Samantha Neri, Khushveen Kaur Umra
CPRE 489, Section 2

25th January 2023

Lab I Report

Qa) Summarize what you learned in a few paragraphs.

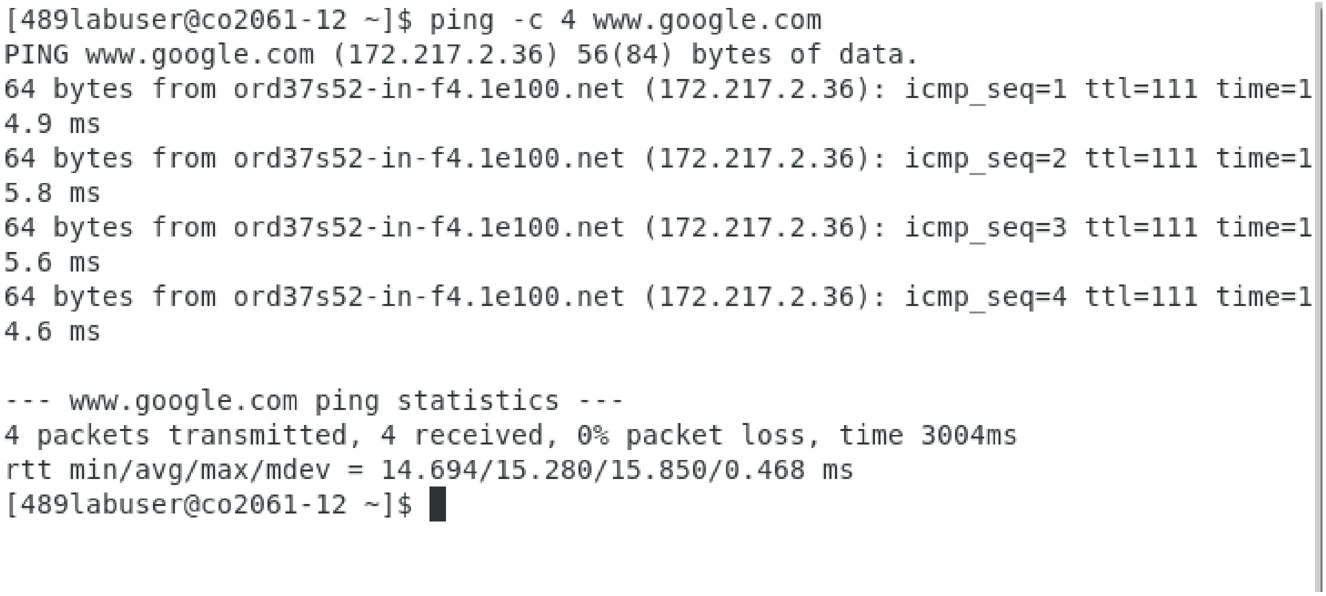
Overall, we've learned how to use basic network diagnostic and probing tools to include: ping, nslookup, ifconfig, iperf, traceroute, tcptraceroute, Nmap, tcpdump, tcptrace, and Wireshark. Starting with ping, we learned about the default loopback address, which helps with checking network setup. We then had to use nslookup, which showed us how to change its search parameters to find different kinds of information. We also had the chance to work with tcpdump and tcptrace, which is something we never used before, and we learnt that it is used to analyze packets sent to and from machines.

Overall, we believe that this lab was extremely useful and informative for new beginners like us. We were able to learn about all the new commands that can be used in a Linux system, and learned about their functionality.

Qb) Answer any questions asked in the exercises throughout the experiment.

1.) Use ping to find the average round-trip time from your machine to each of the following machines (include the output from the third section of ping for verification):

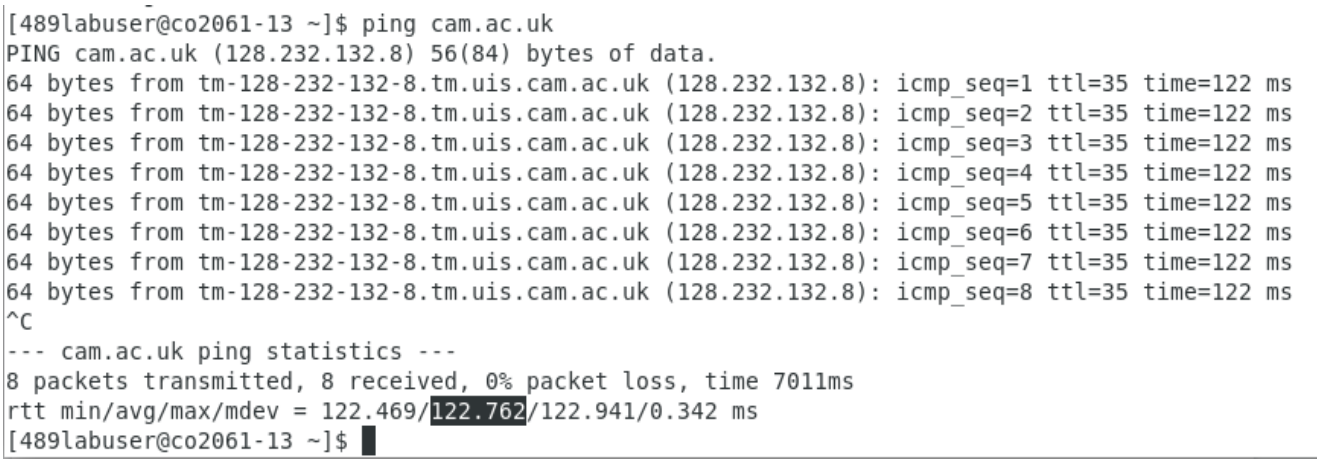
a) www.google.com



```
[489labuser@co2061-12 ~]$ ping -c 4 www.google.com
PING www.google.com (172.217.2.36) 56(84) bytes of data.
64 bytes from ord37s52-in-f4.1e100.net (172.217.2.36): icmp_seq=1 ttl=111 time=1
4.9 ms
64 bytes from ord37s52-in-f4.1e100.net (172.217.2.36): icmp_seq=2 ttl=111 time=1
5.8 ms
64 bytes from ord37s52-in-f4.1e100.net (172.217.2.36): icmp_seq=3 ttl=111 time=1
5.6 ms
64 bytes from ord37s52-in-f4.1e100.net (172.217.2.36): icmp_seq=4 ttl=111 time=1
4.6 ms

--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 14.694/15.280/15.850/0.468 ms
[489labuser@co2061-12 ~]$ █
```

→ Average Round-trip time = 15.280 ms

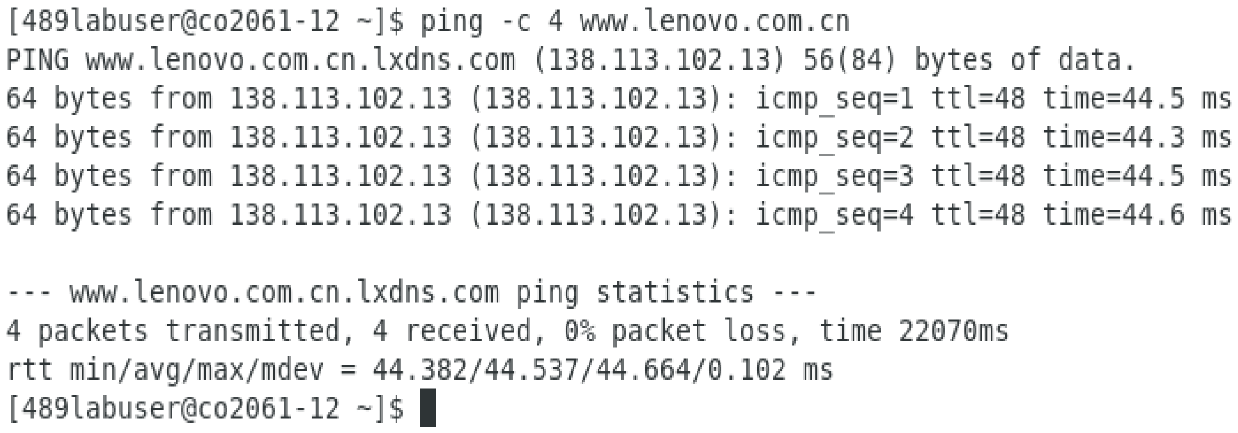
b) www.cam.ac.uk



```
[489labuser@co2061-13 ~]$ ping cam.ac.uk
PING 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=35 time=122 ms
64 bytes from tm-128-232-132-8.tm.uis.cam.ac.uk (128.232.132.8): icmp_seq=2 ttl=35 time=122 ms
64 bytes from tm-128-232-132-8.tm.uis.cam.ac.uk (128.232.132.8): icmp_seq=3 ttl=35 time=122 ms
64 bytes from tm-128-232-132-8.tm.uis.cam.ac.uk (128.232.132.8): icmp_seq=4 ttl=35 time=122 ms
64 bytes from tm-128-232-132-8.tm.uis.cam.ac.uk (128.232.132.8): icmp_seq=5 ttl=35 time=122 ms
64 bytes from tm-128-232-132-8.tm.uis.cam.ac.uk (128.232.132.8): icmp_seq=6 ttl=35 time=122 ms
64 bytes from tm-128-232-132-8.tm.uis.cam.ac.uk (128.232.132.8): icmp_seq=7 ttl=35 time=122 ms
64 bytes from tm-128-232-132-8.tm.uis.cam.ac.uk (128.232.132.8): icmp_seq=8 ttl=35 time=122 ms
^C
--- cam.ac.uk ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7011ms
rtt min/avg/max/mdev = 122.469/122.762/122.941/0.342 ms
[489labuser@co2061-13 ~]$ █
```

→ Avg. Round-trip time = 122.762 ms

c) ***www.lenovo.com.cn***



```
[489labuser@co2061-12 ~]$ ping -c 4 www.lenovo.com.cn
PING www.lenovo.com.cn.lxdns.com (138.113.102.13) 56(84) bytes of data.
64 bytes from 138.113.102.13 (138.113.102.13): icmp_seq=1 ttl=48 time=44.5 ms
64 bytes from 138.113.102.13 (138.113.102.13): icmp_seq=2 ttl=48 time=44.3 ms
64 bytes from 138.113.102.13 (138.113.102.13): icmp_seq=3 ttl=48 time=44.5 ms
64 bytes from 138.113.102.13 (138.113.102.13): icmp_seq=4 ttl=48 time=44.6 ms

--- www.lenovo.com.cn.lxdns.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 22070ms
rtt min/avg/max/mdev = 44.382/44.537/44.664/0.102 ms
[489labuser@co2061-12 ~]$
```

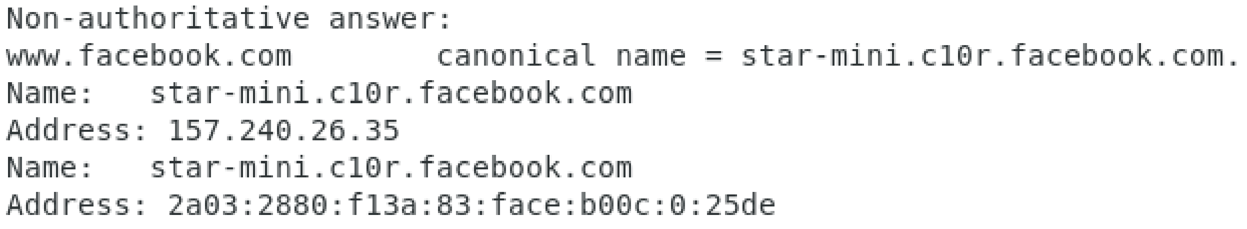
→ Average RTT = 44.537 ms

2) A loopback address is a special IP address, 127.0.0.1, reserved by InterNIC for testing network cards. In other words, pinging the loopback address is not a test of connection, but a test of network setup. Ping 127.0.0.1 and explain the results.

- Pinging the IP address had faster results, due to the computer being able to directly communicate with itself. The primary difference is that the connection avoids using the local network interface hardware. For example, the average RTT was 0.057 ms after 4 packets were transmitted.

3) Use nslookup to non-interactively determine the IP addresses and aliases (canonical names) for the following machines:

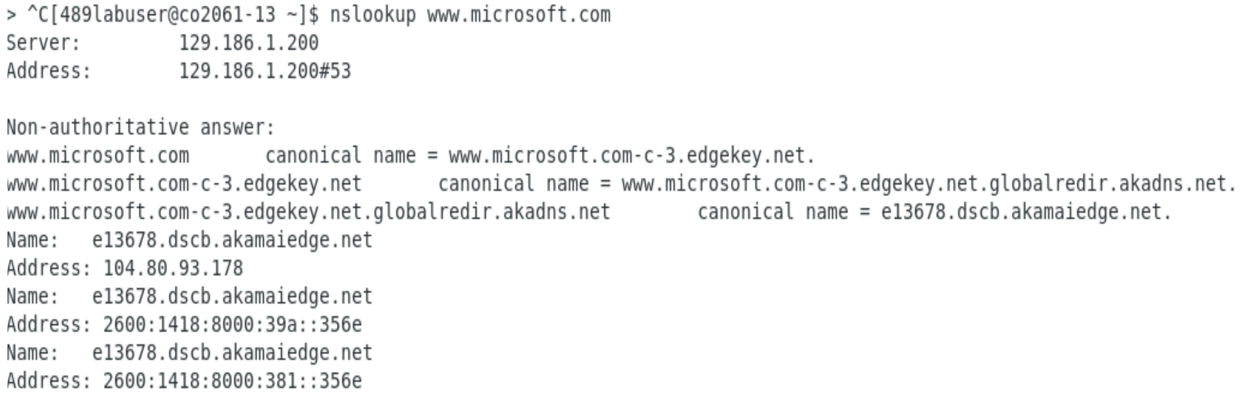
a) www.facebook.com



```
Non-authoritative answer:
www.facebook.com        canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 157.240.26.35
Name:   star-mini.c10r.facebook.com
Address: 2a03:2880:f13a:83:face:b00c:0:25de
```

→ IP address: 157.240.26.35
→ Canonical Names: star-mini.c10r.facebook.com

b) www.microsoft.com

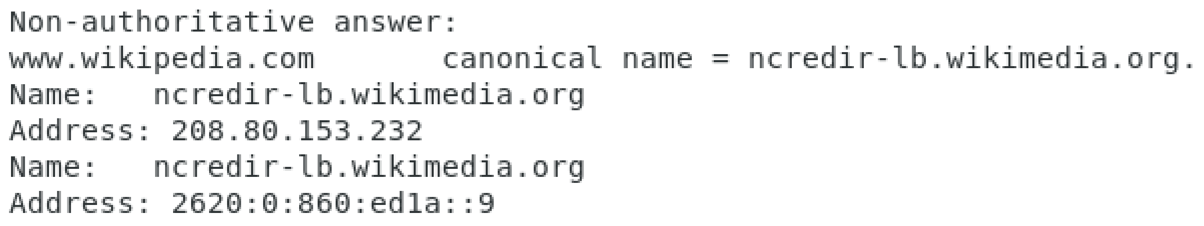


```
> ^C[489labuser@co2061-13 ~]$ nslookup www.microsoft.com
Server:         129.186.1.200
Address:        129.186.1.200#53

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.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: 104.80.93.178
Name:   e13678.dscb.akamaiedge.net
Address: 2600:1418:8000:39a::356e
Name:   e13678.dscb.akamaiedge.net
Address: 2600:1418:8000:381::356e
```

→ IP address: 104.80.93.178

→ Canonical Names: e13678.dscb.akamaiedge.net.

c) www.wikipedia.com

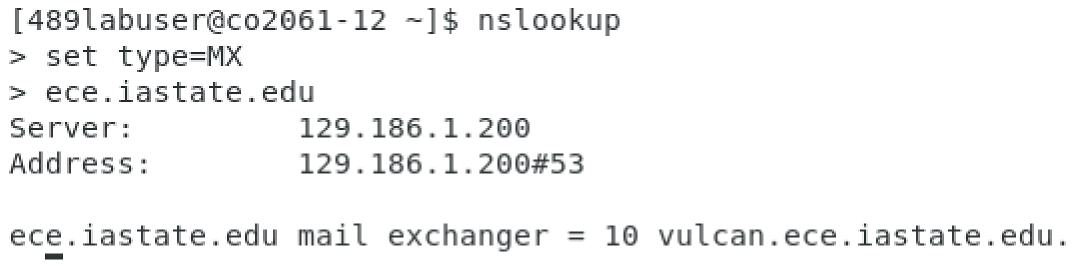


```
Non-authoritative answer:
www.wikipedia.com       canonical name = ncredir-lb.wikimedia.org.
Name:   ncredir-lb.wikimedia.org
Address: 208.80.153.232
Name:   ncredir-lb.wikimedia.org
Address: 2620:0:860:ed1a::9
```

→ IP address: 208.80.153.232

→ Canonical Names: ncredir-lb.wikimedia.org

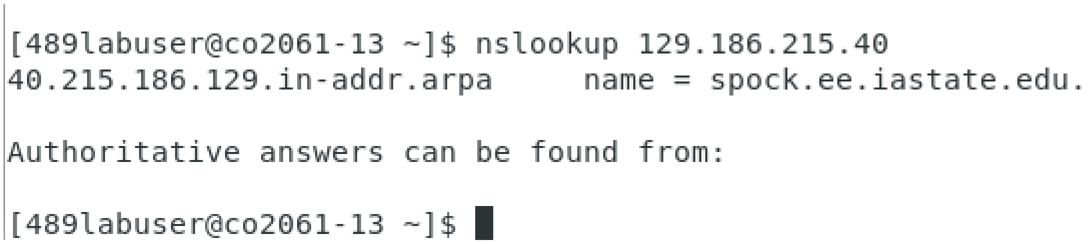
4) Use nslookup to interactively find the mail exchanger for ece.iastate.edu.



```
[489labuser@co2061-12 ~]$ 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.
```

→ Mail Exchanger: 10 vulcan.ece.iastate.edu.

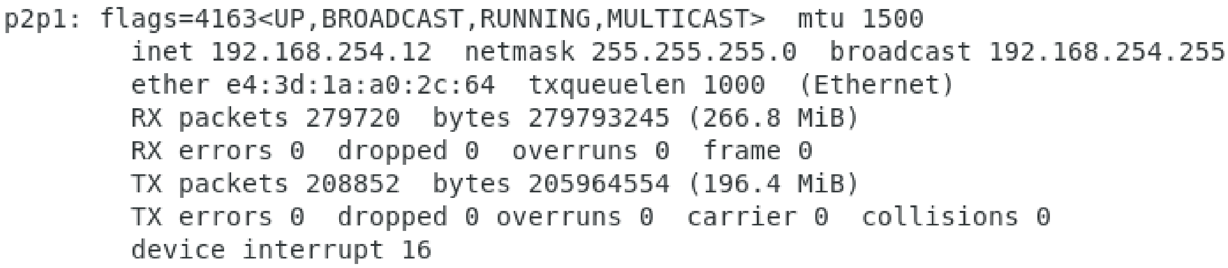
5) Use nslookup to find the name of the machine with IP address 129.186.215.40.



```
[489labuser@co2061-13 ~]$ nslookup 129.186.215.40
40.215.186.129.in-addr.arpa     name = spock.ee.iastate.edu.

Authoritative answers can be found from:

[489labuser@co2061-13 ~]$ █
```

→ Name of the machine: spock.ee.iastate.edu

6) Use ifconfig to determine the IP address for interface p2p1 on your machine. HINT: Record this IP address for use in later exercises.



```
p2p1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.254.12  netmask 255.255.255.0  broadcast 192.168.254.255
        ether e4:3d:1a:a0:2c:64  txqueuelen 1000  (Ethernet)
        RX packets 279720  bytes 279793245 (266.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 208852  bytes 205964554 (196.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16
```

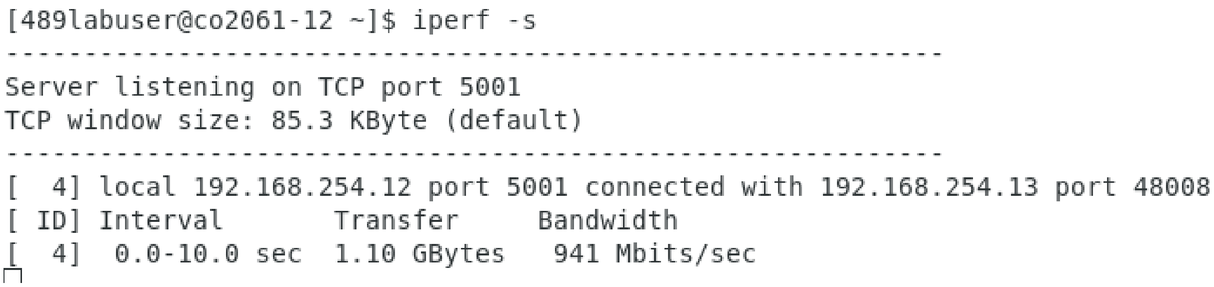
→ Sam: 192.168.254.12
→ Khushveen: 192.168.254.13

7) This exercise will require both partners' machines. On partner1's computer run iperf -s and on partner2's run iperf -c [address] where "address" is the ip address that partner1 recorded earlier (the IP address of interface p2p1).

Make sure to include screenshots from both computers.
Summarize your observations on the bandwidth between the two hosts. Is the connection most likely 10 Mbps or 100 Mbps or 1 Gbps?

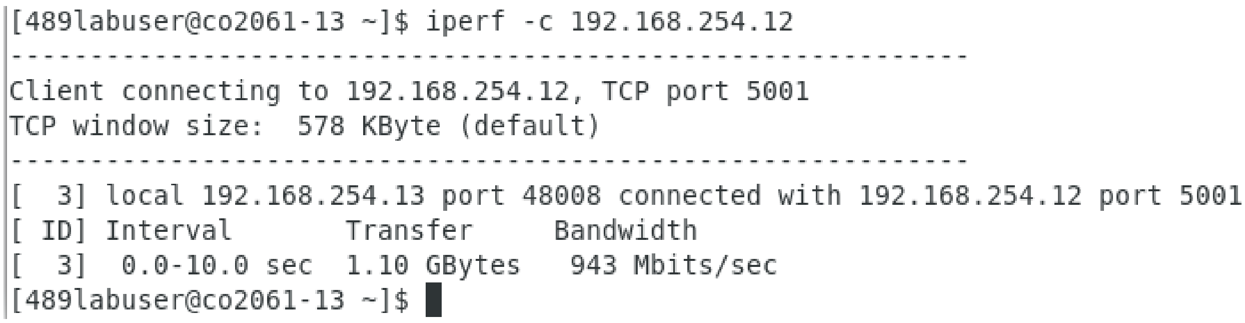
Part 1)

Partner I:



```
[489labuser@co2061-12 ~]$ iperf -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
------------------------------------------------------------
[  4] local 192.168.254.12 port 5001 connected with 192.168.254.13 port 48008
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-10.0 sec  1.10 GBytes   941 Mbits/sec
```

Partner II:

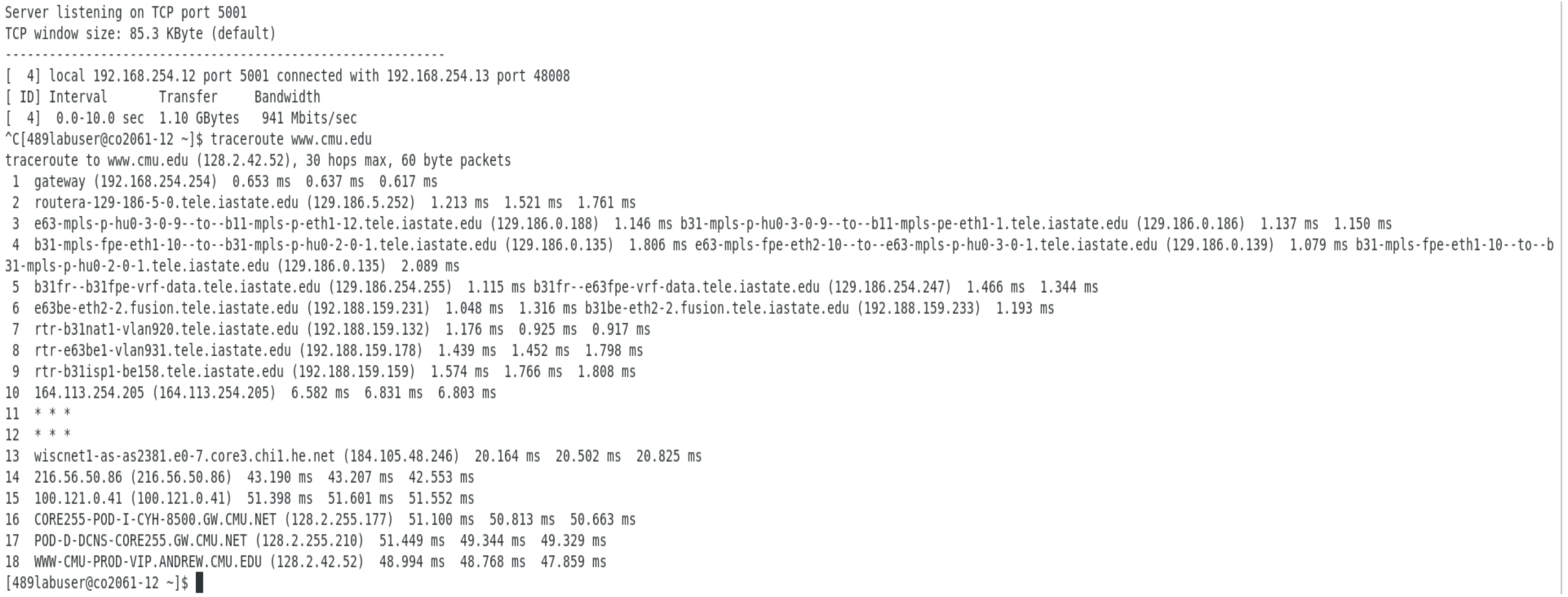


```
[489labuser@co2061-13 ~]$ iperf -c 192.168.254.12
------------------------------------------------------------
Client connecting to 192.168.254.12, TCP port 5001
TCP window size:  578 KByte (default)
------------------------------------------------------------
[  3] local 192.168.254.13 port 48008 connected with 192.168.254.12 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec  1.10 GBytes   943 Mbits/sec
[489labuser@co2061-13 ~]$
```

Part 2)

Observations: Our bandwidth is 943 Mbits / sec. This would round up to be about 1 Gbps for our bandwidth.

8) Perform traceroute from your computer to www.cmu.edu. Summarize your observations on number of hops, routes, gateways, latency, and reachability.



```
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
------------------------------------------------------------
[  4] local 192.168.254.12 port 5001 connected with 192.168.254.13 port 48008
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-10.0 sec  1.10 GBytes   941 Mbits/sec
^C[489labuser@co2061-12 ~]$ 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)  0.653 ms  0.637 ms  0.617 ms
 2  routera-129-186-5-0.tele.iastate.edu (129.186.5.252)  1.213 ms  1.521 ms  1.761 ms
 3  e63-mpls-p-hu0-3-0-9--to--b11-mpls-p-eth1-12.tele.iastate.edu (129.186.0.188)  1.146 ms b31-mpls-p-hu0-3-0-9--to--b11-mpls-pe-eth1-1.tele.iastate.edu (129.186.0.186)  1.137 ms  1.150 ms
 4  b31-mpls-fpe-eth1-10--to--b31-mpls-p-hu0-2-0-1.tele.iastate.edu (129.186.0.135)  1.806 ms e63-mpls-fpe-eth2-10--to--e63-mpls-p-hu0-3-0-1.tele.iastate.edu (129.186.0.139)  1.079 ms b31-mpls-fpe-eth1-10--to--b
31-mpls-p-hu0-2-0-1.tele.iastate.edu (129.186.0.135)  2.089 ms
 5  b31fr--b31fpe-vrf-data.tele.iastate.edu (129.186.254.255)  1.115 ms b31fr--e63fpe-vrf-data.tele.iastate.edu (129.186.254.247)  1.466 ms  1.344 ms
 6  e63be-eth2-2.fusion.tele.iastate.edu (192.188.159.231)  1.048 ms  1.316 ms b31be-eth2-2.fusion.tele.iastate.edu (192.188.159.233)  1.193 ms
 7  rtr-b31nat1-vlan920.tele.iastate.edu (192.188.159.132)  1.176 ms  0.925 ms  0.917 ms
 8  rtr-e63be1-vlan931.tele.iastate.edu (192.188.159.178)  1.439 ms  1.452 ms  1.798 ms
 9  rtr-b31isp1-be158.tele.iastate.edu (192.188.159.159)  1.574 ms  1.766 ms  1.808 ms
10  164.113.254.205 (164.113.254.205)  6.582 ms  6.831 ms  6.803 ms
11  * * *
12  * * *
13  wiscnet1-as-as2381.e0-7.core3.chi1.he.net (184.105.48.246)  20.164 ms  20.502 ms  20.825 ms
14  216.56.50.86 (216.56.50.86)  43.190 ms  43.207 ms  42.553 ms
15  100.121.0.41 (100.121.0.41)  51.398 ms  51.601 ms  51.552 ms
16  CORE255-POD-I-CYH-8500.GW.CMU.NET (128.2.255.177)  51.100 ms  50.813 ms  50.663 ms
17  POD-D-DCNS-CORE255.GW.CMU.NET (128.2.255.210)  51.449 ms  49.344 ms  49.329 ms
18  WWW-CMU-PROD-VIP.ANDREW.CMU.EDU (128.2.42.52)  48.994 ms  48.768 ms  47.859 ms
[489labuser@co2061-12 ~]$ █
```

→ Number of hops = 18

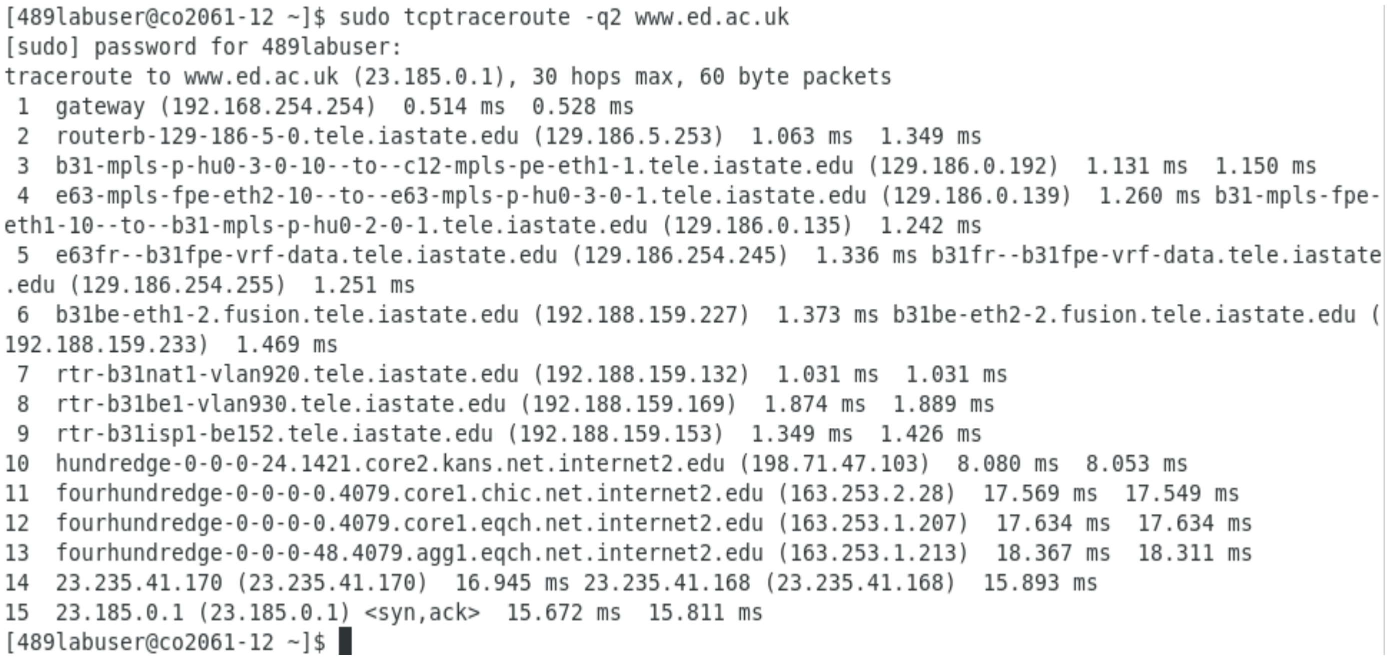
→ Routes = routera-129-186-5-0.tele.iastate.edu (129.186.5.252), the packets make their way through ISU's network, then are routed through the web with routing tables to eventually reach CMU's network. After that, the routing tables find the correct path to www.cmu.edu

→ Gateways = gateway (192.168.254.254), the gateways on this route go from ISU's network, to the www., to CMU's network.

→ Latency = The round trip times for these packets were 48.994 ms, 48.768ms, and 47.859ms. This creates and average round trip time of 48.540ms.

→ Reachability = We noticed that hop 11 and 12 show "* * *". This means that this is where the program didn't receive any response from the router; which means that the host blocked those packets, making it harder to reach to the site to get any network information.

9) Use tcptraceroute to determine the route packets take to www.ed.ac.uk. What is different from the trace using traceroute? Why do you think this is so?

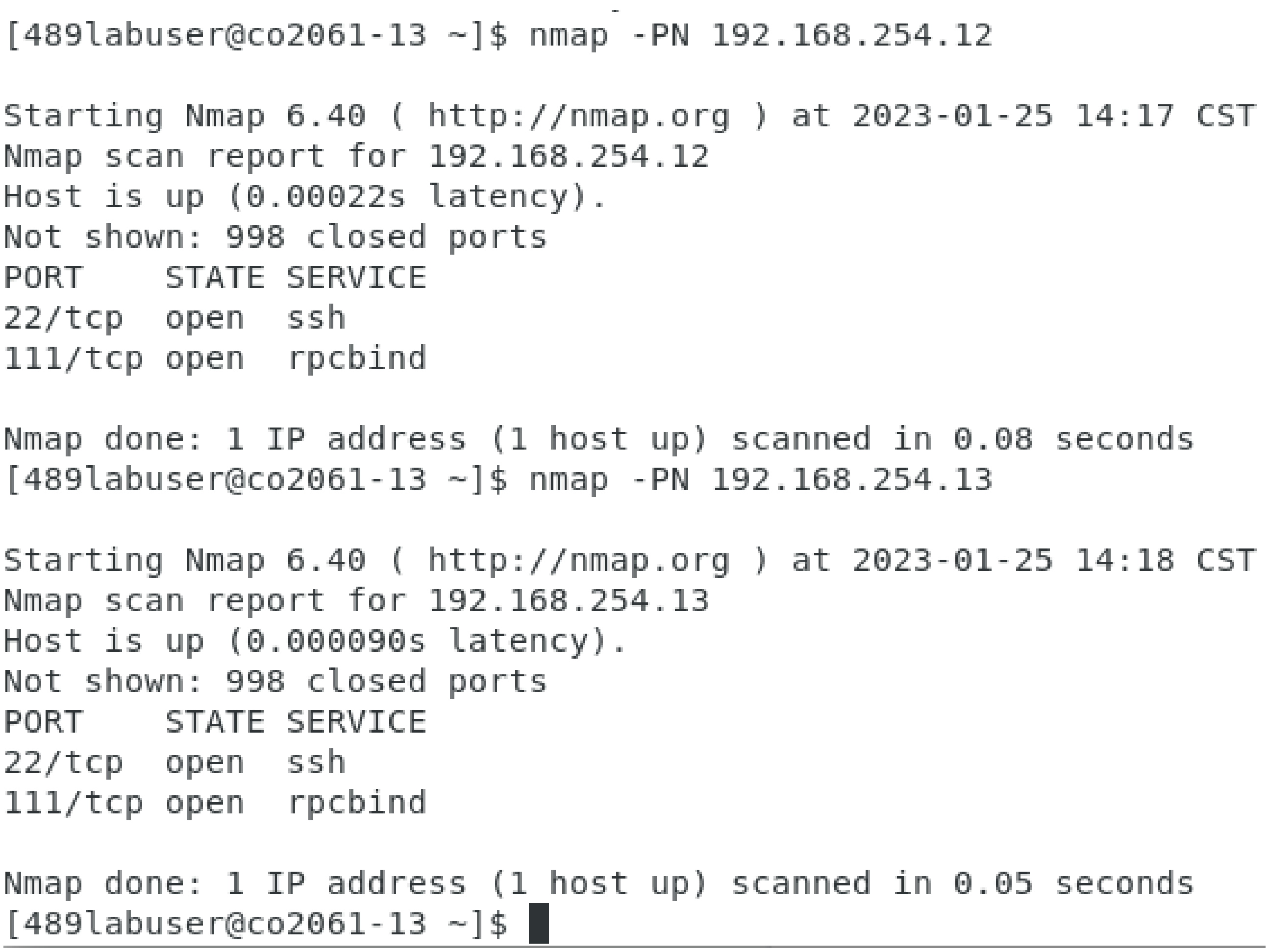


```
[489labuser@co2061-12 ~]$ sudo tcptraceroute -q2 www.ed.ac.uk
[sudo] password for 489labuser:
traceroute to www.ed.ac.uk (23.185.0.1), 30 hops max, 60 byte packets
 1  gateway (192.168.254.254)  0.514 ms  0.528 ms
 2  routerb-129-186-5-0.tele.iastate.edu (129.186.5.253)  1.063 ms  1.349 ms
 3  b31-mpls-p-hu0-3-0-10--to--c12-mpls-pe-eth1-1.tele.iastate.edu (129.186.0.192)  1.131 ms  1.150 ms
 4  e63-mpls-fpe-eth2-10--to--e63-mpls-p-hu0-3-0-1.tele.iastate.edu (129.186.0.139)  1.260 ms b31-mpls-fpe-
eth1-10--to--b31-mpls-p-hu0-2-0-1.tele.iastate.edu (129.186.0.135)  1.242 ms
 5  e63fr--b31fpe-vrf-data.tele.iastate.edu (129.186.254.245)  1.336 ms b31fr--b31fpe-vrf-data.tele.iastate
.edu (129.186.254.255)  1.251 ms
 6  b31be-eth1-2.fusion.tele.iastate.edu (192.188.159.227)  1.373 ms b31be-eth2-2.fusion.tele.iastate.edu (
192.188.159.233)  1.469 ms
 7  rtr-b31nat1-vlan920.tele.iastate.edu (192.188.159.132)  1.031 ms  1.031 ms
 8  rtr-b31be1-vlan930.tele.iastate.edu (192.188.159.169)  1.874 ms  1.889 ms
 9  rtr-b31isp1-be152.tele.iastate.edu (192.188.159.153)  1.349 ms  1.426 ms
10  hundredge-0-0-0-24.1421.core2.kans.net.internet2.edu (198.71.47.103)  8.080 ms  8.053 ms
11  fourhundredge-0-0-0-0.4079.core1.chic.net.internet2.edu (163.253.2.28)  17.569 ms  17.549 ms
12  fourhundredge-0-0-0-0.4079.core1.eqch.net.internet2.edu (163.253.1.207)  17.634 ms  17.634 ms
13  fourhundredge-0-0-0-48.4079.agg1.eqch.net.internet2.edu (163.253.1.213)  18.367 ms  18.311 ms
14  23.235.41.170 (23.235.41.170)  16.945 ms 23.235.41.168 (23.235.41.168)  15.893 ms
15  23.185.0.1 (23.185.0.1) <syn,ack>  15.672 ms  15.811 ms
[489labuser@co2061-12 ~]$ █
```

→ For tcptraceroute, we had to make sure that we were using the super user permissions to run, using “sudo”, which later asked us to input the password for the account being used. It also shows more hop information, because the gateways closer to the destination have a firewall in place that blocks the ICMP packets. Another thing that we noticed is that reachability for tcptraceroute is much better than the reachability for traceroute, and all of the hops in this were able to get a response from the router.

This is because tcptraceroute utilizes TCP SYN packets to bypass the most common firewalls and elicit responses from a wider variety of machines that traceroute, which uses UDP and ICMP packets.

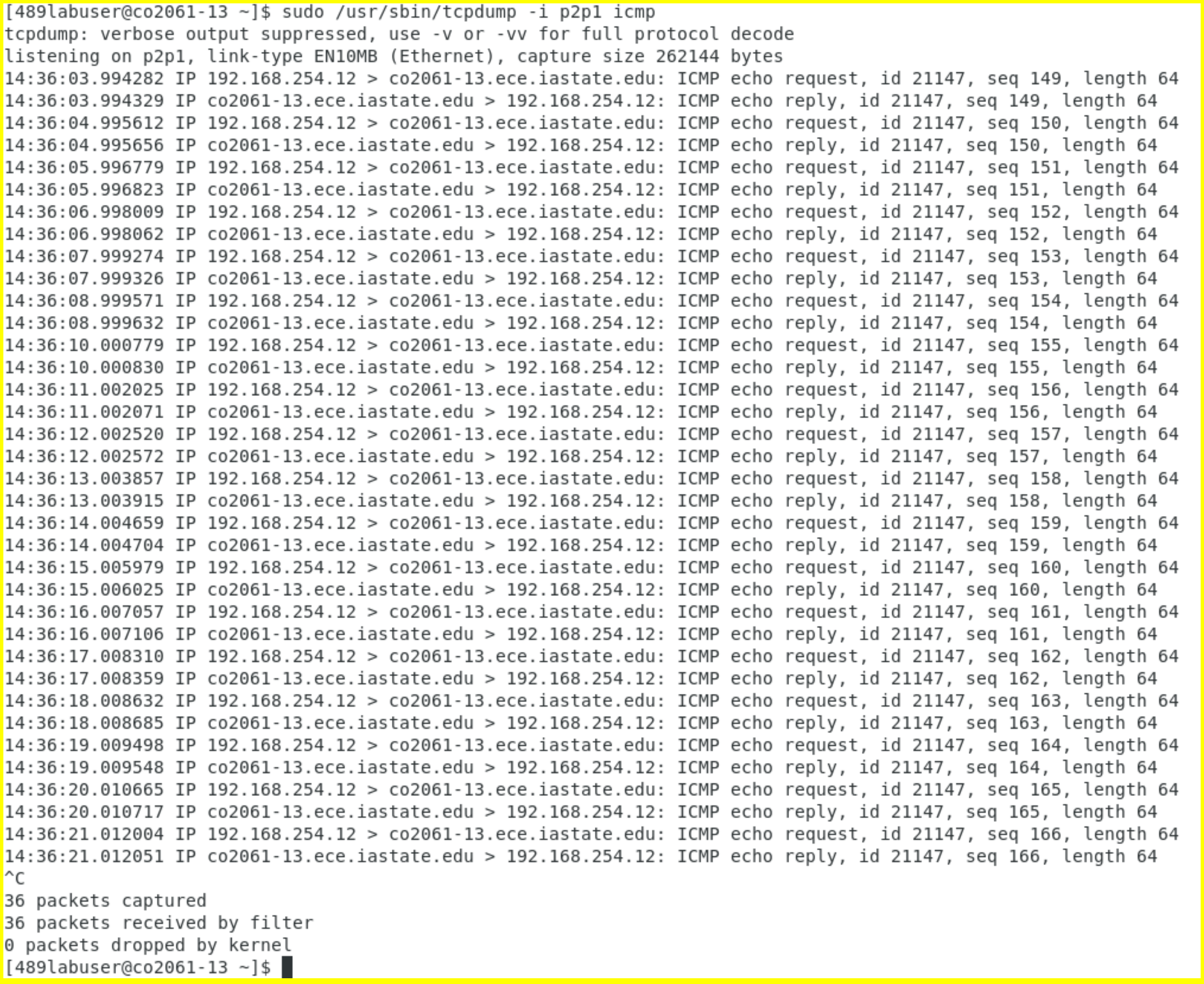
10) Is port 22 (SSH) open on your partner’s computer? Note that nmap accepts only the Host IP.



```
[489labuser@co2061-13 ~]$ nmap -PN 192.168.254.12

Starting Nmap 6.40 ( http://nmap.org ) at 2023-01-25 14:17 CST
Nmap scan report for 192.168.254.12
Host is up (0.00022s 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 0.08 seconds
[489labuser@co2061-13 ~]$ nmap -PN 192.168.254.13

Starting Nmap 6.40 ( http://nmap.org ) at 2023-01-25 14:18 CST
Nmap scan report for 192.168.254.13
Host is up (0.000090s 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 0.05 seconds
[489labuser@co2061-13 ~]$ █
```

→ Yes, we noticed that port 22 is open for both of our computers.

11) Your machine is currently undergoing a ping flood attack! On partner1's computer, execute ping [address] where "address" is partner2's IP. On partner2's computer use tcpdump and filter for ICMP packets to determine the IP address of the machine that is sending the packets.



```
[489labuser@co2061-13 ~]$ sudo /usr/sbin/tcpdump -i p2p1 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on p2p1, link-type EN10MB (Ethernet), capture size 262144 bytes
14:36:03.994282 IP 192.168.254.12 > co2061-13.ece.iastate.edu: ICMP echo request, id 21147, seq 149, length 64
14:36:03.994329 IP co2061-13.ece.iastate.edu > 192.168.254.12: ICMP echo reply, id 21147, seq 149, length 64
14:36:04.995612 IP 192.168.254.12 > co2061-13.ece.iastate.edu: ICMP echo request, id 21147, seq 150, length 64
14:36:04.995656 IP co2061-13.ece.iastate.edu > 192.168.254.12: ICMP echo reply, id 21147, seq 150, length 64
14:36:05.996779 IP 192.168.254.12 > co2061-13.ece.iastate.edu: ICMP echo request, id 21147, seq 151, length 64
14:36:05.996823 IP co2061-13.ece.iastate.edu > 192.168.254.12: ICMP echo reply, id 21147, seq 151, length 64
14:36:06.998009 IP 192.168.254.12 > co2061-13.ece.iastate.edu: ICMP echo request, id 21147, seq 152, length 64
14:36:06.998062 IP co2061-13.ece.iastate.edu > 192.168.254.12: ICMP echo reply, id 21147, seq 152, length 64
14:36:07.999274 IP 192.168.254.12 > co2061-13.ece.iastate.edu: ICMP echo request, id 21147, seq 153, length 64
14:36:07.999326 IP co2061-13.ece.iastate.edu > 192.168.254.12: ICMP echo reply, id 21147, seq 153, length 64
14:36:08.999571 IP 192.168.254.12 > co2061-13.ece.iastate.edu: ICMP echo request, id 21147, seq 154, length 64
14:36:08.999632 IP co2061-13.ece.iastate.edu > 192.168.254.12: ICMP echo reply, id 21147, seq 154, length 64
14:36:10.000779 IP 192.168.254.12 > co2061-13.ece.iastate.edu: ICMP echo request, id 21147, seq 155, length 64
14:36:10.000830 IP co2061-13.ece.iastate.edu > 192.168.254.12: ICMP echo reply, id 21147, seq 155, length 64
14:36:11.002025 IP 192.168.254.12 > co2061-13.ece.iastate.edu: ICMP echo request, id 21147, seq 156, length 64
14:36:11.002071 IP co2061-13.ece.iastate.edu > 192.168.254.12: ICMP echo reply, id 21147, seq 156, length 64
14:36:12.002520 IP 192.168.254.12 > co2061-13.ece.iastate.edu: ICMP echo request, id 21147, seq 157, length 64
14:36:12.002572 IP co2061-13.ece.iastate.edu > 192.168.254.12: ICMP echo reply, id 21147, seq 157, length 64
14:36:13.003857 IP 192.168.254.12 > co2061-13.ece.iastate.edu: ICMP echo request, id 21147, seq 158, length 64
14:36:13.003915 IP co2061-13.ece.iastate.edu > 192.168.254.12: ICMP echo reply, id 21147, seq 158, length 64
14:36:14.004659 IP 192.168.254.12 > co2061-13.ece.iastate.edu: ICMP echo request, id 21147, seq 159, length 64
14:36:14.004704 IP co2061-13.ece.iastate.edu > 192.168.254.12: ICMP echo reply, id 21147, seq 159, length 64
14:36:15.005979 IP 192.168.254.12 > co2061-13.ece.iastate.edu: ICMP echo request, id 21147, seq 160, length 64
14:36:15.006025 IP co2061-13.ece.iastate.edu > 192.168.254.12: ICMP echo reply, id 21147, seq 160, length 64
14:36:16.007057 IP 192.168.254.12 > co2061-13.ece.iastate.edu: ICMP echo request, id 21147, seq 161, length 64
14:36:16.007106 IP co2061-13.ece.iastate.edu > 192.168.254.12: ICMP echo reply, id 21147, seq 161, length 64
14:36:17.008310 IP 192.168.254.12 > co2061-13.ece.iastate.edu: ICMP echo request, id 21147, seq 162, length 64
14:36:17.008359 IP co2061-13.ece.iastate.edu > 192.168.254.12: ICMP echo reply, id 21147, seq 162, length 64
14:36:18.008632 IP 192.168.254.12 > co2061-13.ece.iastate.edu: ICMP echo request, id 21147, seq 163, length 64
14:36:18.008685 IP co2061-13.ece.iastate.edu > 192.168.254.12: ICMP echo reply, id 21147, seq 163, length 64
14:36:19.009498 IP 192.168.254.12 > co2061-13.ece.iastate.edu: ICMP echo request, id 21147, seq 164, length 64
14:36:19.009548 IP co2061-13.ece.iastate.edu > 192.168.254.12: ICMP echo reply, id 21147, seq 164, length 64
14:36:20.010665 IP 192.168.254.12 > co2061-13.ece.iastate.edu: ICMP echo request, id 21147, seq 165, length 64
14:36:20.010717 IP co2061-13.ece.iastate.edu > 192.168.254.12: ICMP echo reply, id 21147, seq 165, length 64
14:36:21.012004 IP 192.168.254.12 > co2061-13.ece.iastate.edu: ICMP echo request, id 21147, seq 166, length 64
14:36:21.012051 IP co2061-13.ece.iastate.edu > 192.168.254.12: ICMP echo reply, id 21147, seq 166, length 64
^C
36 packets captured
36 packets received by filter
0 packets dropped by kernel
[489labuser@co2061-13 ~]$
```

12) Use tcpdump to capture packets and save the data to a dump file. While you are capturing, make HTTP connections to the following machines:

www.iastate.edu
www.google.com

In order to generate HTTP connections, open a web browser such as Firefox on the command line with, for instance, firefox www.google.com.
Use tcptrace to analyze the output of tcpdump. Identify the following information:

a. Source and destination IP addresses and port numbers of the TCP connections.

→ 1: co2061-13.ece.iastate.edu:45580 -
ec2-3-230-67-66.compute-1.amazonaws.com:443 (a2b)   6>   5<

2: co2061-13.ece.iastate.edu:58198 -
ec2-3-232-171-121.compute-1.amazonaws.com:443 (c2d)   2>   1<

3: co2061-13.ece.iastate.edu:912 - h10.ece.iastate.edu:2049 (e2f) 1>   1<

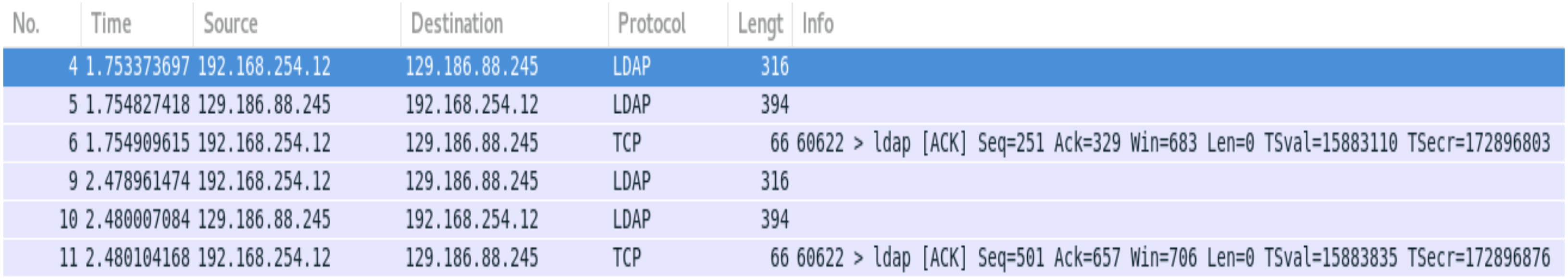
b. Duration of TCP connections.

→ TCP Connection 1: Elapsed time = 0:00:01.098184
TCP Connection 2: Elapsed time = 0:00:00.030994
TCP Connection 3: Elapsed time = 0:00:00.000916

c. Total number of packets sent from your machine to each server.

→ TCP Connection 1: Total packets: 11
TCP Connection 2: Total packets: 3
TCP Connection 3: Total packets: 2

13) Continuing the tcpdump example, your computer is still under a ping flood (ICMP request and reply packets). Start a new capture, and let it run for about 10 seconds.



No.	Time	Source	Destination	Protocol	Lengt	Info
4	1.753373697	192.168.254.12	129.186.88.245	LDAP	316	
5	1.754827418	129.186.88.245	192.168.254.12	LDAP	394	
6	1.754909615	192.168.254.12	129.186.88.245	TCP	66	60622 > ldap [ACK] Seq=251 Ack=329 Win=683 Len=0 TSval=15883110 TSecr=172896803
9	2.478961474	192.168.254.12	129.186.88.245	LDAP	316	
10	2.480007084	129.186.88.245	192.168.254.12	LDAP	394	
11	2.480104168	192.168.254.12	129.186.88.245	TCP	66	60622 > ldap [ACK] Seq=501 Ack=657 Win=706 Len=0 TSval=15883835 TSecr=172896876

- **Determine how much data (in bytes) each ICMP packet contains.**

-> Length column shows the data in bytes for each ICMP packet

- **Determine the arrival time for each ping request packet.**

-> Arrival time is shown under the time column

14) Start a new capture, and let it run while you complete a traceroute and tcptraceroute to www.ebay.com.

- **What types of packets are sent with traceroute?**

-> ICMP, DNS, LDAP, TCP, UDP packets

- **What types of packets are sent with tcptraceroute?**

-> UDP, ARP, ICMP, LDAP, DNS, MDNS, TCP packets