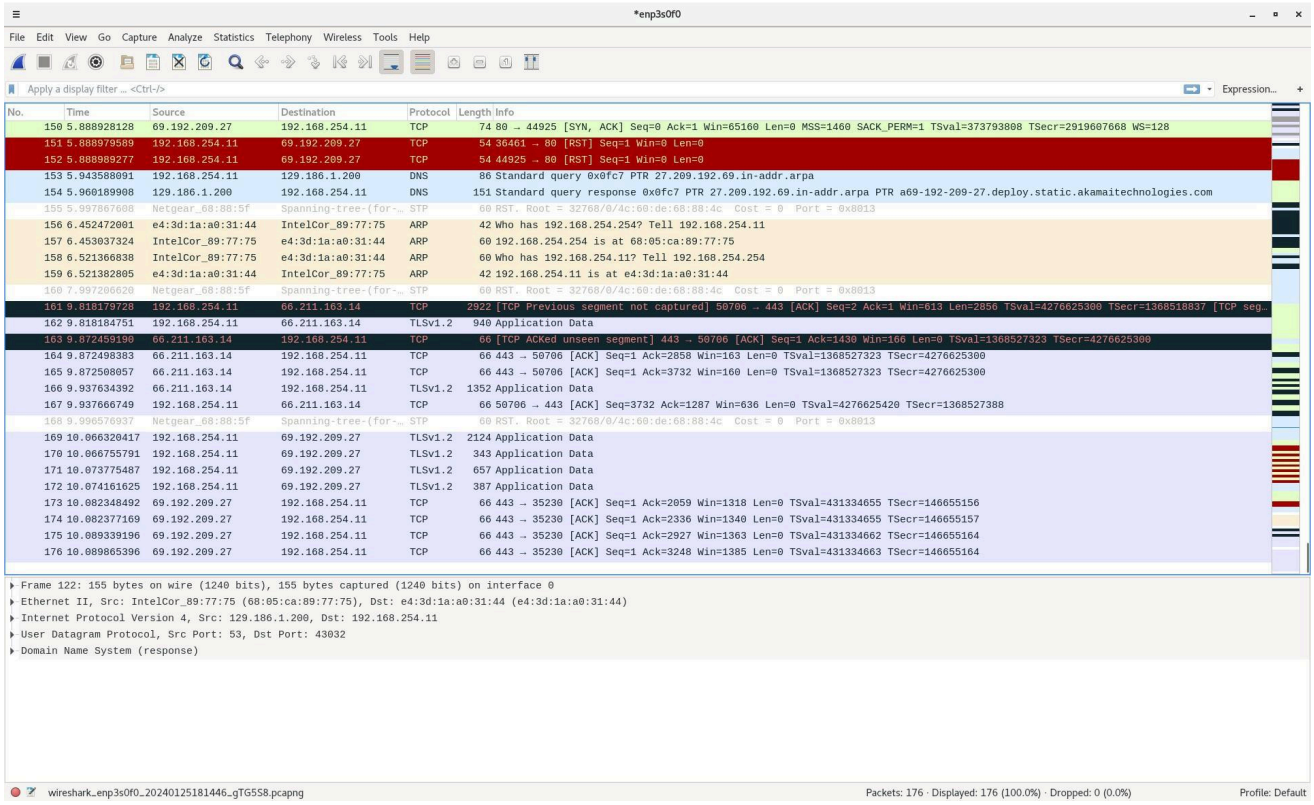
5 others:
-142.250.69.227, port 443, HTTPS, 8 packets sent 0.1244 Duration
-142.250.69.232, port 443, HTTPS, 9 packets sent 0.1404 Duration
-108.157.150.32, port 443, HTTPS, 23 packets sent, 7.4286 Duration
-54.172.223.177, port 443, HTTPS, 15 packets sent, 14.9257 Duration, used nslookup this was AWS
-52.162.92.72, port 443, HTTPS, 7 packets sent, 0.1315 Duration



13. 192.168.254.11 is me (I changed computers for this part), and 192.168.254.10 is the partner. 98 bytes are sent when the partner requests and I send 98 bytes back to him. The arrival time ranges from 1 to 59.



14. This is a capture of wireshark after running traceroute to www.ebay.com. All the packets we are sending and receiving are UDP.



This is after running tcptraceroute. We can see we are transmitting and receiving TCP packets.

Conclusion:

In this lab I learned about many different networking tools. I also learned about many different networking terms. Some of the tools I learned about were: nslookup, nmap, traceroute, ifconfig, ping, tcpdump, iperf, and wireshark. Some of the terms I learned about were TCP and UDP.

We used nslookup in order to find the ip address of domain names and find domain names for ips. We used nmap in order to see what ports we had open. Traceroute was used to see the path that a UDP took to get to a target ip. We also used the tcp version of it called tcptraceroute that allowed us to get past UDP firewalls. We used ifconfig to find our ip address. Ping was a command we could use with an ip to see if we could connect to them by sending packets and receiving packets back. We used tcpdump as a network sniffer to track the packets we were receiving. Using this I was able to get the ip of a friend who was pinging me. We also used iperf to check the bandwidth between two ips. The last tool we used was wireshark. This was another network sniffer. It was a GUI though and had many filters and tools built into it. We were able to organize by tcp and UDP packets. We could also sort by certain ip addresses. TCP and UDP are different network packet protocols. TCP packets are sent through a connection. UDP are just individual packets sent.