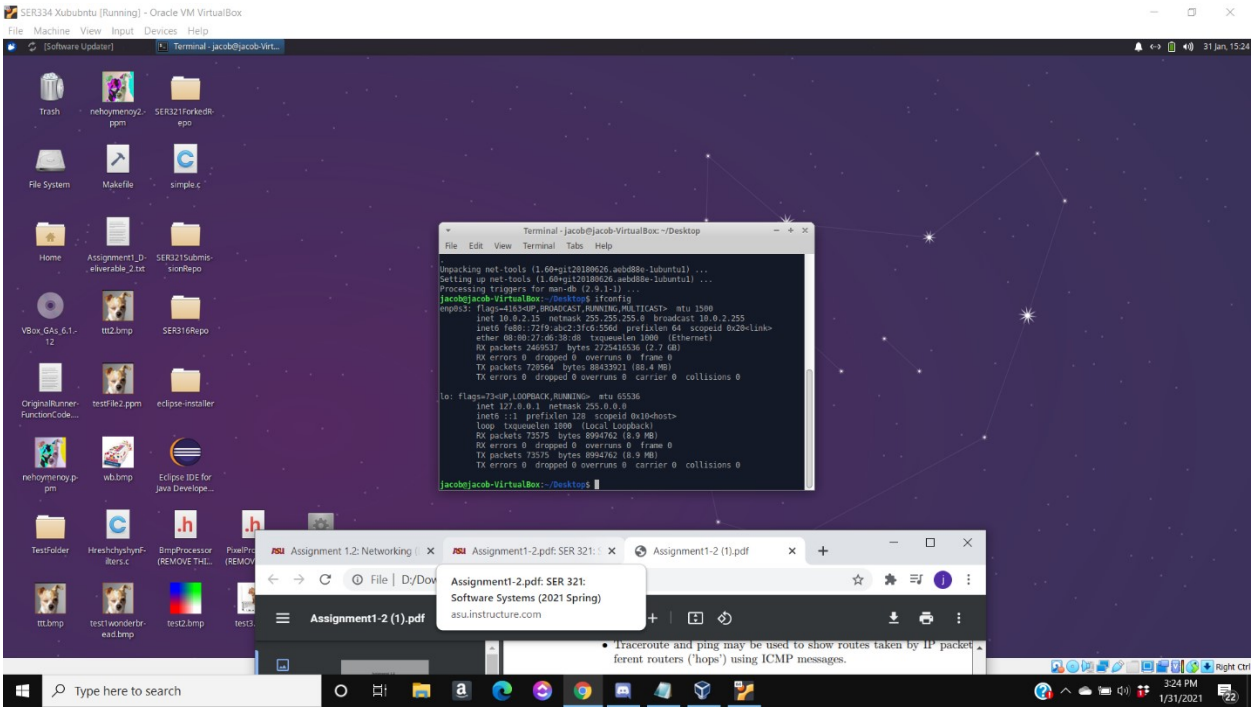
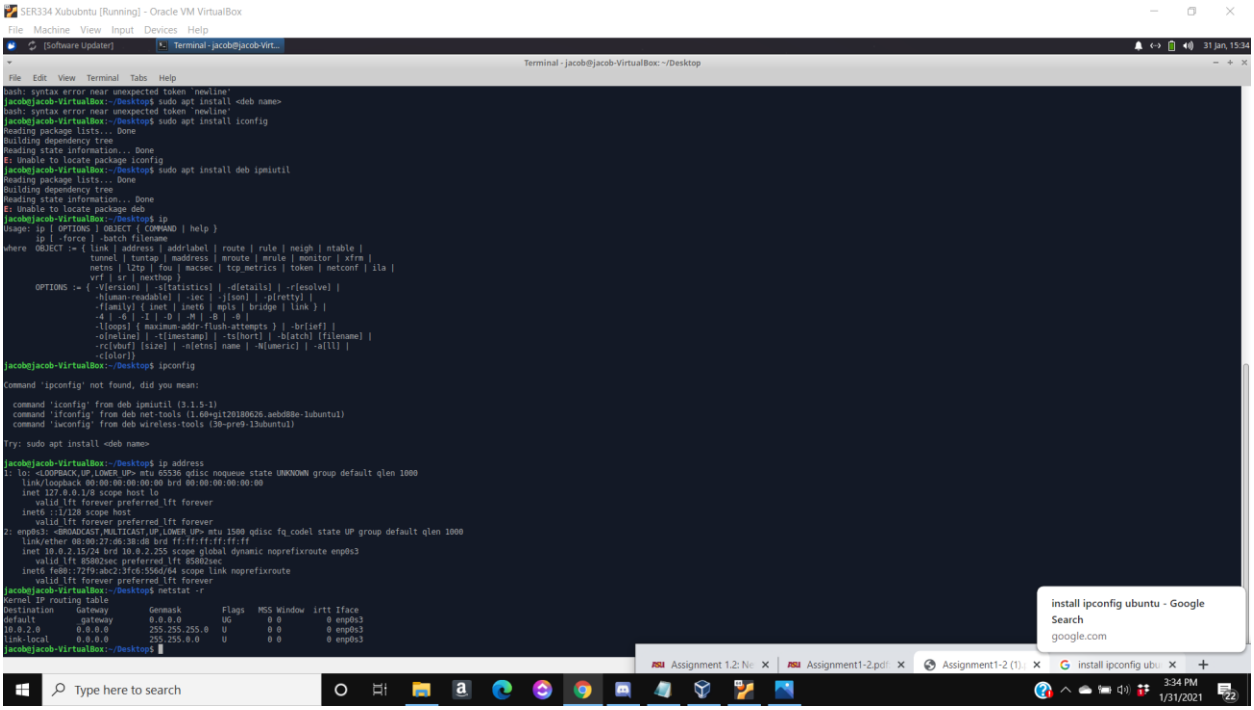
Task 1.1

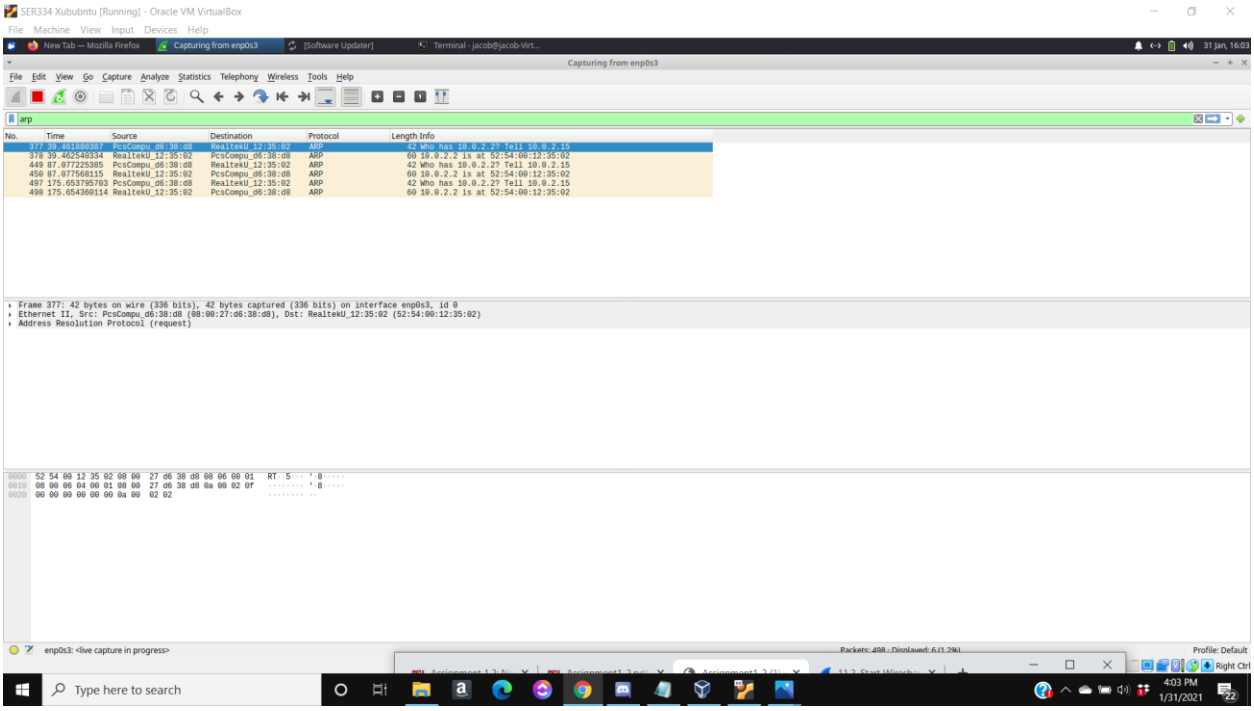
Step 1:

Finding network interface and gateway.

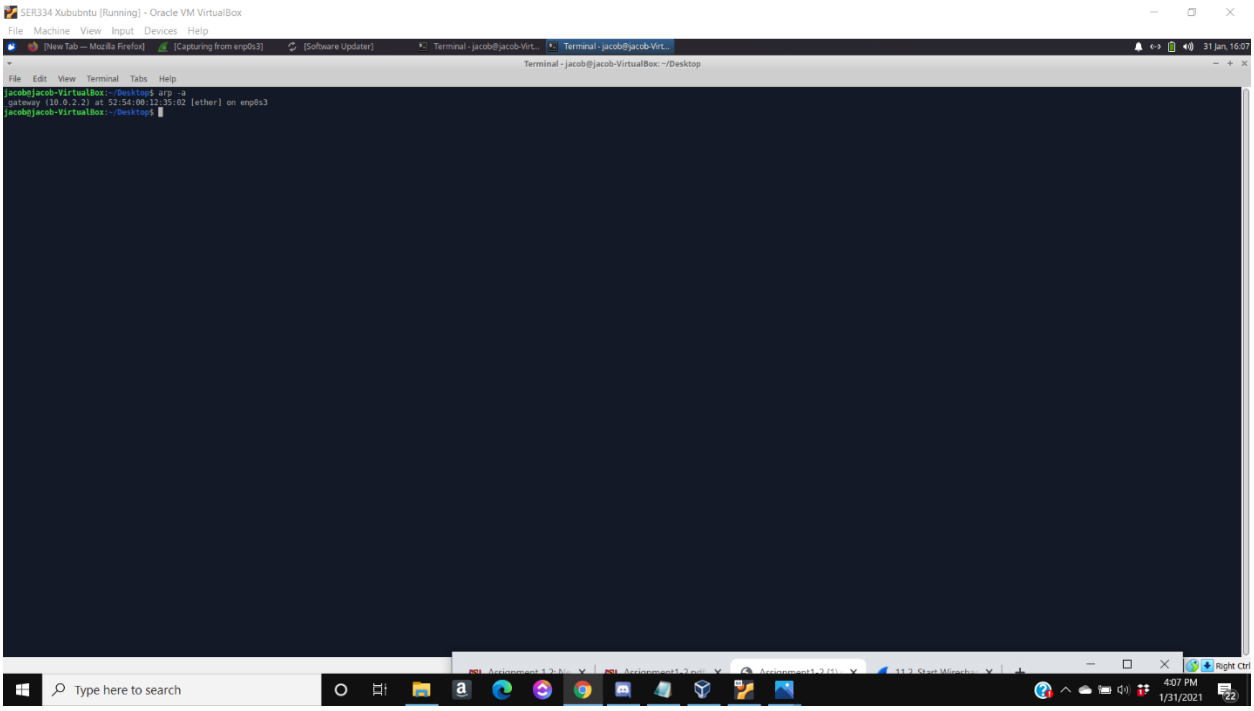


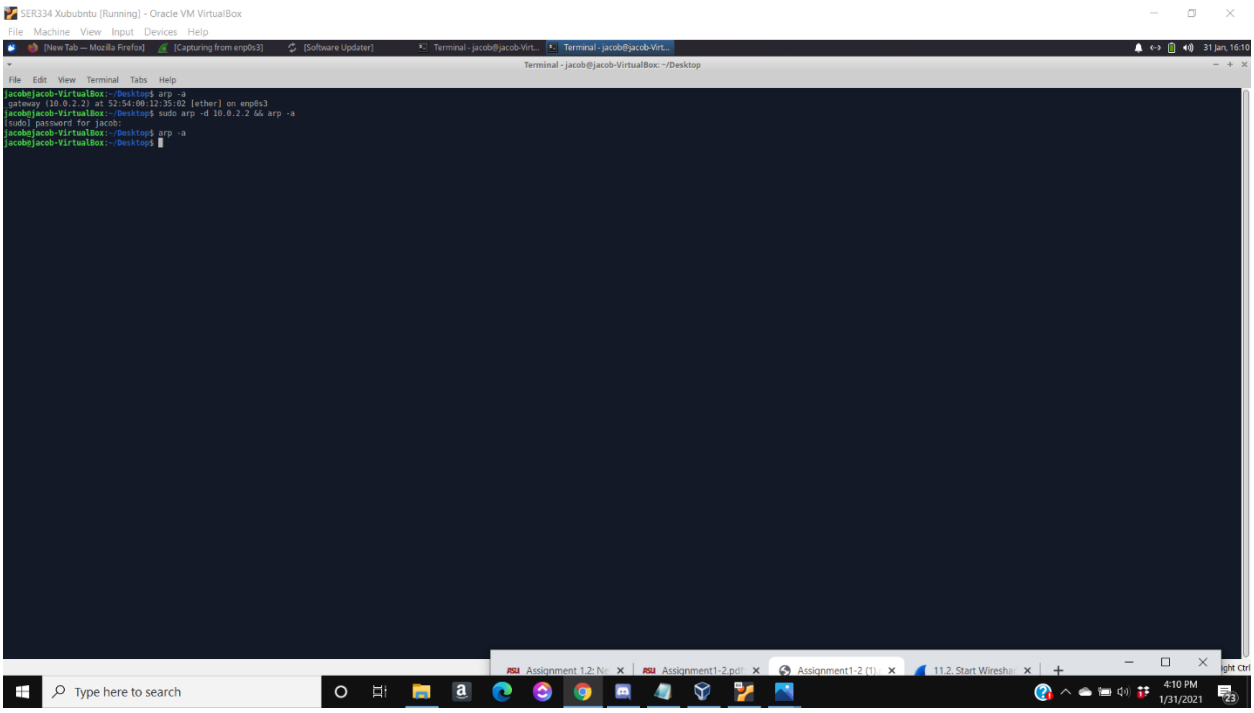


Wireshark with ARP filters.

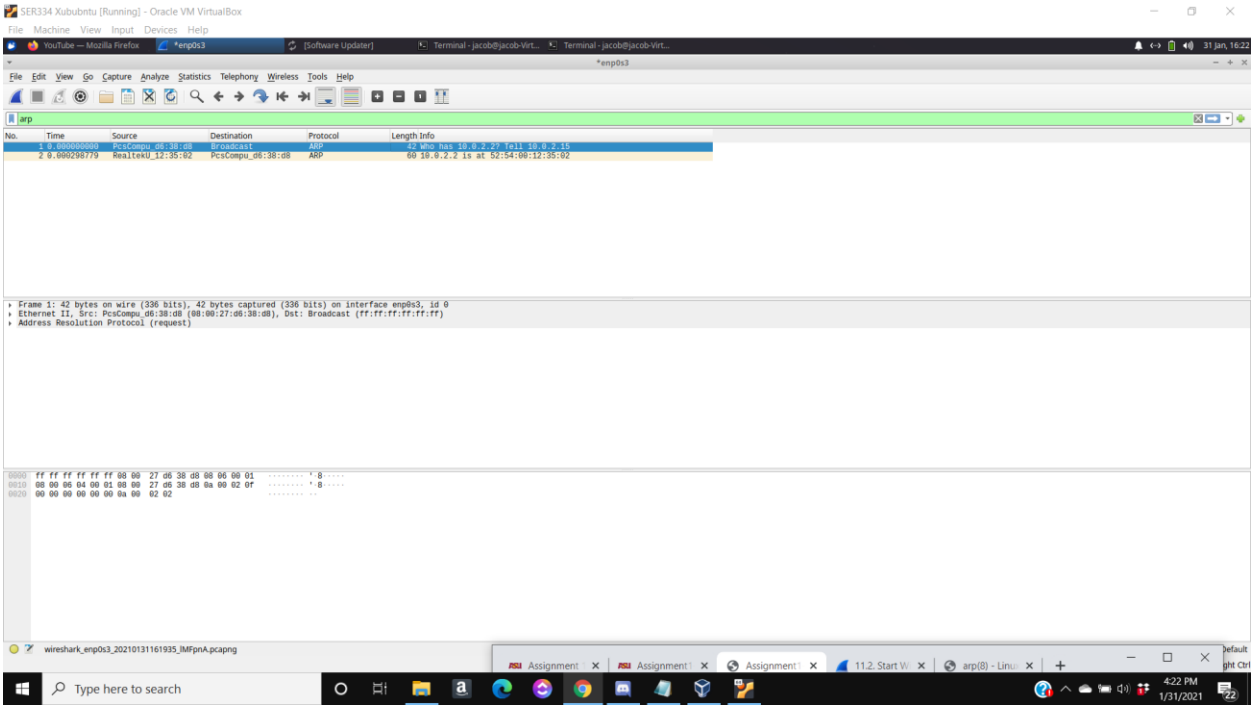


ARP commands.



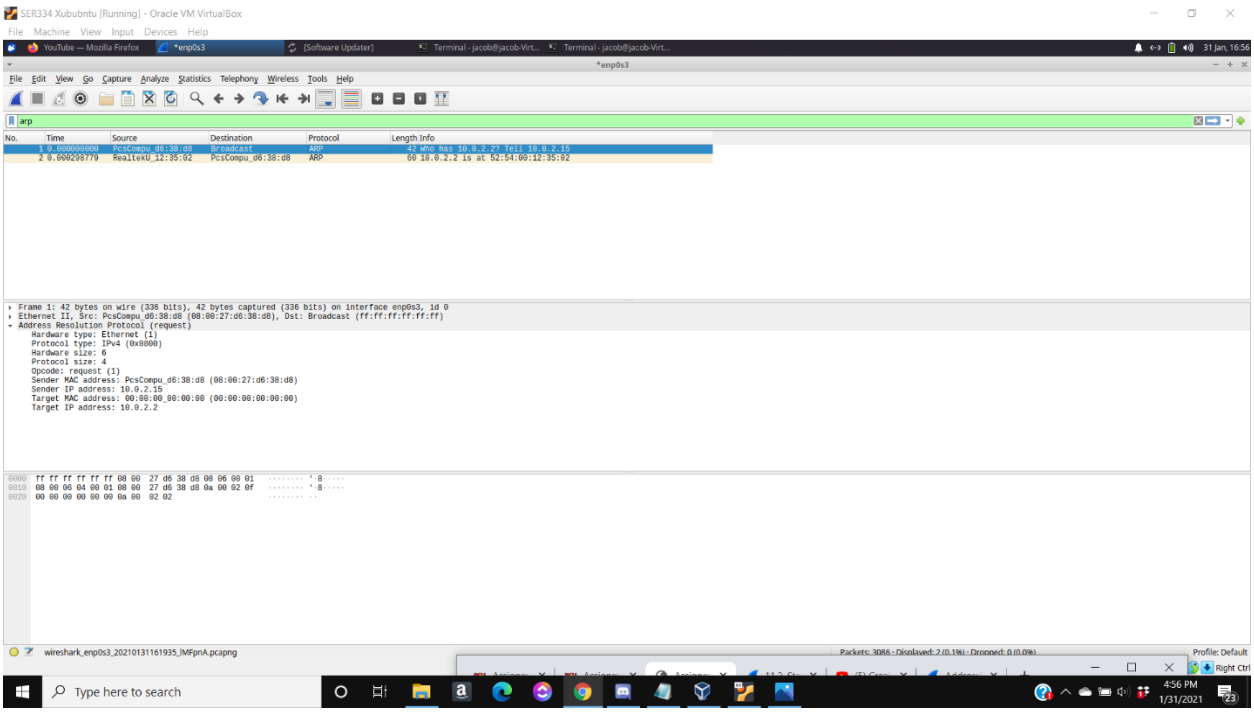


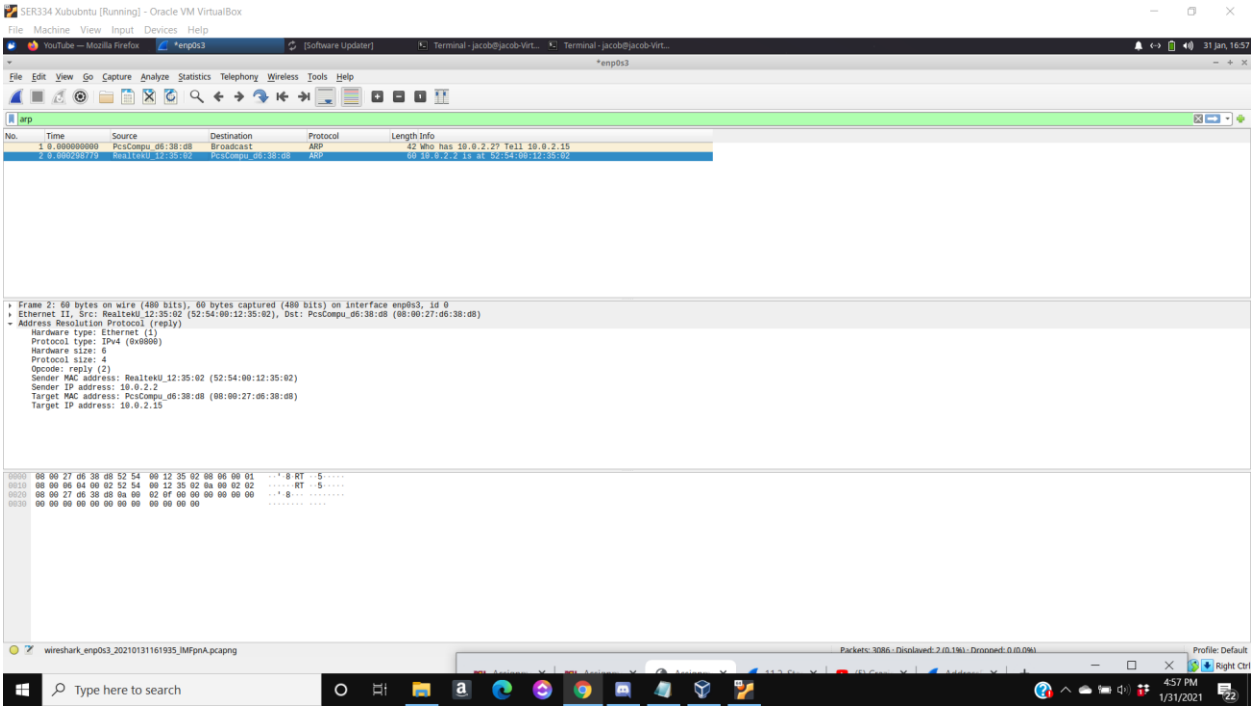
Updated Wireshark trace.



Step 2:

ARP request and reply.





Step 3:

1. What opcode is used to indicate a request? What about a reply?

1 is used to indicate a request. 2 is used to indicate a reply.

2. How large is the ARP header for a request? What about for a reply?

For both a request and a reply, the ARP header size is 28 bytes.

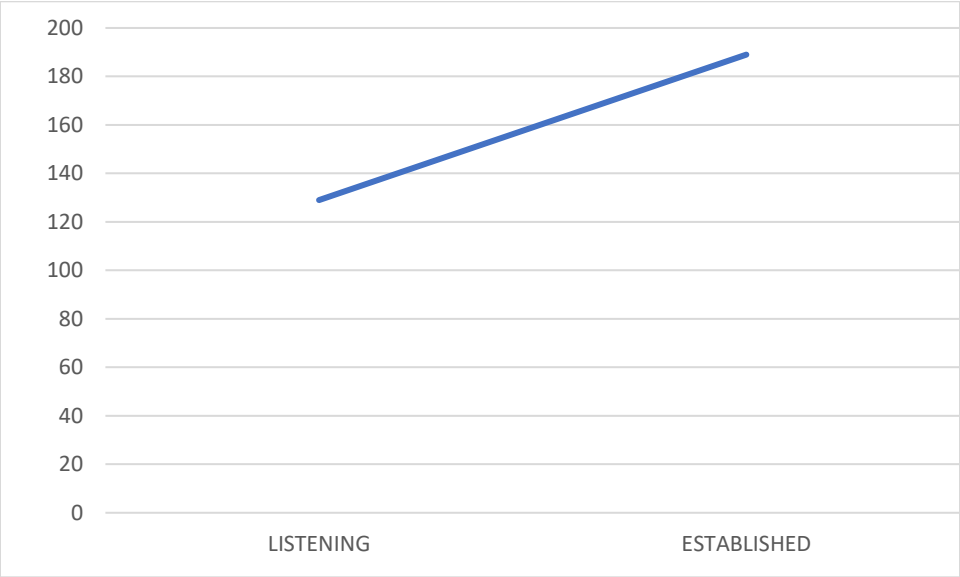
3. What value is carried on request for the unknown target MAC address?

The value 00:00:00_00:00:00 is carried on request for the unknown target MAC address.

4. What Ethernet Type value indicates that ARP is the higher layer protocol?

The value is 0x0806.

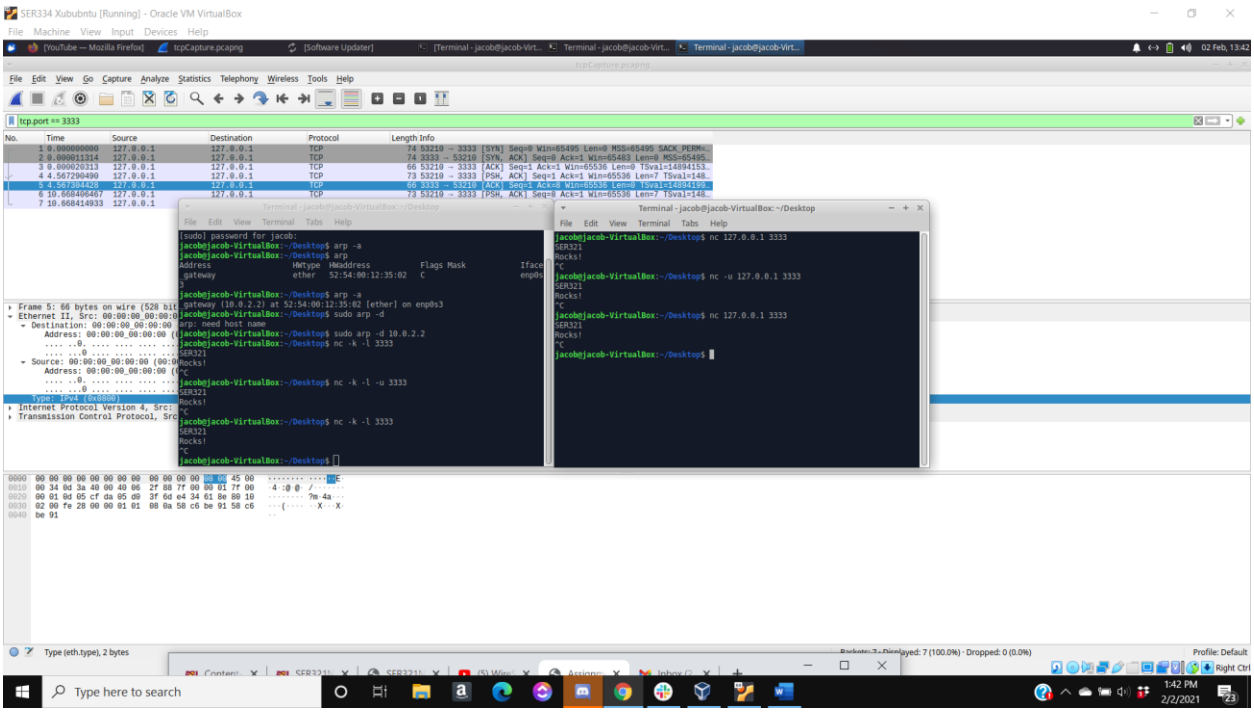
Task 1.2



This is a simplified line graph of the socket connections. The raw data can be found in the excel spreadsheet. Connection data was collected over 10 minutes. Worth noting that this data was collected via the Windows Command Line.

Task 1.3

Step 1 TCP:



1. How many frames were needed to capture those 2 lines?

2 frames were needed to capture the 2 lines.

2. How many packets were needed to capture those 2 lines?

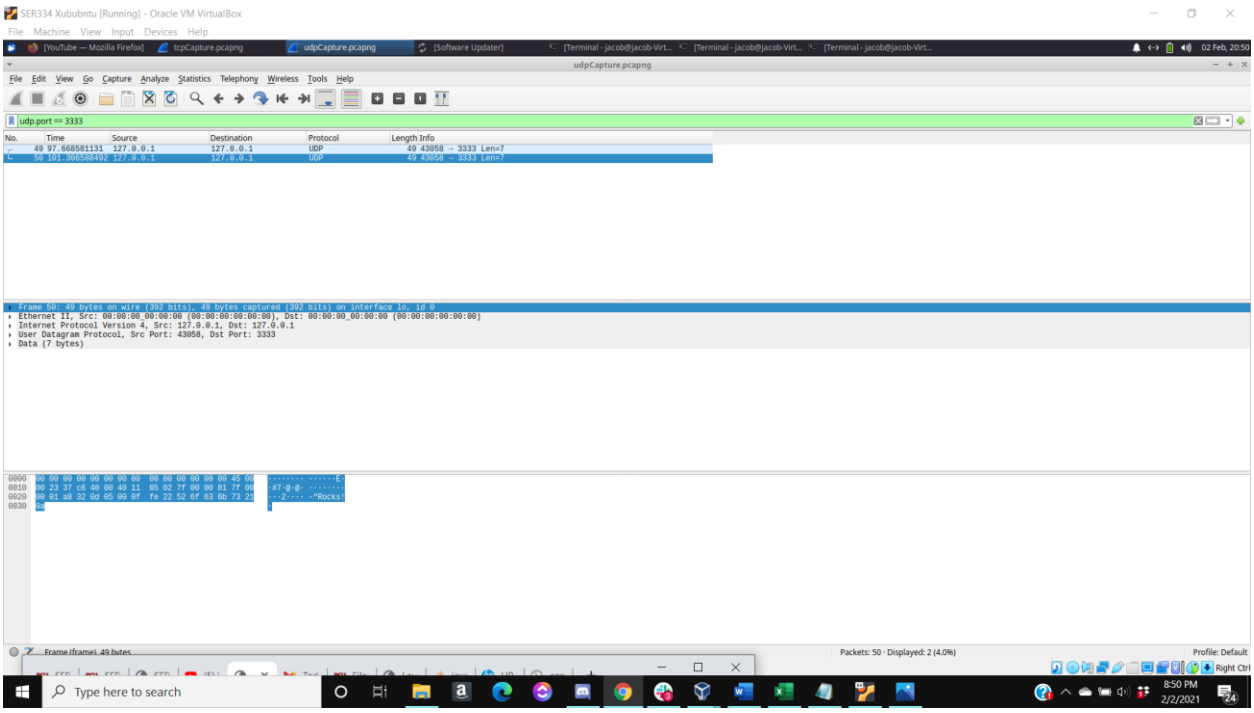
2 packets were needed to capture the 2 lines.

3. How many total bytes went over the wire? How much overhead was there (basically the percentage of traffic that was not needed to send SER321 Rocks!)?

Over all the 7 frames used in the traffic, 492 bytes were sent over the wire. Only 146 bytes were needed to contain the message, meaning less than 30% of the traffic was needed.

Step 2 UDP:

UDP commands shown in above picture. Below is the Wireshark capture of the UDP trace.



1. How many frames were needed to capture those 2 lines?

2 frames were needed to capture those 2 lines.

2. How many packets were needed to capture those 2 lines?

2 packets were needed to capture those 2 lines.

3. How many total bytes went over the wire? How much overhead was there (basically the percentage of traffic that was not needed to send SER321 Rocks!)?

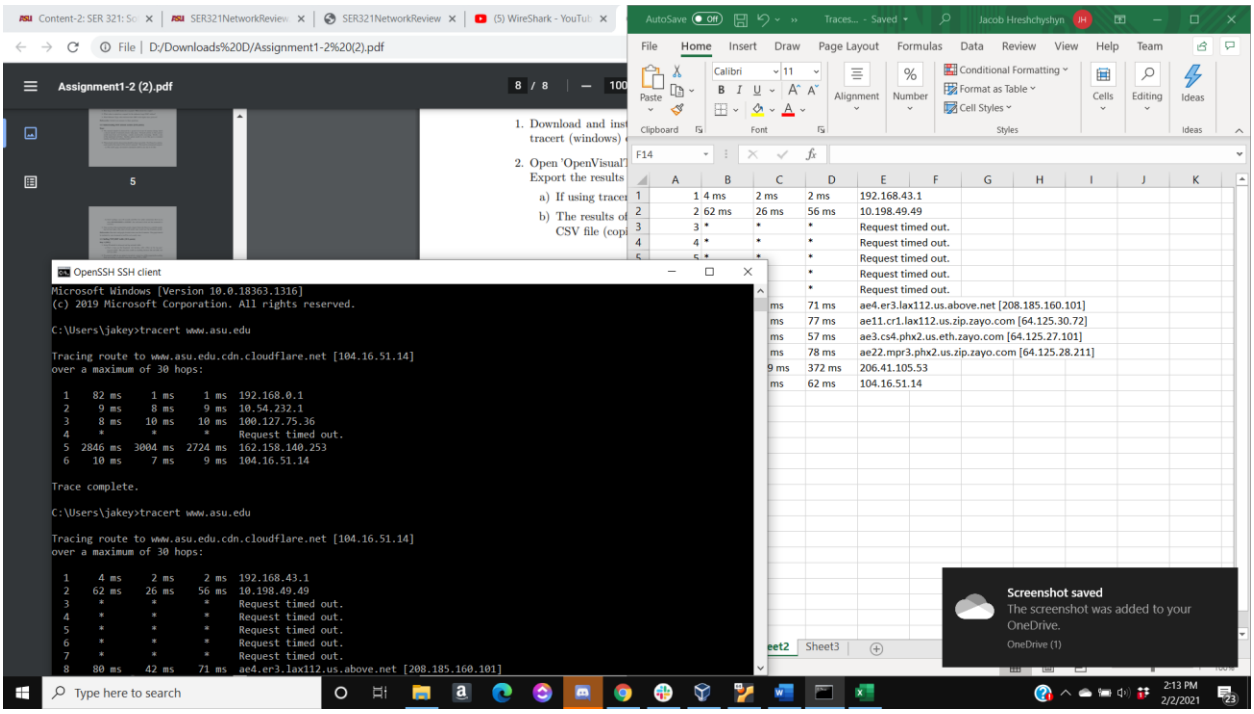
98 total bytes were sent over the wire, none of which was wasted in sending the message over the wire.

4. What is the difference in relative overhead between UDP and TCP and why? Specifically, what kind of information was exchanged in TCP that was not exchanged in UDP? Show the relative parts of the packet traces.

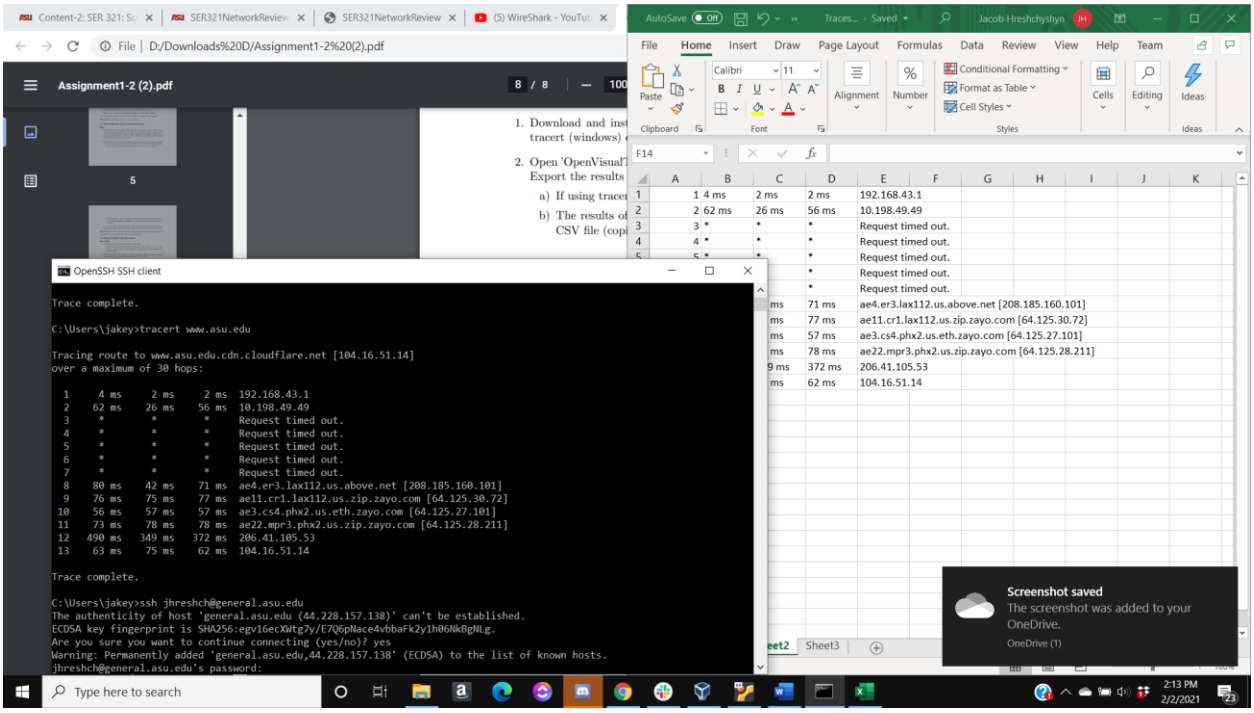
Much more overhead exists with the TCP trace as opposed to the UDP trace. Much of this overhead is the result of TCP's measures to ensure that the data is not lost when it is sent over the wire. The overhead presents itself first in the 3-way handshake with the [SYN], [SYN, ACK], and [ACK] frames. Once data is sent over the wire, an additional frame is sent to acknowledge reception of the data.

Task 1.4:

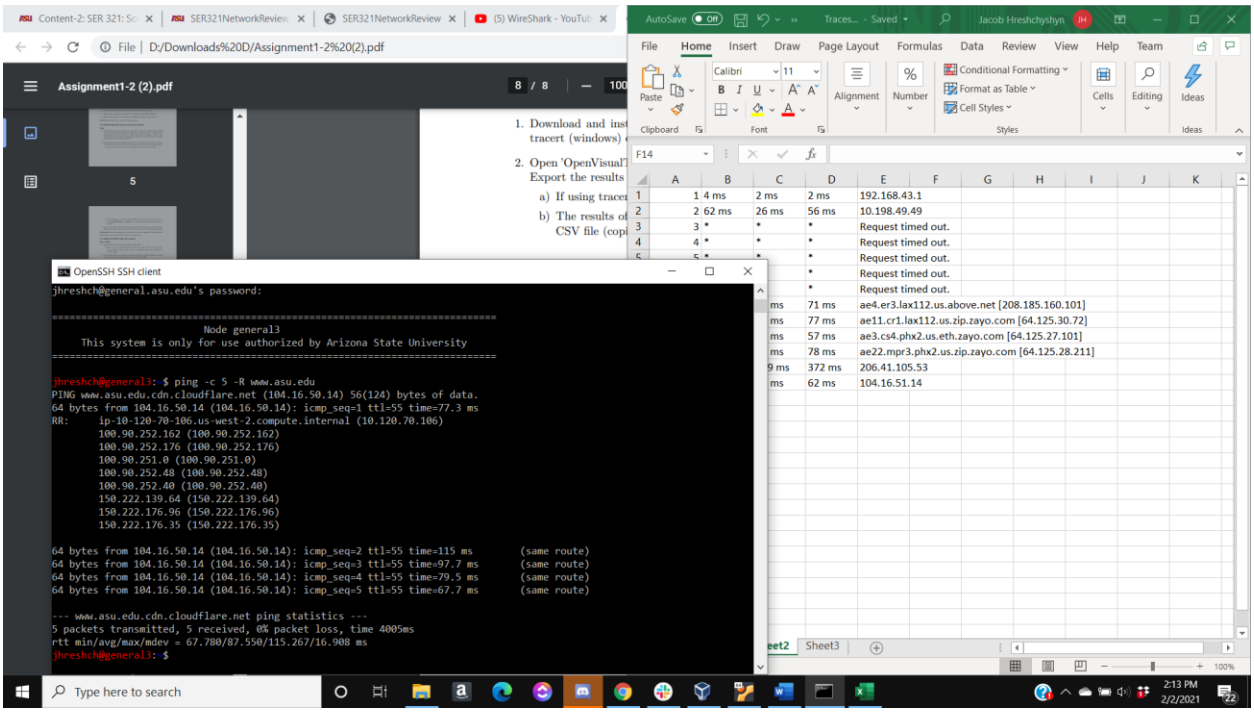
Local network.



Mobile hotspot.


Assignment1-2 (2).pdf
OpenSSH SSH client
Trace complete.
C:\Users\jakey>tracert www.asu.edu
Tracing route to www.asu.edu.cdn.cloudflare.net [104.16.51.14]
over a maximum of 30 hops:
1 4 ms 2 ms 2 ms 192.168.43.1
2 62 ms 26 ms 56 ms 10.198.49.49
3 * * * Request timed out.
4 * * * Request timed out.
5 * * * Request timed out.
6 * * * Request timed out.
7 * * * Request timed out.
8 80 ms 42 ms 71 ms ae4.er3.lax112.us.above.net [208.185.160.101]
9 76 ms 75 ms 77 ms ae11.cr1.lax112.us.zip.zayo.com [64.125.30.72]
10 56 ms 57 ms 57 ms ae3.cs4.phx2.us.eth.zayo.com [64.125.27.101]
11 73 ms 78 ms 78 ms ae22.mpr3.phx2.us.zip.zayo.com [64.125.28.211]
12 490 ms 349 ms 372 ms 206.41.105.53
13 63 ms 75 ms 62 ms 104.16.51.14
Trace complete.
C:\Users\jakey>ssh jhreshch@general.asu.edu
The authenticity of host 'general.asu.edu (44.228.157.138)' can't be established.
ECDSA key fingerprint is SHA256:egv16ecXWtg7y/E7Q6pNace4vbbaFk2y1h06NkBgNLg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'general.asu.edu,44.228.157.138' (ECDSA) to the list of known hosts.
jhreshch@general.asu.edu's password:
Screenshot saved
The screenshot was added to your OneDrive.
OneDrive (1)

SSH.


Assignment1-2 (2).pdf
OpenSSH SSH client
jhreshch@general.asu.edu's password:
Node general3
This system is only for use authorized by Arizona State University
jhreshch@general3:~$ ping -c 5 -R www.asu.edu
PING www.asu.edu.cdn.cloudflare.net (104.16.50.14) 56(124) bytes of data.
64 bytes from 104.16.50.14 (104.16.50.14): icmp_seq=1 ttl=55 time=77.3 ms
RR: ip-10-120-70-106.us-west-2.compute.internal (10.120.70.106)
100.90.252.162 (100.90.252.162)
100.90.252.176 (100.90.252.176)
100.90.251.0 (100.90.251.0)
100.90.252.48 (100.90.252.48)
100.90.252.40 (100.90.252.40)
150.222.139.64 (150.222.139.64)
150.222.176.96 (150.222.176.96)
150.222.176.35 (150.222.176.35)
64 bytes from 104.16.50.14 (104.16.50.14): icmp_seq=2 ttl=55 time=115 ms (same route)
64 bytes from 104.16.50.14 (104.16.50.14): icmp_seq=3 ttl=55 time=97.7 ms (same route)
64 bytes from 104.16.50.14 (104.16.50.14): icmp_seq=4 ttl=55 time=79.5 ms (same route)
64 bytes from 104.16.50.14 (104.16.50.14): icmp_seq=5 ttl=55 time=67.7 ms (same route)
--- www.asu.edu.cdn.cloudflare.net ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 67.780/87.550/115.267/16.908 ms
jhreshch@general3:~$

1. The SSH route appears to be the fastest with 5 packets being routed for a total of 433.2 ms while the mobile hotspot took 2383 ms with 15 timeouts and the local network taking 8738 ms with 3 timeouts.
2. The local network had the fewest hops with 6 hops while the mobile hotspot had 13 hops and the SSH route had 9.
3. The hotspot routing appears to run traffic through a bridge judging by its linking of various websites that eventually route to the final destination.