Lab 1: Network Utility Programs

Mason Walls

CPRE 489

Spring 2021

What I Learned:

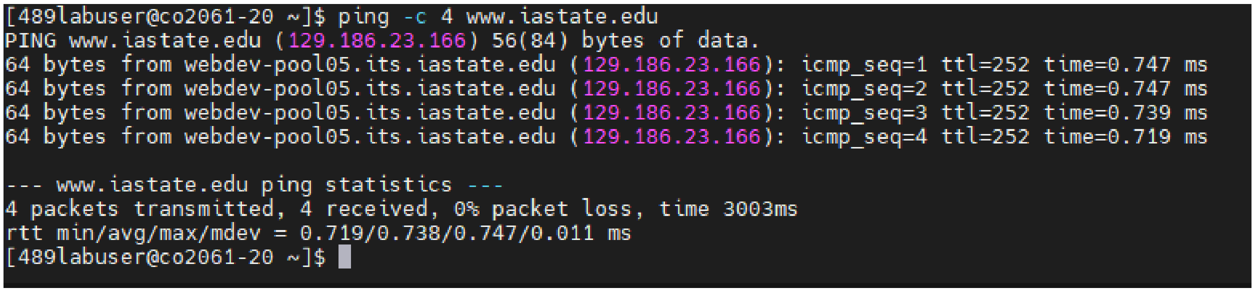
Before this class, I took CPRE 430, which also went into depth about these specific network utility programs. Surprisingly, I still learned a good deal about more options and information about these utilities.

Starting with ping, I learned about the default loopback address, which helps with checking network setup. In this lab, we used nslookup differently than I have before, showing me how to change its search parameters to find different information such as the mail exchanger. I also learned about iperf, helping me test bandwidth between two hosts. This is useful to test hardware for problems. We used traceroute a lot in CPRE 430, but we never were told about tcptraceroute. The ability to penetrate basic firewalls has shown its usefulness, as many gateways will block standard ICMP ping requests. This is the first time I have also used tcpdump and tcptrace to analyze packets sent to and from machines, as I had only used Wireshark before this lab. This lab also taught me some more linux operators that I have not used before to help with running things in background, writing to files etc.

Overall, I believe that this lab, whether all the information was new to me or not, was very informative. I was able to get a refresher on familiar commands, while also learning about their extra functionality. I also was able to learn about new commands that are helpful for network diagnosing.

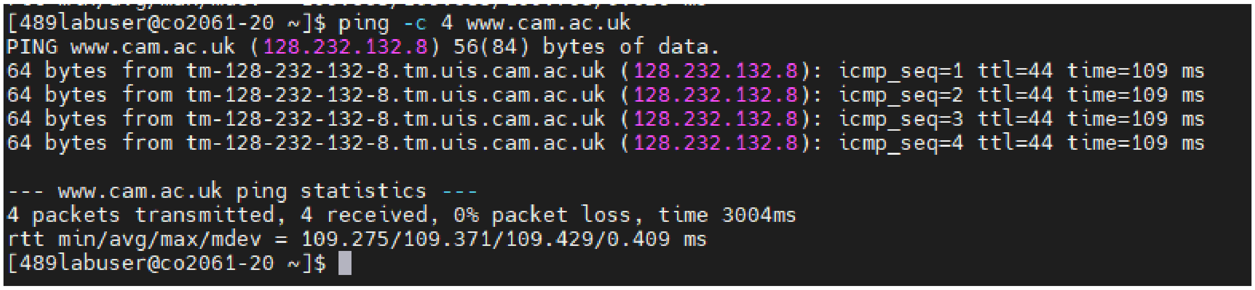
Note: If the way I formatted this lab report isn’t what is to be expected, I would love a comment that explains better how you would like reports to be created. There wasn’t a ton of information about how to write these up, thanks.

Exercise 1:



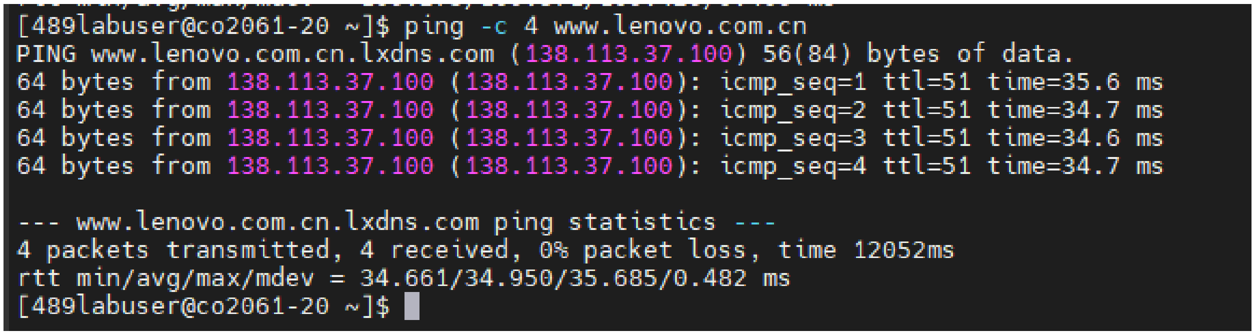
```
[489labuser@co2061-20 ~]$ ping -c 4 www.iastate.edu
PING www.iastate.edu (129.186.23.166) 56(84) bytes of data.
64 bytes from webdev-pool05.its.iastate.edu (129.186.23.166): icmp_seq=1 ttl=252 time=0.747 ms
64 bytes from webdev-pool05.its.iastate.edu (129.186.23.166): icmp_seq=2 ttl=252 time=0.747 ms
64 bytes from webdev-pool05.its.iastate.edu (129.186.23.166): icmp_seq=3 ttl=252 time=0.739 ms
64 bytes from webdev-pool05.its.iastate.edu (129.186.23.166): icmp_seq=4 ttl=252 time=0.719 ms

--- www.iastate.edu ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.719/0.738/0.747/0.011 ms
[489labuser@co2061-20 ~]$ 
```

Average: .738



```
[489labuser@co2061-20 ~]$ ping -c 4 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=44 time=109 ms
64 bytes from tm-128-232-132-8.tm.uis.cam.ac.uk (128.232.132.8): icmp_seq=2 ttl=44 time=109 ms
64 bytes from tm-128-232-132-8.tm.uis.cam.ac.uk (128.232.132.8): icmp_seq=3 ttl=44 time=109 ms
64 bytes from tm-128-232-132-8.tm.uis.cam.ac.uk (128.232.132.8): icmp_seq=4 ttl=44 time=109 ms

--- www.cam.ac.uk ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 109.275/109.371/109.429/0.409 ms
[489labuser@co2061-20 ~]$
```

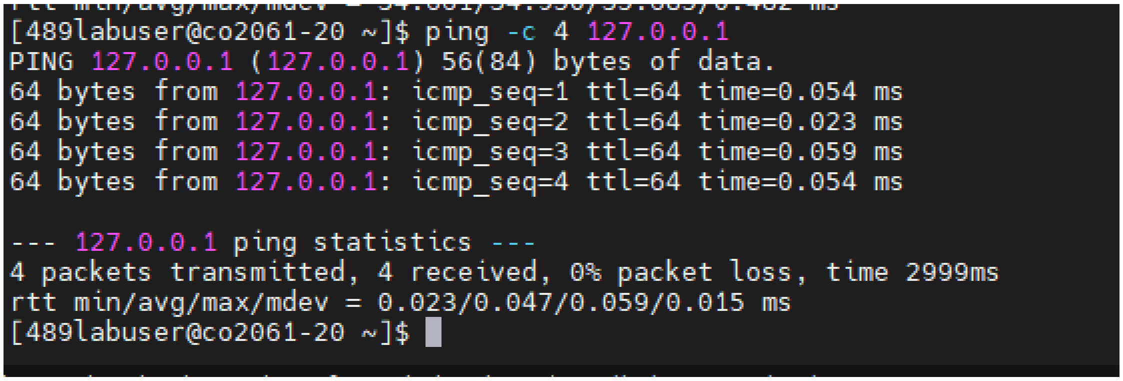
Average: 109.371



```
[489labuser@co2061-20 ~]$ ping -c 4 www.lenovo.com.cn
PING www.lenovo.com.cn.lxdns.com (138.113.37.100) 56(84) bytes of data.
64 bytes from 138.113.37.100 (138.113.37.100): icmp_seq=1 ttl=51 time=35.6 ms
64 bytes from 138.113.37.100 (138.113.37.100): icmp_seq=2 ttl=51 time=34.7 ms
64 bytes from 138.113.37.100 (138.113.37.100): icmp_seq=3 ttl=51 time=34.6 ms
64 bytes from 138.113.37.100 (138.113.37.100): icmp_seq=4 ttl=51 time=34.7 ms

--- www.lenovo.com.cn.lxdns.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 12052ms
rtt min/avg/max/mdev = 34.661/34.950/35.685/0.482 ms
[489labuser@co2061-20 ~]$
```

Average: 34.950

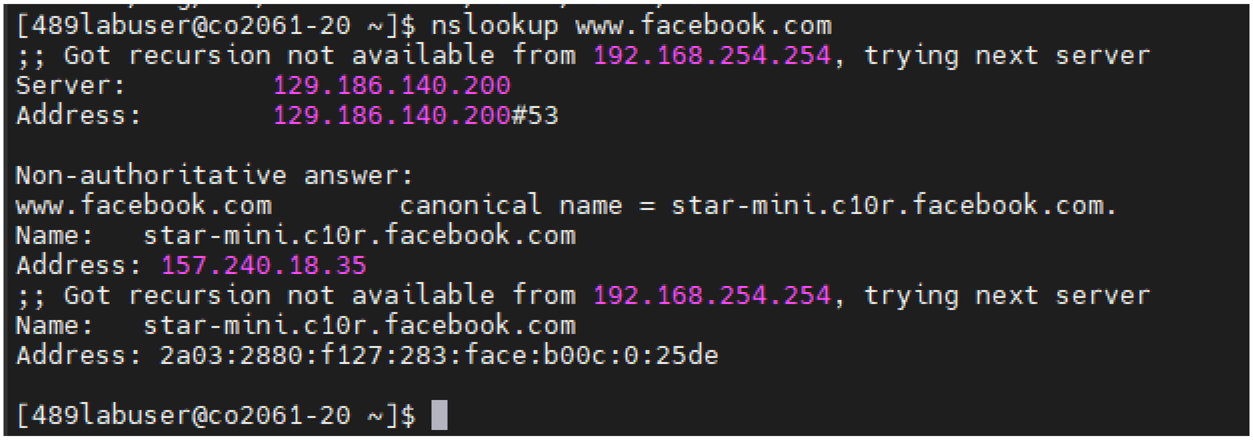
Exercise 2:



```
[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=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.023 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.059 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.054 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.023/0.047/0.059/0.015 ms
[489labuser@co2061-20 ~]$
```

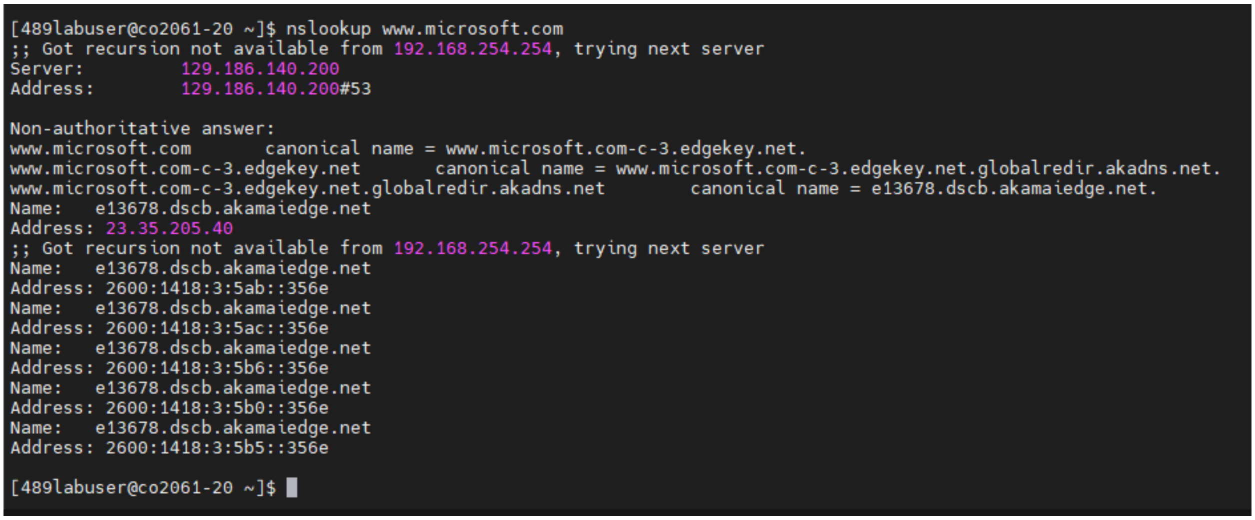
This command pings the default loop-back address, which verifies that the network stack of an Operating System is working properly. This shows that my ping packets are being processed correctly by the OS.

Exercise 3:



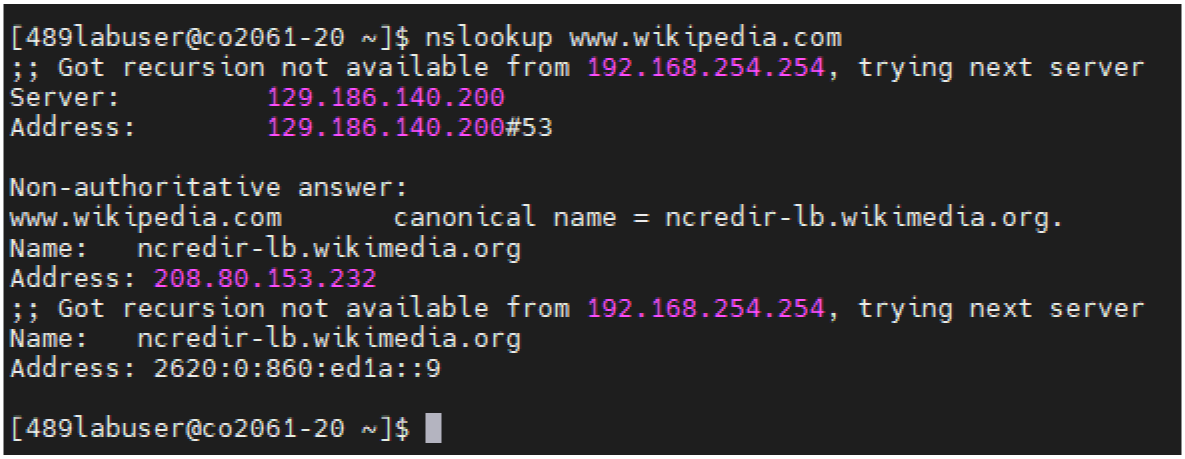
```
[489labuser@co2061-20 ~]$ nslookup www.facebook.com
;; Got recursion not available from 192.168.254.254, trying next server
Server:         129.186.140.200
Address:        129.186.140.200#53

Non-authoritative answer:
www.facebook.com        canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 157.240.18.35
;; Got recursion not available from 192.168.254.254, trying next server
Name:   star-mini.c10r.facebook.com
Address: 2a03:2880:f127:283:face:b00c:0:25de

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

IP: 157.240.18.35   canonical name: star-mini-c10r.facebook.com



```
[489labuser@co2061-20 ~]$ nslookup www.microsoft.com
;; Got recursion not available from 192.168.254.254, trying next server
Server:         129.186.140.200
Address:        129.186.140.200#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.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: 23.35.205.40
;; Got recursion not available from 192.168.254.254, trying next server
Name:   e13678.dscb.akamaiedge.net
Address: 2600:1418:3:5ab::356e
Name:   e13678.dscb.akamaiedge.net
Address: 2600:1418:3:5ac::356e
Name:   e13678.dscb.akamaiedge.net
Address: 2600:1418:3:5b6::356e
Name:   e13678.dscb.akamaiedge.net
Address: 2600:1418:3:5b0::356e
Name:   e13678.dscb.akamaiedge.net
Address: 2600:1418:3:5b5::356e

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

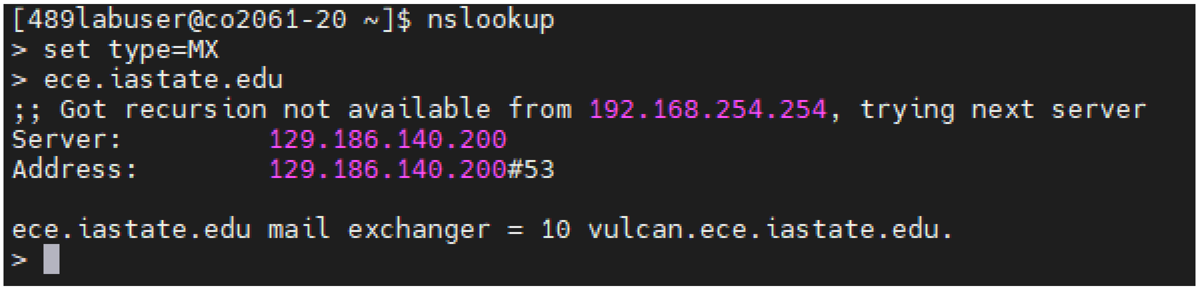
IP: 23.35.205.40   canonical name: www.microsoft.com-c-3.edgekey.net



```
[489labuser@co2061-20 ~]$ nslookup www.wikipedia.com
;; Got recursion not available from 192.168.254.254, trying next server
Server:         129.186.140.200
Address:        129.186.140.200#53

Non-authoritative answer:
www.wikipedia.com       canonical name = ncredir-lb.wikimedia.org.
Name:   ncredir-lb.wikimedia.org
Address: 208.80.153.232
;; Got recursion not available from 192.168.254.254, trying next server
Name:   ncredir-lb.wikimedia.org
Address: 2620:0:860:ed1a::9

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

IP: 208.80.153.232   canonical name: ncredir-lb.wikimedia.org

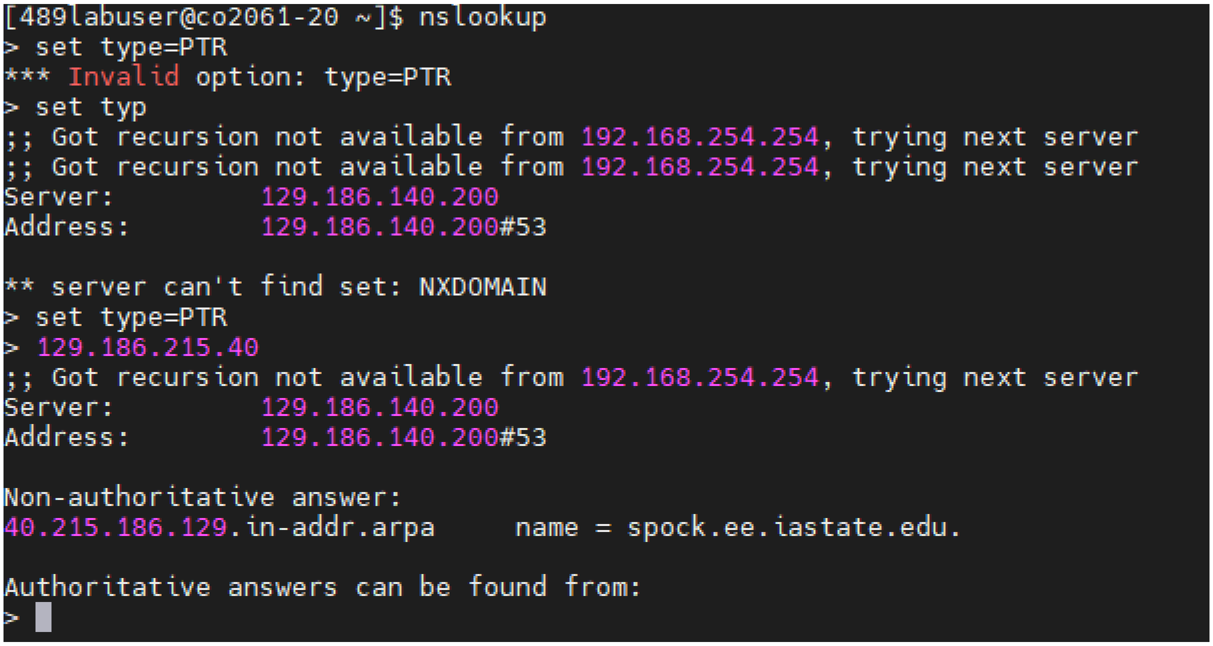
Exercise 4:



```
[489labuser@co2061-20 ~]$ nslookup
> set type=MX
> ece.iastate.edu
;; Got recursion not available from 192.168.254.254, trying next server
Server:         129.186.140.200
Address:        129.186.140.200#53

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

Mail exchanger: 10 vulcan.ece.iastate.edu

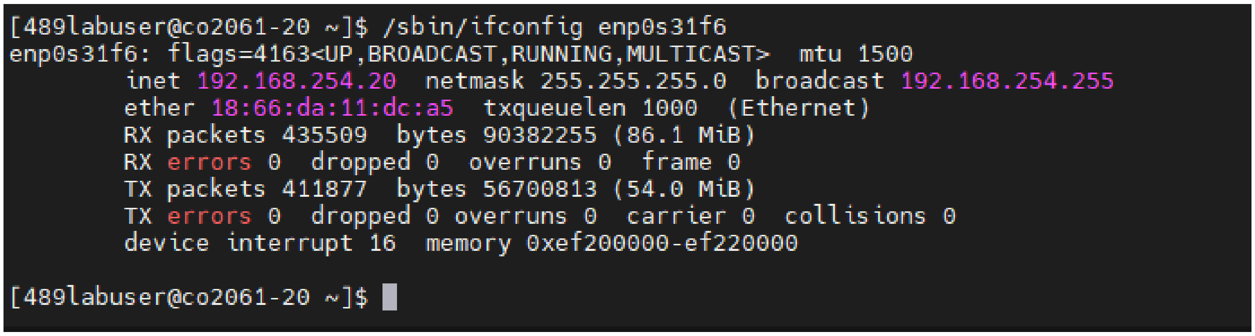
Exercise 5:



```
[489labuser@co2061-20 ~]$ nslookup
> set type=PTR
*** Invalid option: type=PTR
> set typ
;; Got recursion not available from 192.168.254.254, trying next server
;; Got recursion not available from 192.168.254.254, trying next server
Server:         129.186.140.200
Address:        129.186.140.200#53

** server can't find set: NXDOMAIN
> set type=PTR
> 129.186.215.40
;; Got recursion not available from 192.168.254.254, trying next server
Server:         129.186.140.200
Address:        129.186.140.200#53

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

Authoritative answers can be found from:
> 
```

Name: spock.ee.iastate.edu

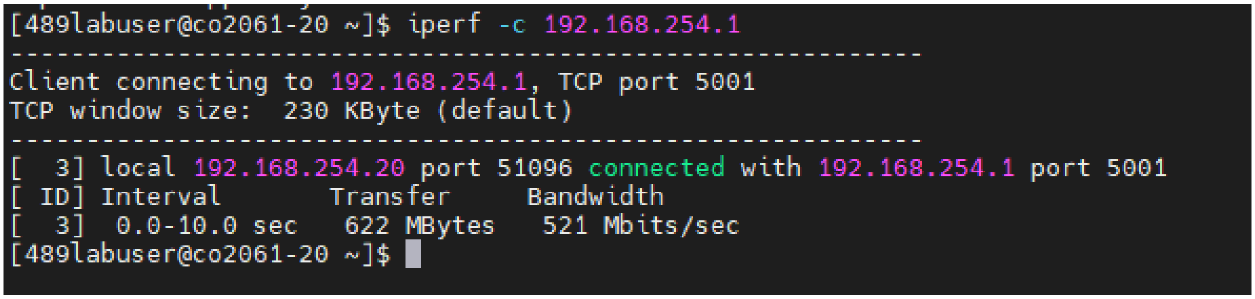
Exercise 6:



```
[489labuser@co2061-20 ~]$ /sbin/ifconfig enp0s31f6
enp0s31f6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.254.20  netmask 255.255.255.0  broadcast 192.168.254.255
        ether 18:66:da:11:dc:a5  txqueuelen 1000  (Ethernet)
        RX packets 435509  bytes 90382255 (86.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 411877  bytes 56700813 (54.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  memory 0xef200000-ef220000

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

IP: 192.168.254.20

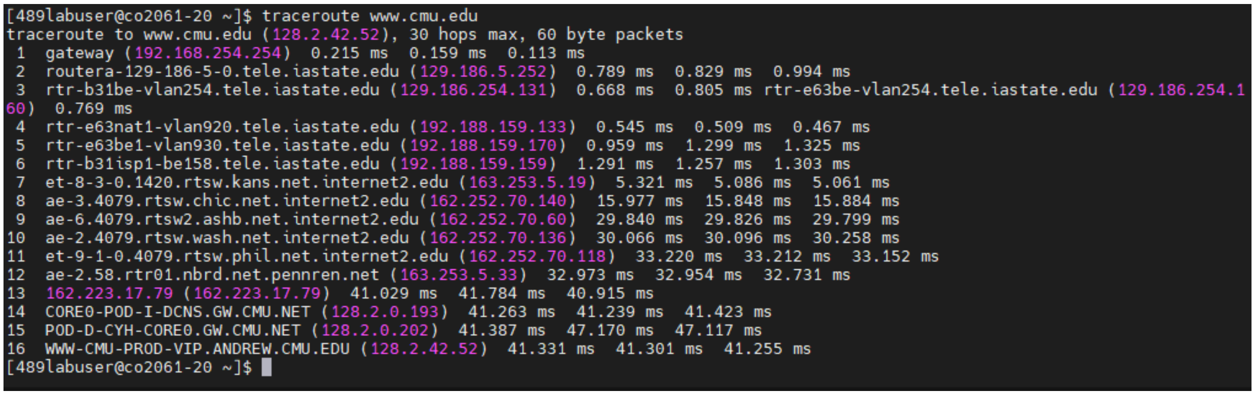
Exercise 7:



```
[489labuser@co2061-20 ~]$ iperf -c 192.168.254.1
------------------------------------------------------------
Client connecting to 192.168.254.1, TCP port 5001
TCP window size:  230 KByte (default)
------------------------------------------------------------
[  3] local 192.168.254.20 port 51096 connected with 192.168.254.1 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec   622 MBytes   521 Mbits/sec
[489labuser@co2061-20 ~]$ 
```

This connection is most likely 1 Gbps. My apartment has 1Gbps, and so does ISU's network. This speed is probably lower due to VPN routing etc.

Exercise 8:



```
[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)  0.215 ms  0.159 ms  0.113 ms
 2  routera-129-186-5-0.tele.iastate.edu (129.186.5.252)  0.789 ms  0.829 ms  0.994 ms
 3  rtr-b31be-vlan254.tele.iastate.edu (129.186.254.131)  0.668 ms  0.805 ms rtr-e63be-vlan254.tele.iastate.edu (129.186.254.1
60)  0.769 ms
 4  rtr-e63nat1-vlan920.tele.iastate.edu (192.188.159.133)  0.545 ms  0.509 ms  0.467 ms
 5  rtr-e63be1-vlan930.tele.iastate.edu (192.188.159.170)  0.959 ms  1.299 ms  1.325 ms
 6  rtr-b31isp1-be158.tele.iastate.edu (192.188.159.159)  1.291 ms  1.257 ms  1.303 ms
 7  et-8-3-0.1420.rtsw.kans.net.internet2.edu (163.253.5.19)  5.321 ms  5.086 ms  5.061 ms
 8  ae-3.4079.rtsw.chic.net.internet2.edu (162.252.70.140)  15.977 ms  15.848 ms  15.884 ms
 9  ae-6.4079.rtsw2.ashb.net.internet2.edu (162.252.70.60)  29.840 ms  29.826 ms  29.799 ms
10  ae-2.4079.rtsw.wash.net.internet2.edu (162.252.70.136)  30.066 ms  30.096 ms  30.258 ms
11  et-9-1-0.4079.rtsw.phil.net.internet2.edu (162.252.70.118)  33.220 ms  33.212 ms  33.152 ms
12  ae-2.58.rtr01.nbrd.net.pennren.net (163.253.5.33)  32.973 ms  32.954 ms  32.731 ms
13  162.223.17.79 (162.223.17.79)  41.029 ms  41.784 ms  40.915 ms
14  CORE0-POD-I-DCNS.GW.CMU.NET (128.2.0.193)  41.263 ms  41.239 ms  41.423 ms
15  POD-D-CYH-CORE0.GW.CMU.NET (128.2.0.202)  41.387 ms  47.170 ms  47.117 ms
16  WWW-CMU-PROD-VIP.ANDREW.CMU.EDU (128.2.42.52)  41.331 ms  41.301 ms  41.255 ms
[489labuser@co2061-20 ~]$ 
```

Number of hops: 16

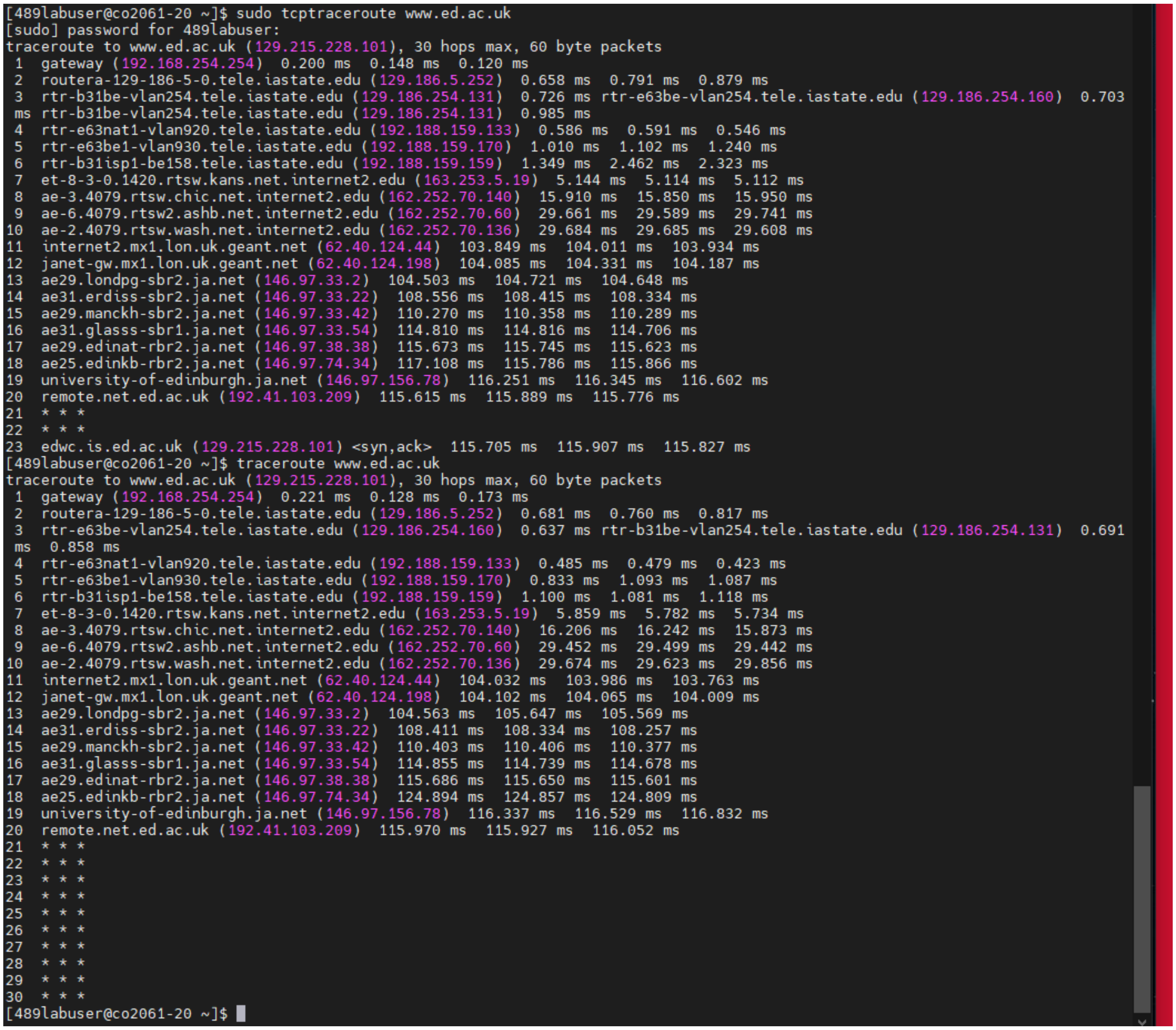
Routes: The packets make their way through ISU's network in 6 hops, then are routed through the web with routing tables to eventually reach CMU's network. Once it is in CMU's network, the routing tables find the correct path to www.cmu.edu

Gateways: The gateways on this route go from ISU's network, to the world wide web, to CMU's network.

Latency: The round trip times for these packets were 41.331ms, 41.301 ms, and 41.255 ms. This creates an average round trip time of 41.296 ms, making this server have quite low latency.

Reachability: This host is very reachable as it did not block any of the ICMP packets that were sent. Some hosts will block these packets, making it hard to reach a site to get any network information.

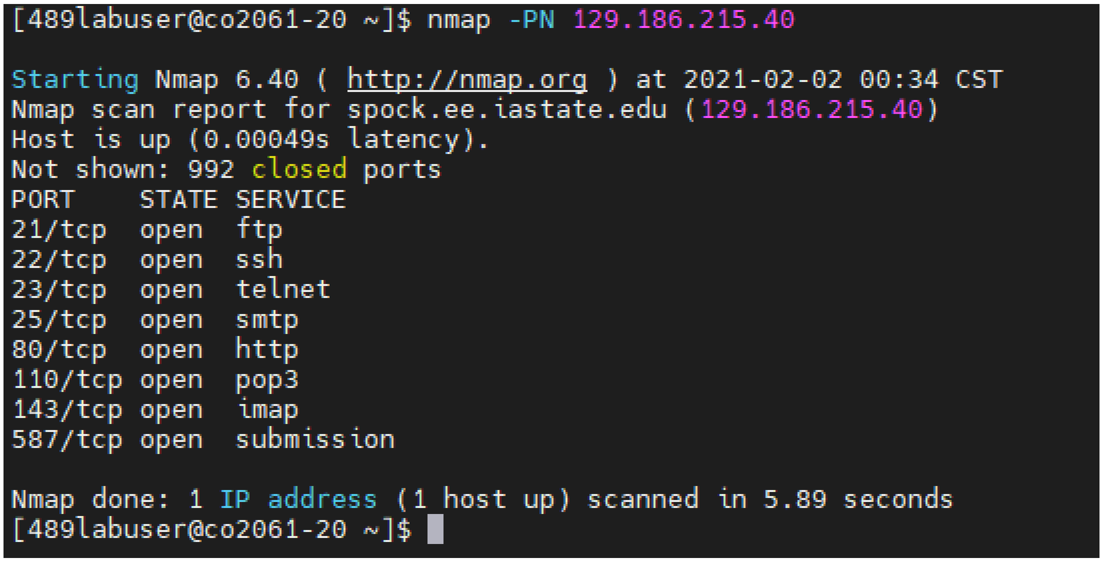
Exercise 9:



```
[489labuser@co2061-20 ~]$ sudo tcptraceroute www.ed.ac.uk
[sudo] password for 489labuser:
traceroute to www.ed.ac.uk (129.215.228.101), 30 hops max, 60 byte packets
 1  gateway (192.168.254.254)  0.200 ms  0.148 ms  0.120 ms
 2  routera-129-186-5-0.tele.iastate.edu (129.186.5.252)  0.658 ms  0.791 ms  0.879 ms
 3  rtr-b31be-vlan254.tele.iastate.edu (129.186.254.131)  0.726 ms rtr-e63be-vlan254.tele.iastate.edu (129.186.254.160)  0.703
 ms rtr-b31be-vlan254.tele.iastate.edu (129.186.254.131)  0.985 ms
 4  rtr-e63nat1-vlan920.tele.iastate.edu (192.188.159.133)  0.586 ms  0.591 ms  0.546 ms
 5  rtr-e63be1-vlan930.tele.iastate.edu (192.188.159.170)  1.010 ms  1.102 ms  1.240 ms
 6  rtr-b31isp1-be158.tele.iastate.edu (192.188.159.159)  1.349 ms  2.462 ms  2.323 ms
 7  et-8-3-0.1420.rtsw.kans.net.internet2.edu (163.253.5.19)  5.144 ms  5.114 ms  5.112 ms
 8  ae-3.4079.rtsw.chic.net.internet2.edu (162.252.70.140)  15.910 ms  15.850 ms  15.950 ms
 9  ae-6.4079.rtsw2.ashb.net.internet2.edu (162.252.70.60)  29.661 ms  29.589 ms  29.741 ms
10  ae-2.4079.rtsw.wash.net.internet2.edu (162.252.70.136)  29.684 ms  29.685 ms  29.608 ms
11  internet2.mx1.lon.uk.geant.net (62.40.124.44)  103.849 ms  104.011 ms  103.934 ms
12  janet-gw.mx1.lon.uk.geant.net (62.40.124.198)  104.085 ms  104.331 ms  104.187 ms
13  ae29.londpg-sbr2.ja.net (146.97.33.2)  104.503 ms  104.721 ms  104.648 ms
14  ae31.erdiss-sbr2.ja.net (146.97.33.22)  108.556 ms  108.415 ms  108.334 ms
15  ae29.manckh-sbr2.ja.net (146.97.33.42)  110.270 ms  110.358 ms  110.289 ms
16  ae31.glasss-sbr1.ja.net (146.97.33.54)  114.810 ms  114.816 ms  114.706 ms
17  ae29.edinat-rbr2.ja.net (146.97.38.38)  115.673 ms  115.745 ms  115.623 ms
18  ae25.edinkb-rbr2.ja.net (146.97.74.34)  117.108 ms  115.786 ms  115.866 ms
19  university-of-edinburgh.ja.net (146.97.156.78)  116.251 ms  116.345 ms  116.602 ms
20  remote.net.ed.ac.uk (192.41.103.209)  115.615 ms  115.889 ms  115.776 ms
21  * * *
22  * * *
23  edwc.is.ed.ac.uk (129.215.228.101) <syn,ack>  115.705 ms  115.907 ms  115.827 ms
[489labuser@co2061-20 ~]$ traceroute www.ed.ac.uk
traceroute to www.ed.ac.uk (129.215.228.101), 30 hops max, 60 byte packets
 1  gateway (192.168.254.254)  0.221 ms  0.128 ms  0.173 ms
 2  routera-129-186-5-0.tele.iastate.edu (129.186.5.252)  0.681 ms  0.760 ms  0.817 ms
 3  rtr-e63be-vlan254.tele.iastate.edu (129.186.254.160)  0.637 ms rtr-b31be-vlan254.tele.iastate.edu (129.186.254.131)  0.691
 ms  0.858 ms
 4  rtr-e63nat1-vlan920.tele.iastate.edu (192.188.159.133)  0.485 ms  0.479 ms  0.423 ms
 5  rtr-e63be1-vlan930.tele.iastate.edu (192.188.159.170)  0.833 ms  1.093 ms  1.087 ms
 6  rtr-b31isp1-be158.tele.iastate.edu (192.188.159.159)  1.100 ms  1.081 ms  1.118 ms
 7  et-8-3-0.1420.rtsw.kans.net.internet2.edu (163.253.5.19)  5.859 ms  5.782 ms  5.734 ms
 8  ae-3.4079.rtsw.chic.net.internet2.edu (162.252.70.140)  16.206 ms  16.242 ms  15.873 ms
 9  ae-6.4079.rtsw2.ashb.net.internet2.edu (162.252.70.60)  29.452 ms  29.499 ms  29.442 ms
10  ae-2.4079.rtsw.wash.net.internet2.edu (162.252.70.136)  29.674 ms  29.623 ms  29.856 ms
11  internet2.mx1.lon.uk.geant.net (62.40.124.44)  104.032 ms  103.986 ms  103.763 ms
12  janet-gw.mx1.lon.uk.geant.net (62.40.124.198)  104.102 ms  104.065 ms  104.009 ms
13  ae29.londpg-sbr2.ja.net (146.97.33.2)  104.563 ms  105.647 ms  105.569 ms
14  ae31.erdiss-sbr2.ja.net (146.97.33.22)  108.411 ms  108.334 ms  108.257 ms
15  ae29.manckh-sbr2.ja.net (146.97.33.42)  110.403 ms  110.406 ms  110.377 ms
16  ae31.glasss-sbr1.ja.net (146.97.33.54)  114.855 ms  114.739 ms  114.678 ms
17  ae29.edinat-rbr2.ja.net (146.97.38.38)  115.686 ms  115.650 ms  115.601 ms
18  ae25.edinkb-rbr2.ja.net (146.97.74.34)  124.894 ms  124.857 ms  124.809 ms
19  university-of-edinburgh.ja.net (146.97.156.78)  116.337 ms  116.529 ms  116.832 ms
20  remote.net.ed.ac.uk (192.41.103.209)  115.970 ms  115.927 ms  116.052 ms
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
[489labuser@co2061-20 ~]$ 
```

The tcptraceroute shows more hop information. This is the case because the gateways closer to the destination have a firewall in place that blocks the ICMP packets. The TCP SYN/ACK packets are able to penetrate more of the firewalls, resulting in more information being given to us.

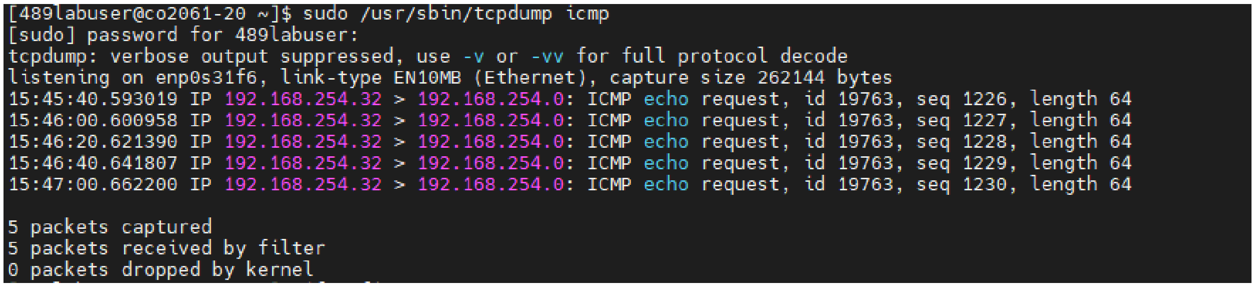
Exercise 10:



```
[489labuser@co2061-20 ~]$ nmap -PN 129.186.215.40

Starting Nmap 6.40 ( http://nmap.org ) at 2021-02-02 00:34 CST
Nmap scan report for spock.ee.iastate.edu (129.186.215.40)
Host is up (0.00049s latency).
Not shown: 992 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
587/tcp open  submission

Nmap done: 1 IP address (1 host up) scanned in 5.89 seconds
[489labuser@co2061-20 ~]$ 
```

Port 22 is open for SSH.

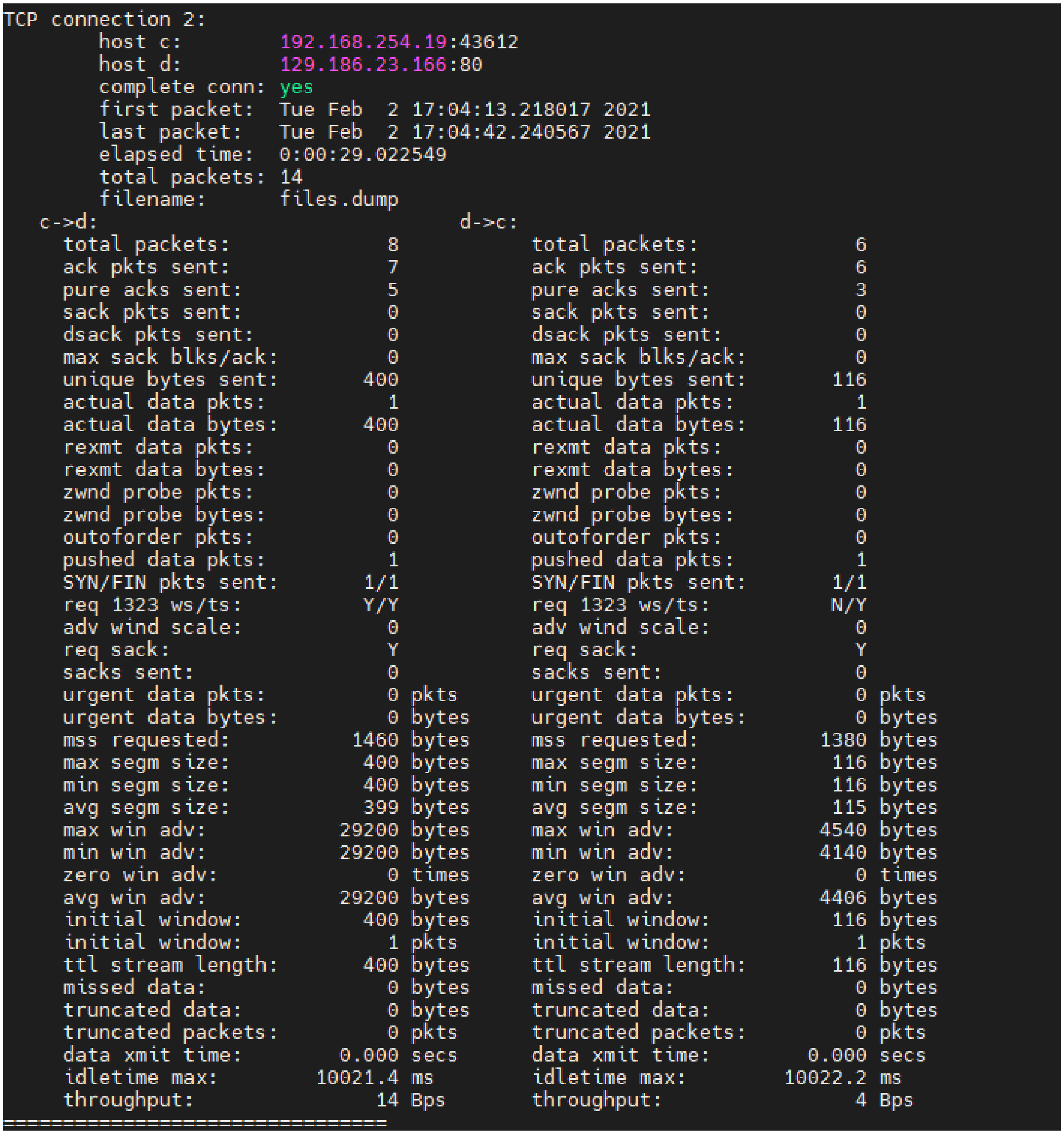
Exercise 11:



```
[489labuser@co2061-20 ~]$ sudo /usr/sbin/tcpdump icmp
[sudo] password for 489labuser:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s31f6, link-type EN10MB (Ethernet), capture size 262144 bytes
15:45:40.593019 IP 192.168.254.32 > 192.168.254.0: ICMP echo request, id 19763, seq 1226, length 64
15:46:00.600958 IP 192.168.254.32 > 192.168.254.0: ICMP echo request, id 19763, seq 1227, length 64
15:46:20.621390 IP 192.168.254.32 > 192.168.254.0: ICMP echo request, id 19763, seq 1228, length 64
15:46:40.641807 IP 192.168.254.32 > 192.168.254.0: ICMP echo request, id 19763, seq 1229, length 64
15:47:00.662200 IP 192.168.254.32 > 192.168.254.0: ICMP echo request, id 19763, seq 1230, length 64

5 packets captured
5 packets received by filter
0 packets dropped by kernel
```

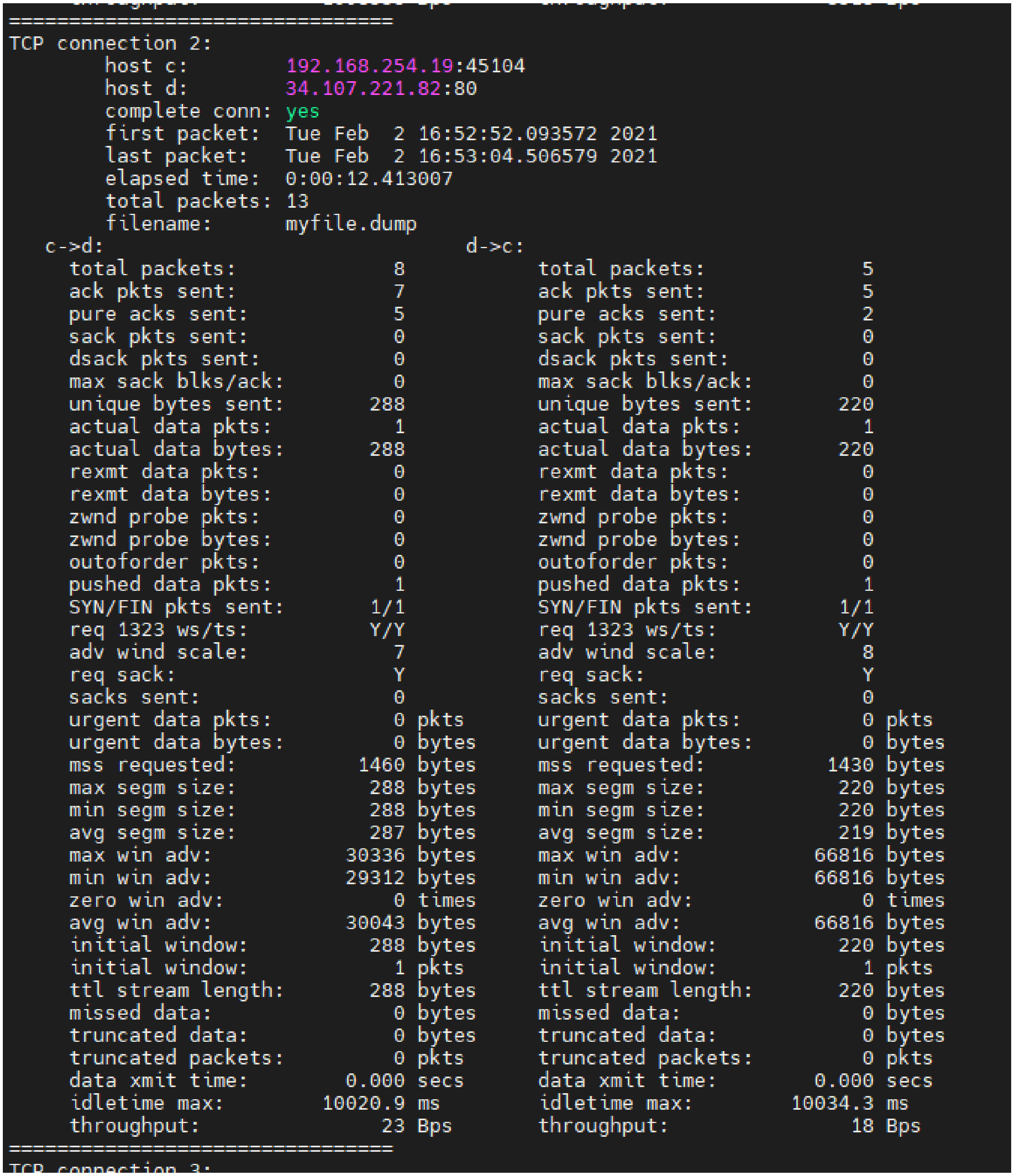
The IP of the attacking computer is 192.168.254.32

Exercise 12:



```
TCP connection 2:
        host c:        192.168.254.19:43612
        host d:        129.186.23.166:80
        complete conn: yes
        first packet:  Tue Feb  2 17:04:13.218017 2021
        last packet:   Tue Feb  2 17:04:42.240567 2021
        elapsed time:  0:00:29.022549
        total packets: 14
        filename:      files.dump
   c->d:                              d->c:
     total packets:            8           total packets:            6
     ack pkts sent:            7           ack pkts sent:            6
     pure acks sent:           5           pure acks sent:           3
     sack pkts sent:           0           sack pkts sent:           0
     dsack pkts sent:          0           dsack pkts sent:          0
     max sack blks/ack:        0           max sack blks/ack:        0
     unique bytes sent:      400           unique bytes sent:      116
     actual data pkts:         1           actual data pkts:         1
     actual data bytes:      400           actual data bytes:      116
     rexmt data pkts:          0           rexmt data pkts:          0
     rexmt data bytes:         0           rexmt data bytes:         0
     zwnd probe pkts:          0           zwnd probe pkts:          0
     zwnd probe bytes:         0           zwnd probe bytes:         0
     outoforder pkts:          0           outoforder pkts:          0
     pushed data pkts:         1           pushed data pkts:         1
     SYN/FIN pkts sent:      1/1           SYN/FIN pkts sent:      1/1
     req 1323 ws/ts:         Y/Y           req 1323 ws/ts:         N/Y
     adv wind scale:           0           adv wind scale:           0
     req sack:                 Y           req sack:                 Y
     sacks sent:               0           sacks sent:               0
     urgent data pkts:         0 pkts      urgent data pkts:         0 pkts
     urgent data bytes:        0 bytes     urgent data bytes:        0 bytes
     mss requested:         1460 bytes     mss requested:         1380 bytes
     max segm size:          400 bytes     max segm size:          116 bytes
     min segm size:          400 bytes     min segm size:          116 bytes
     avg segm size:          399 bytes     avg segm size:          115 bytes
     max win adv:          29200 bytes     max win adv:           4540 bytes
     min win adv:          29200 bytes     min win adv:           4140 bytes
     zero win adv:             0 times     zero win adv:             0 times
     avg win adv:          29200 bytes     avg win adv:           4406 bytes
     initial window:         400 bytes     initial window:         116 bytes
     initial window:           1 pkts      initial window:           1 pkts
     ttl stream length:      400 bytes     ttl stream length:      116 bytes
     missed data:              0 bytes     missed data:              0 bytes
     truncated data:           0 bytes     truncated data:           0 bytes
     truncated packets:        0 pkts      truncated packets:        0 pkts
     data xmit time:       0.000 secs      data xmit time:       0.000 secs
     idletime max:       10021.4 ms        idletime max:       10022.2 ms
     throughput:              14 Bps       throughput:               4 Bps
================================
```

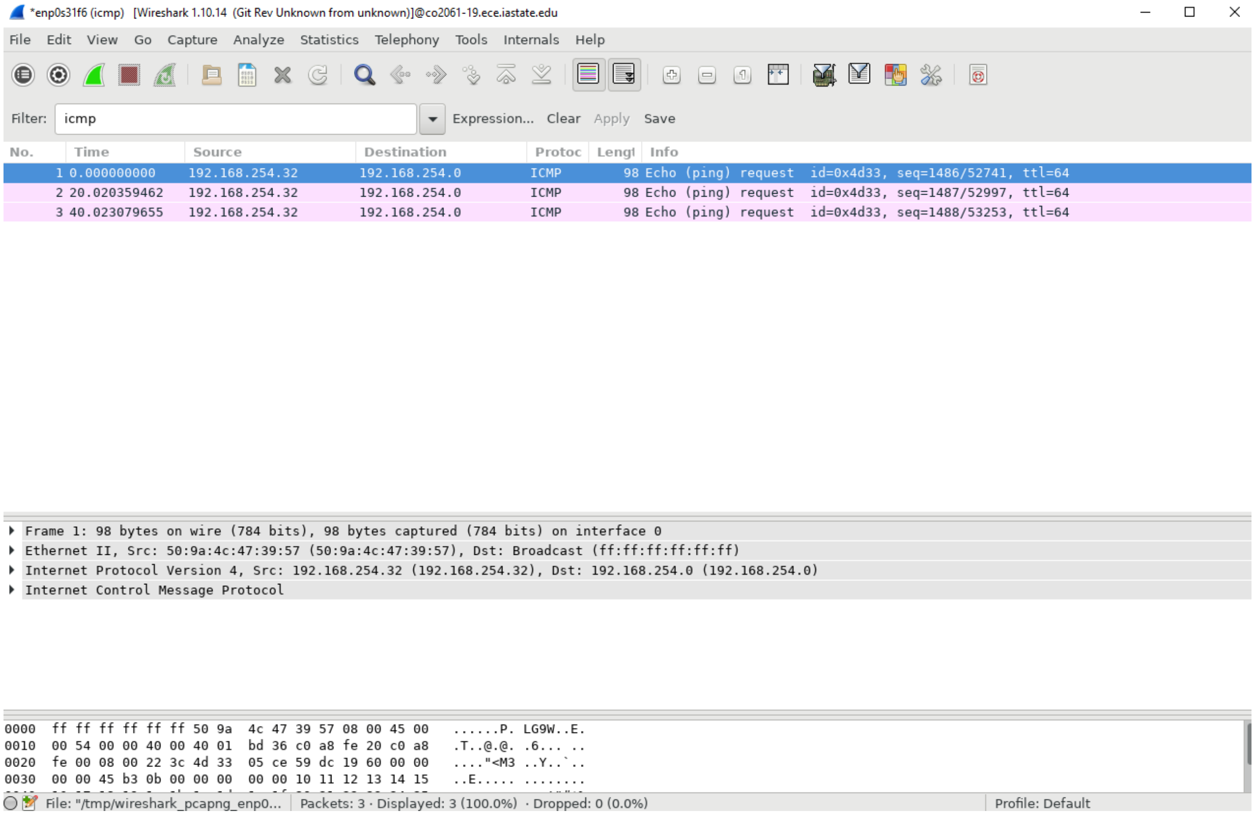
a. Source IP: 192.168.254.19 Destination IP: 129.186.23.166 Port: 80
b. Duration of connection: 29.022549 seconds
c. Packets sent: 14



```
================================
TCP connection 2:
        host c:        192.168.254.19:45104
        host d:        34.107.221.82:80
        complete conn: yes
        first packet:  Tue Feb  2 16:52:52.093572 2021
        last packet:   Tue Feb  2 16:53:04.506579 2021
        elapsed time:  0:00:12.413007
        total packets: 13
        filename:      myfile.dump
   c->d:                              d->c:
     total packets:            8           total packets:            5
     ack pkts sent:            7           ack pkts sent:            5
     pure acks sent:           5           pure acks sent:           2
     sack pkts sent:           0           sack pkts sent:           0
     dsack pkts sent:          0           dsack pkts sent:          0
     max sack blks/ack:        0           max sack blks/ack:        0
     unique bytes sent:      288           unique bytes sent:      220
     actual data pkts:         1           actual data pkts:         1
     actual data bytes:      288           actual data bytes:      220
     rexmt data pkts:          0           rexmt data pkts:          0
     rexmt data bytes:         0           rexmt data bytes:         0
     zwnd probe pkts:          0           zwnd probe pkts:          0
     zwnd probe bytes:         0           zwnd probe bytes:         0
     outoforder pkts:          0           outoforder pkts:          0
     pushed data pkts:         1           pushed data pkts:         1
     SYN/FIN pkts sent:      1/1           SYN/FIN pkts sent:      1/1
     req 1323 ws/ts:         Y/Y           req 1323 ws/ts:         Y/Y
     adv wind scale:           7           adv wind scale:           8
     req sack:                 Y           req sack:                 Y
     sacks sent:               0           sacks sent:               0
     urgent data pkts:         0 pkts      urgent data pkts:         0 pkts
     urgent data bytes:        0 bytes     urgent data bytes:        0 bytes
     mss requested:         1460 bytes     mss requested:         1430 bytes
     max segm size:          288 bytes     max segm size:          220 bytes
     min segm size:          288 bytes     min segm size:          220 bytes
     avg segm size:          287 bytes     avg segm size:          219 bytes
     max win adv:          30336 bytes     max win adv:          66816 bytes
     min win adv:          29312 bytes     min win adv:          66816 bytes
     zero win adv:             0 times     zero win adv:             0 times
     avg win adv:          30043 bytes     avg win adv:          66816 bytes
     initial window:         288 bytes     initial window:         220 bytes
     initial window:           1 pkts      initial window:           1 pkts
     ttl stream length:      288 bytes     ttl stream length:      220 bytes
     missed data:              0 bytes     missed data:              0 bytes
     truncated data:           0 bytes     truncated data:           0 bytes
     truncated packets:        0 pkts      truncated packets:        0 pkts
     data xmit time:       0.000 secs      data xmit time:       0.000 secs
     idletime max:       10020.9 ms        idletime max:       10034.3 ms
     throughput:              23 Bps       throughput:              18 Bps
================================
TCP connection 3:
```

a. Source IP: 192.168.3254.19 Destination IP: 34.107.221.82 Port: 80
b. Duration of the connection: 12.413007 seconds
c. Packets sent: 13

Exercise 13:



*enp0s31f6 (icmp) [Wireshark 1.10.14 (Git Rev Unknown from unknown)]@co2061-19.ece.iastate.edu
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: icmp

```
No.  Time          Source          Destination    Protoc Lengt Info
   1 0.000000000   192.168.254.32  192.168.254.0  ICMP     98 Echo (ping) request  id=0x4d33, seq=1486/52741, ttl=64
   2 20.020359462  192.168.254.32  192.168.254.0  ICMP     98 Echo (ping) request  id=0x4d33, seq=1487/52997, ttl=64
   3 40.023079655  192.168.254.32  192.168.254.0  ICMP     98 Echo (ping) request  id=0x4d33, seq=1488/53253, ttl=64
```

```
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: 50:9a:4c:47:39:57 (50:9a:4c:47:39:57), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.254.32 (192.168.254.32), Dst: 192.168.254.0 (192.168.254.0)
Internet Control Message Protocol
```

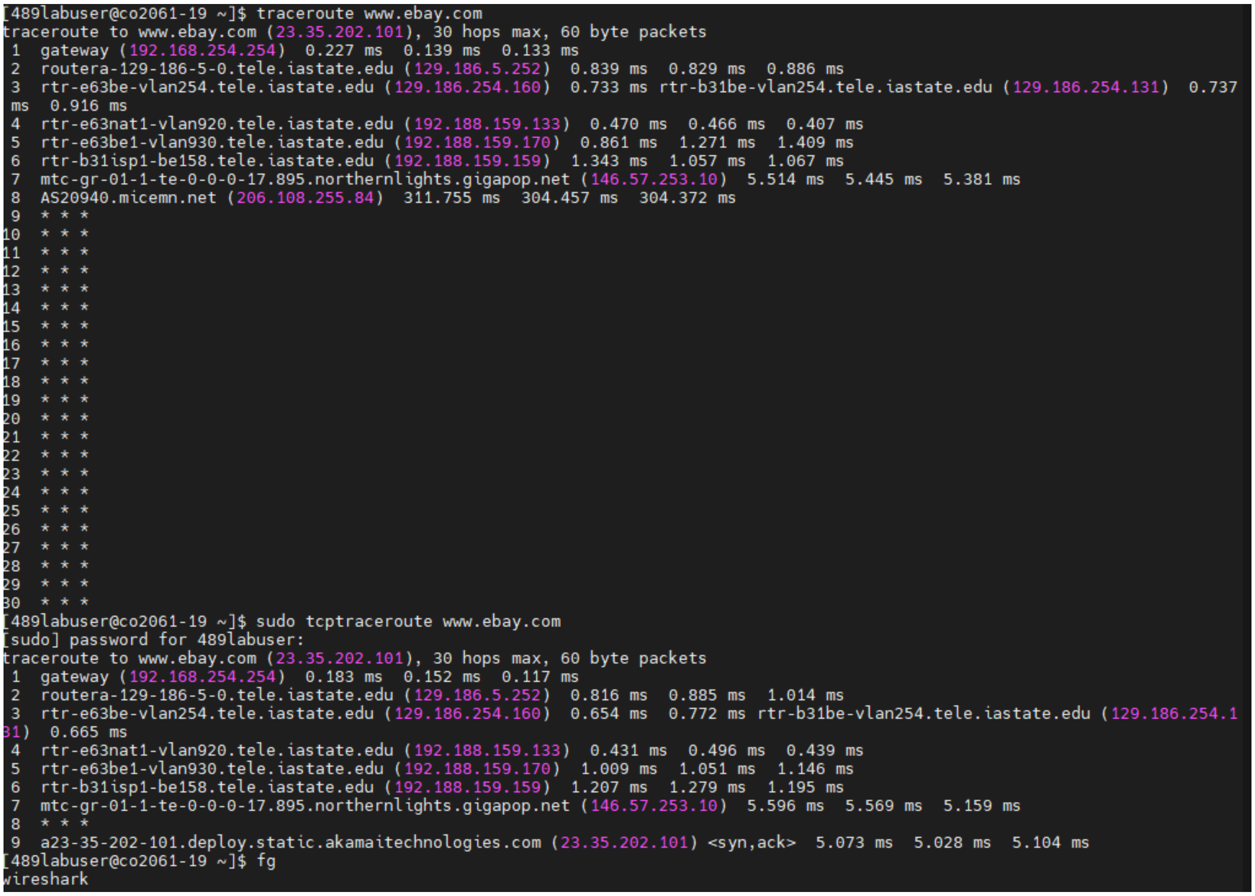
```
0000  ff ff ff ff ff ff 50 9a  4c 47 39 57 08 00 45 00   ......P. LG9W..E.
0010  00 54 00 00 40 00 40 01  bd 36 c0 a8 fe 20 c0 a8   .T..@.@. .6... ..
0020  fe 00 08 00 22 3c 4d 33  05 ce 59 dc 19 60 00 00   ...."<M3 ..Y..`..
0030  00 00 45 b3 0b 00 00 00  00 00 10 11 12 13 14 15   ..E..... ........
```

File: "/tmp/wireshark_pcapng_enp0... Packets: 3 · Displayed: 3 (100.0%) · Dropped: 0 (0.0%) Profile: Default

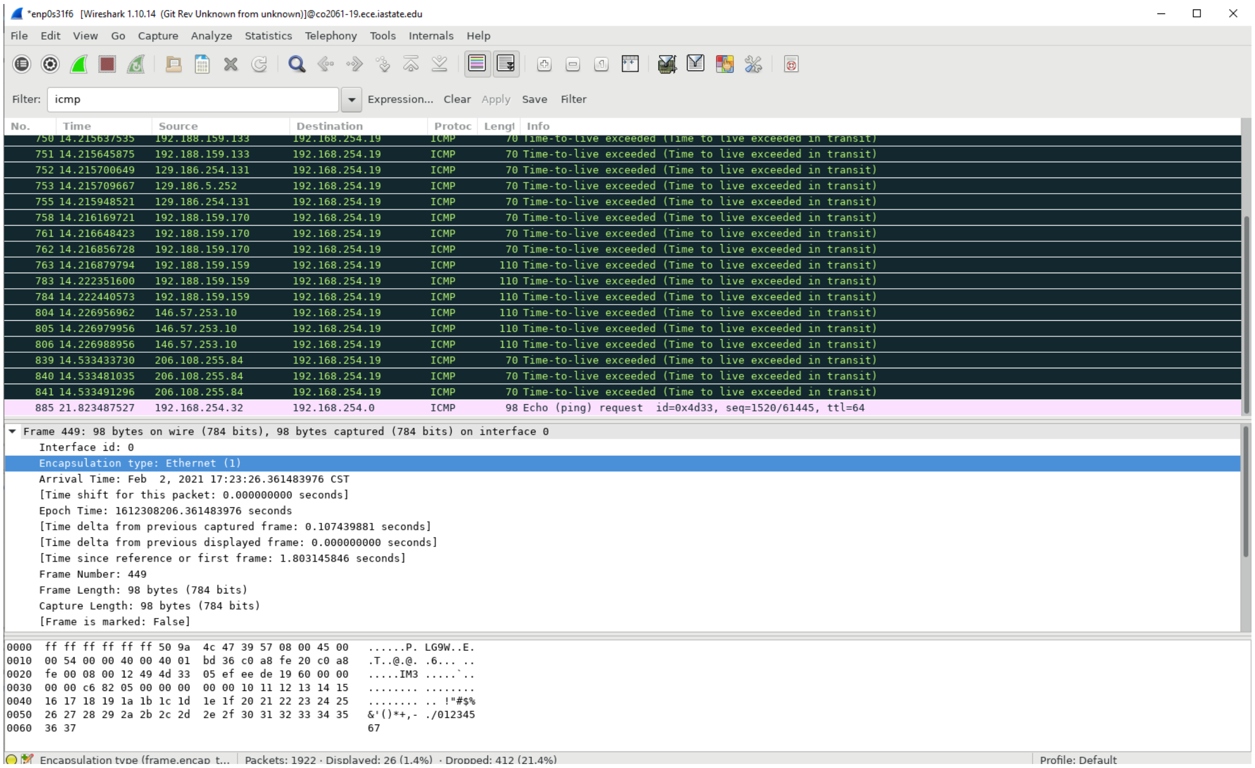
98 bytes per ICMP packet are sent. The arrival times are as follows:

- Feb 2, 2021 17:15:45.914
- Feb 2, 2021 17:16:05.934
- Feb 2, 2021 17:16:25.955

Exercise 14:



```
[489labuser@co2061-19 ~]$ traceroute www.ebay.com
traceroute to www.ebay.com (23.35.202.101), 30 hops max, 60 byte packets
 1  gateway (192.168.254.254)  0.227 ms  0.139 ms  0.133 ms
 2  routera-129-186-5-0.tele.iastate.edu (129.186.5.252)  0.839 ms  0.829 ms  0.886 ms
 3  rtr-e63be-vlan254.tele.iastate.edu (129.186.254.160)  0.733 ms rtr-b31be-vlan254.tele.iastate.edu (129.186.254.131)  0.737
 ms  0.916 ms
 4  rtr-e63nat1-vlan920.tele.iastate.edu (192.188.159.133)  0.470 ms  0.466 ms  0.407 ms
 5  rtr-e63be1-vlan930.tele.iastate.edu (192.188.159.170)  0.861 ms  1.271 ms  1.409 ms
 6  rtr-b31isp1-be158.tele.iastate.edu (192.188.159.159)  1.343 ms  1.057 ms  1.067 ms
 7  mtc-gr-01-1-te-0-0-0-17.895.northernlights.gigapop.net (146.57.253.10)  5.514 ms  5.445 ms  5.381 ms
 8  AS20940.micemn.net (206.108.255.84)  311.755 ms  304.457 ms  304.372 ms
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
[489labuser@co2061-19 ~]$ sudo tcptraceroute www.ebay.com
[sudo] password for 489labuser:
traceroute to www.ebay.com (23.35.202.101), 30 hops max, 60 byte packets
 1  gateway (192.168.254.254)  0.183 ms  0.152 ms  0.117 ms
 2  routera-129-186-5-0.tele.iastate.edu (129.186.5.252)  0.816 ms  0.885 ms  1.014 ms
 3  rtr-e63be-vlan254.tele.iastate.edu (129.186.254.160)  0.654 ms  0.772 ms rtr-b31be-vlan254.tele.iastate.edu (129.186.254.1
31)  0.665 ms
 4  rtr-e63nat1-vlan920.tele.iastate.edu (192.188.159.133)  0.431 ms  0.496 ms  0.439 ms
 5  rtr-e63be1-vlan930.tele.iastate.edu (192.188.159.170)  1.009 ms  1.051 ms  1.146 ms
 6  rtr-b31isp1-be158.tele.iastate.edu (192.188.159.159)  1.207 ms  1.279 ms  1.195 ms
 7  mtc-gr-01-1-te-0-0-0-17.895.northernlights.gigapop.net (146.57.253.10)  5.596 ms  5.569 ms  5.159 ms
 8  * * *
 9  a23-35-202-101.deploy.static.akamaitechnologies.com (23.35.202.101) <syn,ack>  5.073 ms  5.028 ms  5.104 ms
[489labuser@co2061-19 ~]$ fg
wireshark
```


*enp0s31f6 [Wireshark 1.10.14 (Git Rev Unknown from unknown)]@co2061-19.ece.iastate.edu
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save Filter

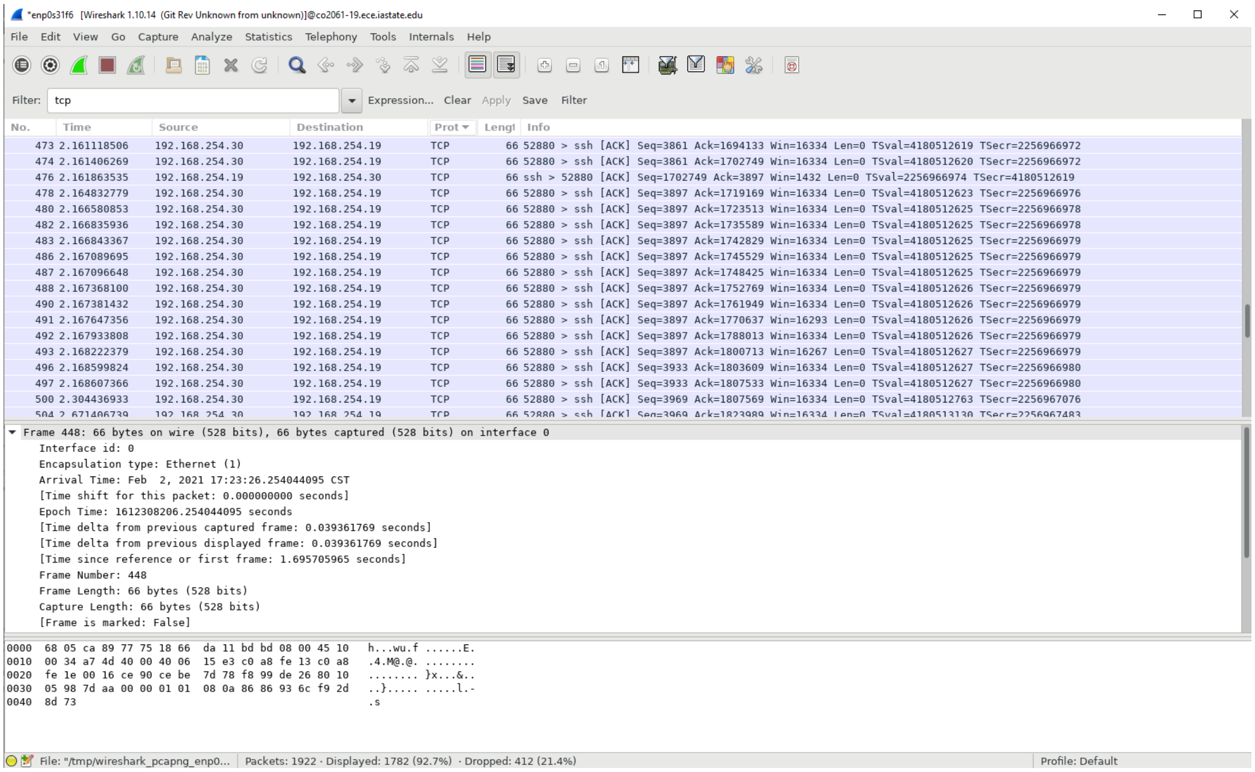
Filter: icmp

```
No.   Time          Source           Destination      Protoc Lengt Info
  750 14.215637535  192.188.159.133  192.168.254.19   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
  751 14.215645875  192.188.159.133  192.168.254.19   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
  752 14.215700649  129.186.254.131  192.168.254.19   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
  753 14.215709667  129.186.5.252    192.168.254.19   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
  755 14.215948521  129.186.254.131  192.168.254.19   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
  758 14.216169721  192.188.159.170  192.168.254.19   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
  761 14.216648423  192.188.159.170  192.168.254.19   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
  762 14.216856728  192.188.159.170  192.168.254.19   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
  763 14.216879794  192.188.159.159  192.168.254.19   ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
  783 14.222351600  192.188.159.159  192.168.254.19   ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
  784 14.222440573  192.188.159.159  192.168.254.19   ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
  804 14.226956962  146.57.253.10    192.168.254.19   ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
  805 14.226979956  146.57.253.10    192.168.254.19   ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
  806 14.226988956  146.57.253.10    192.168.254.19   ICMP   110 Time-to-live exceeded (Time to live exceeded in transit)
  839 14.533433730  206.108.255.84   192.168.254.19   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
  840 14.533481035  206.108.255.84   192.168.254.19   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
  841 14.533491296  206.108.255.84   192.168.254.19   ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
  885 21.823487527  192.168.254.32   192.168.254.0    ICMP    98 Echo (ping) request  id=0x4d33, seq=1520/61445, ttl=64
```

```
▼ Frame 449: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
    Interface id: 0
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb  2, 2021 17:23:26.361483976 CST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1612308206.361483976 seconds
    [Time delta from previous captured frame: 0.107439881 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 1.803145846 seconds]
    Frame Number: 449
    Frame Length: 98 bytes (784 bits)
    Capture Length: 98 bytes (784 bits)
    [Frame is marked: False]
```

```
0000  ff ff ff ff ff ff 50 9a  4c 47 39 57 08 00 45 00   ......P. LG9W..E.
0010  00 54 00 00 40 00 40 01  bd 36 c0 a8 fe 20 c0 a8   .T..@.@. .6... ..
0020  fe 00 08 00 12 49 4d 33  05 ef ee de 19 60 00 00   .....IM3 .....`..
0030  00 00 c6 82 05 00 00 00  00 00 10 11 12 13 14 15   ........ ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

Encapsulation type (frame.encap_t... | Packets: 1922 · Displayed: 26 (1.4%) · Dropped: 412 (21.4%) | Profile: Default



Filter: tcp

```
No.   Time          Source            Destination       Prot  Lengt Info
  473 2.161118506   192.168.254.30    192.168.254.19    TCP        66 52880 > ssh [ACK] Seq=3861 Ack=1694133 Win=16334 Len=0 TSval=4180512619 TSecr=2256966972
  474 2.161406269   192.168.254.30    192.168.254.19    TCP        66 52880 > ssh [ACK] Seq=3861 Ack=1702749 Win=16334 Len=0 TSval=4180512620 TSecr=2256966972
  476 2.161863535   192.168.254.19    192.168.254.30    TCP        66 ssh > 52880 [ACK] Seq=1702749 Ack=3897 Win=1432 Len=0 TSval=2256966974 TSecr=4180512619
  478 2.164832779   192.168.254.30    192.168.254.19    TCP        66 52880 > ssh [ACK] Seq=3897 Ack=1719169 Win=16334 Len=0 TSval=4180512623 TSecr=2256966976
  480 2.166580853   192.168.254.30    192.168.254.19    TCP        66 52880 > ssh [ACK] Seq=3897 Ack=1723513 Win=16334 Len=0 TSval=4180512625 TSecr=2256966978
  482 2.166835936   192.168.254.30    192.168.254.19    TCP        66 52880 > ssh [ACK] Seq=3897 Ack=1735589 Win=16334 Len=0 TSval=4180512625 TSecr=2256966978
  483 2.166843367   192.168.254.30    192.168.254.19    TCP        66 52880 > ssh [ACK] Seq=3897 Ack=1742829 Win=16334 Len=0 TSval=4180512625 TSecr=2256966979
  486 2.167089695   192.168.254.30    192.168.254.19    TCP        66 52880 > ssh [ACK] Seq=3897 Ack=1745529 Win=16334 Len=0 TSval=4180512625 TSecr=2256966979
  487 2.167096648   192.168.254.30    192.168.254.19    TCP        66 52880 > ssh [ACK] Seq=3897 Ack=1748425 Win=16334 Len=0 TSval=4180512625 TSecr=2256966979
  488 2.167368100   192.168.254.30    192.168.254.19    TCP        66 52880 > ssh [ACK] Seq=3897 Ack=1752769 Win=16334 Len=0 TSval=4180512626 TSecr=2256966979
  490 2.167381432   192.168.254.30    192.168.254.19    TCP        66 52880 > ssh [ACK] Seq=3897 Ack=1761949 Win=16334 Len=0 TSval=4180512626 TSecr=2256966979
  491 2.167647356   192.168.254.30    192.168.254.19    TCP        66 52880 > ssh [ACK] Seq=3897 Ack=1770637 Win=16293 Len=0 TSval=4180512626 TSecr=2256966979
  492 2.167933808   192.168.254.30    192.168.254.19    TCP        66 52880 > ssh [ACK] Seq=3897 Ack=1788013 Win=16334 Len=0 TSval=4180512626 TSecr=2256966979
  493 2.168222379   192.168.254.30    192.168.254.19    TCP        66 52880 > ssh [ACK] Seq=3897 Ack=1800713 Win=16267 Len=0 TSval=4180512627 TSecr=2256966979
  496 2.168599824   192.168.254.30    192.168.254.19    TCP        66 52880 > ssh [ACK] Seq=3933 Ack=1803609 Win=16334 Len=0 TSval=4180512627 TSecr=2256966980
  497 2.168607366   192.168.254.30    192.168.254.19    TCP        66 52880 > ssh [ACK] Seq=3933 Ack=1807533 Win=16334 Len=0 TSval=4180512627 TSecr=2256966980
  500 2.304436933   192.168.254.30    192.168.254.19    TCP        66 52880 > ssh [ACK] Seq=3969 Ack=1807569 Win=16334 Len=0 TSval=4180512763 TSecr=2256967076
  504 2.671406739   192.168.254.30    192.168.254.19    TCP        66 52880 > ssh [ACK] Seq=3969 Ack=1823989 Win=16334 Len=0 TSval=4180513130 TSecr=2256967483
```

```
▾ Frame 448: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
    Interface id: 0
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb  2, 2021 17:23:26.254044095 CST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1612308206.254044095 seconds
    [Time delta from previous captured frame: 0.039361769 seconds]
    [Time delta from previous displayed frame: 0.039361769 seconds]
    [Time since reference or first frame: 1.695705965 seconds]
    Frame Number: 448
    Frame Length: 66 bytes (528 bits)
    Capture Length: 66 bytes (528 bits)
    [Frame is marked: False]
```

```
0000  68 05 ca 89 77 75 18 66  da 11 bd bd 08 00 45 10   h...wu.f ......E.
0010  00 34 a7 4d 40 00 40 06  15 e3 c0 a8 fe 13 c0 a8   .4.M@.@. ........
0020  fe 1e 00 16 ce 90 ce be  7d 78 f8 99 de 26 80 10   ........ }x...&..
0030  05 98 7d aa 00 00 01 01  08 0a 86 86 93 6c f9 2d   ..}..... .....l.-
0040  8d 73                                              .s
```

File: "/tmp/wireshark_pcapng_enp0... Packets: 1922 · Displayed: 1782 (92.7%) · Dropped: 412 (21.4%) Profile: Default

Traceroute sends ICMP and UDP packets, shown in the top screenshot. Tcptraceroute sends TCP SYN packets shown in the bottom screenshot.