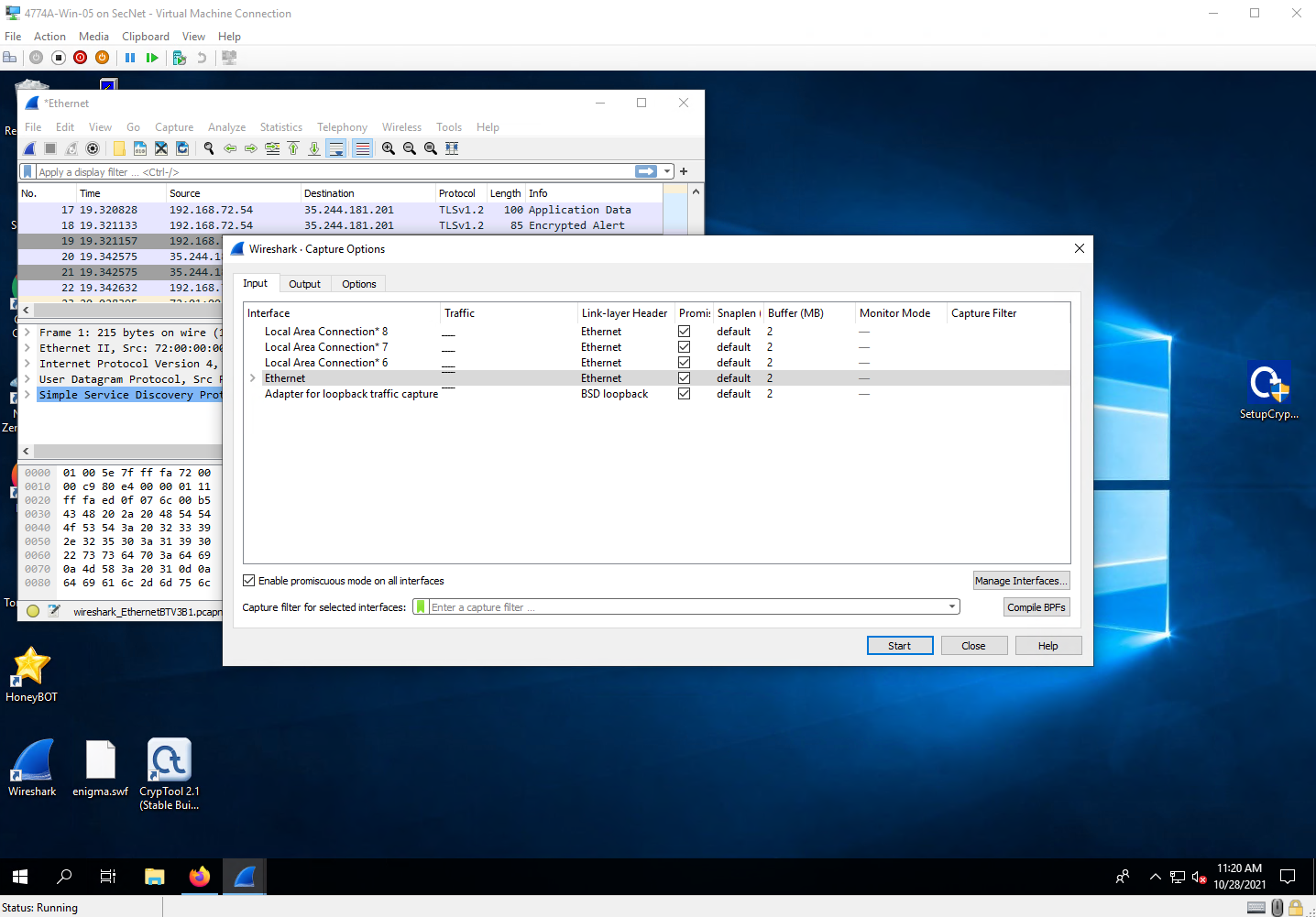
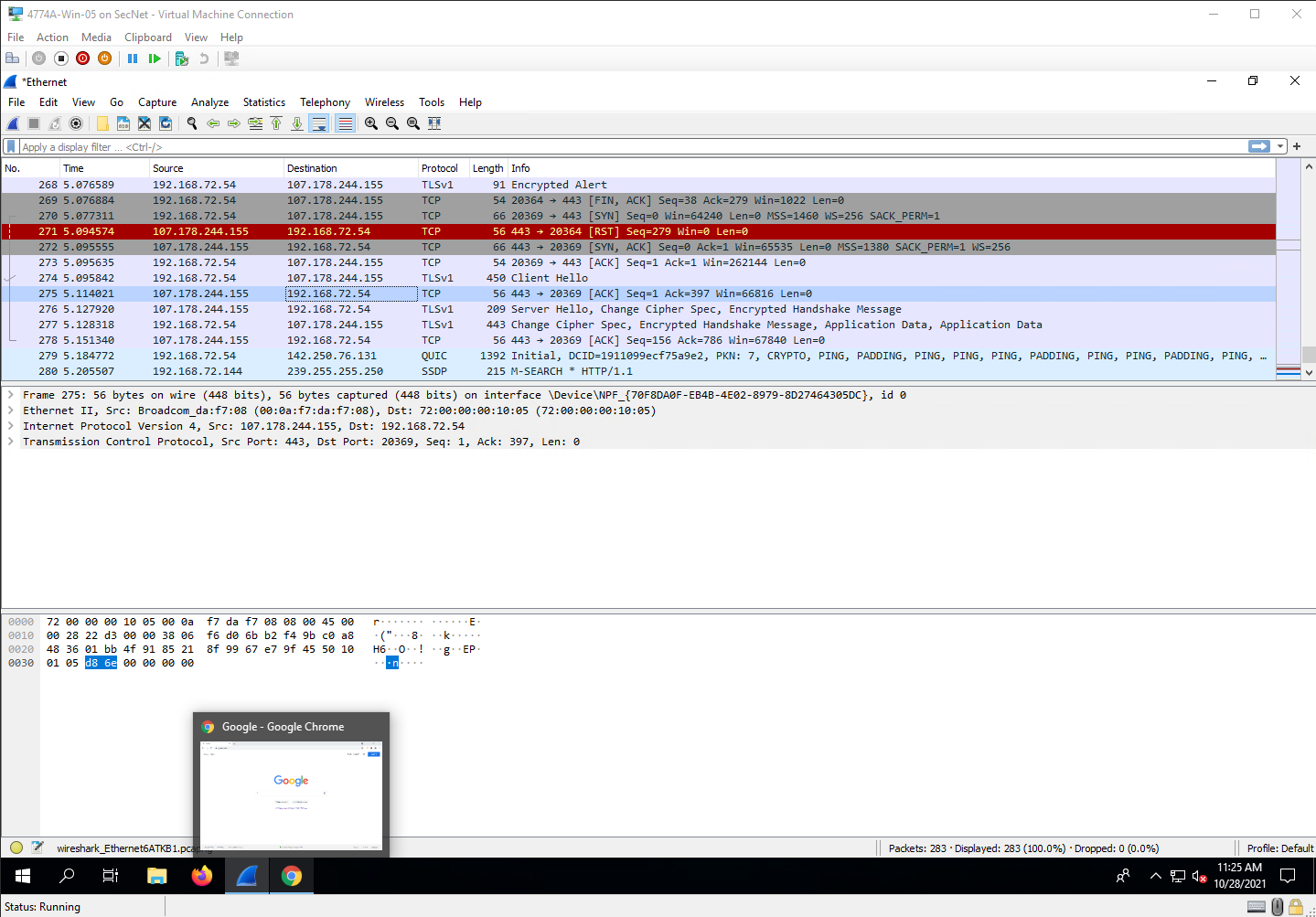
1 Wireshark I

Screenshots

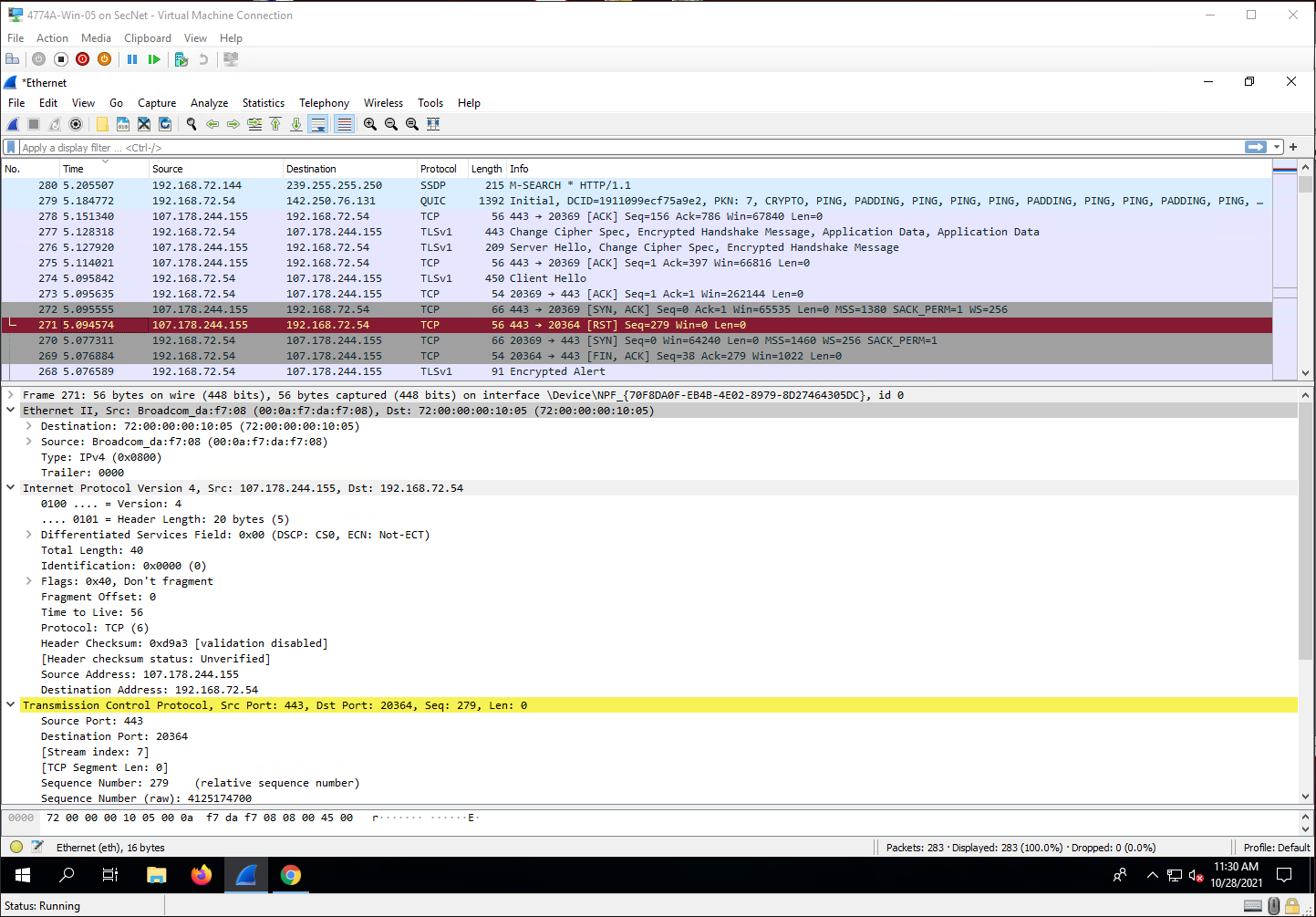
Step 17



Step 25



Step 30



Project Questions

1. My IP address is 192.168.72.54
2. One of the remote IP addresses my computer was communicating with was 107.178.244.155
3. I captured 280 packets
4. The blue entities are of the Simple Service Discovery Protocol (SSDP) and QUIC protocol types.

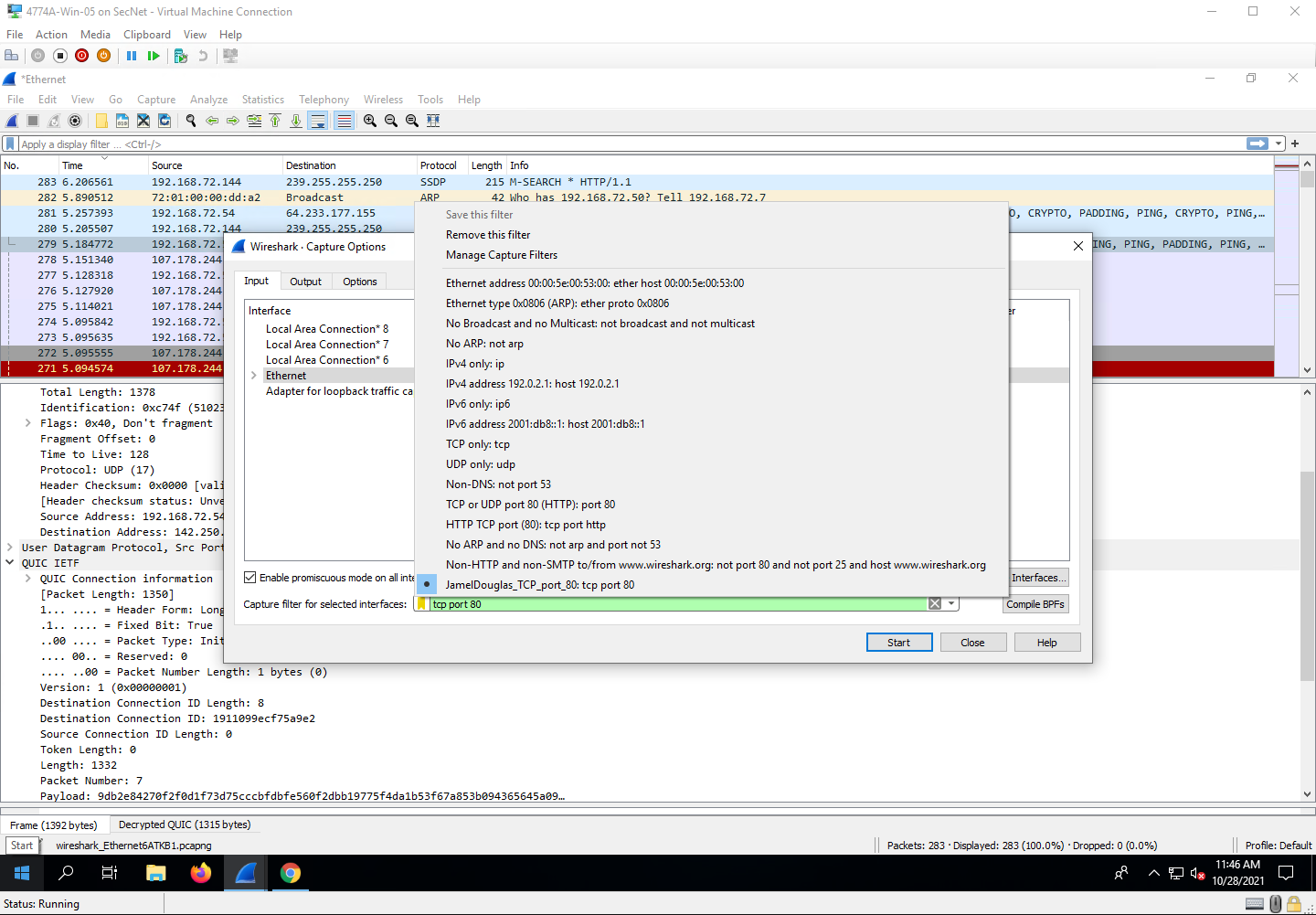
Thought Questions

1. The different colors represent different types of packets.
2. My computer sometimes got packets addressed for a machine with a different MAC address. These packets are broadcast packets and get sent to every machine on the network, the machine that it is meant for will then reply once it gets the packet.
3. The number of packets sent/received on a single mouse click depends on the content that is being displayed.
4. Yes, you can filter out specific packets so that only those ones a logged.

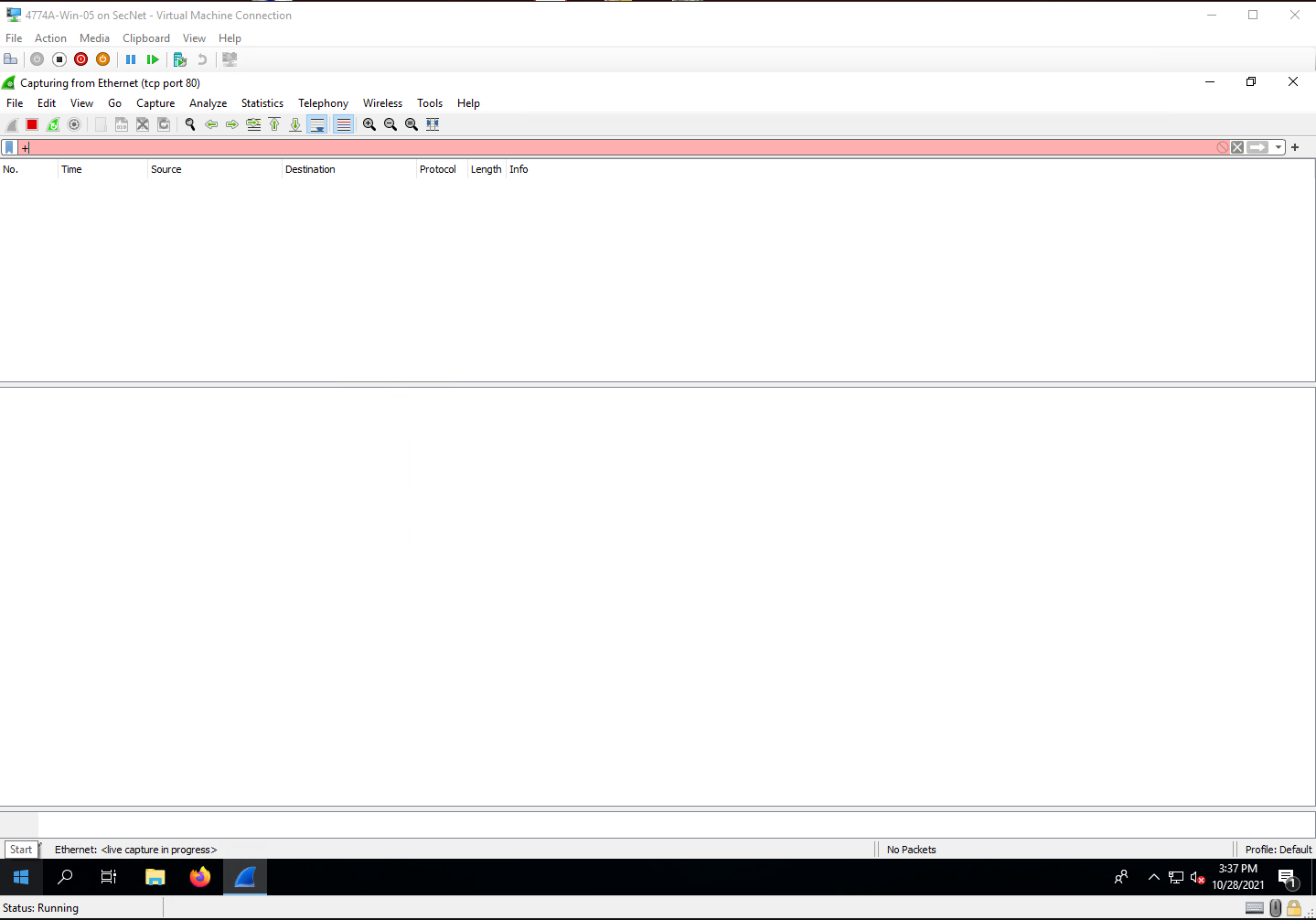
2 Wireshark II

Screenshots

Step 7



Step 20



Project Questions

1. I did not capture any packets. Sites now use encrypted protocols (HTTPS) to communicate, port 80 is pretty much obsolete.
2. I did not capture any packets; I was unable to determine the row number.
3. I did not capture any packets; I was not able to see the source port on a GET request.
4. My IP address is 192.168.72.54.

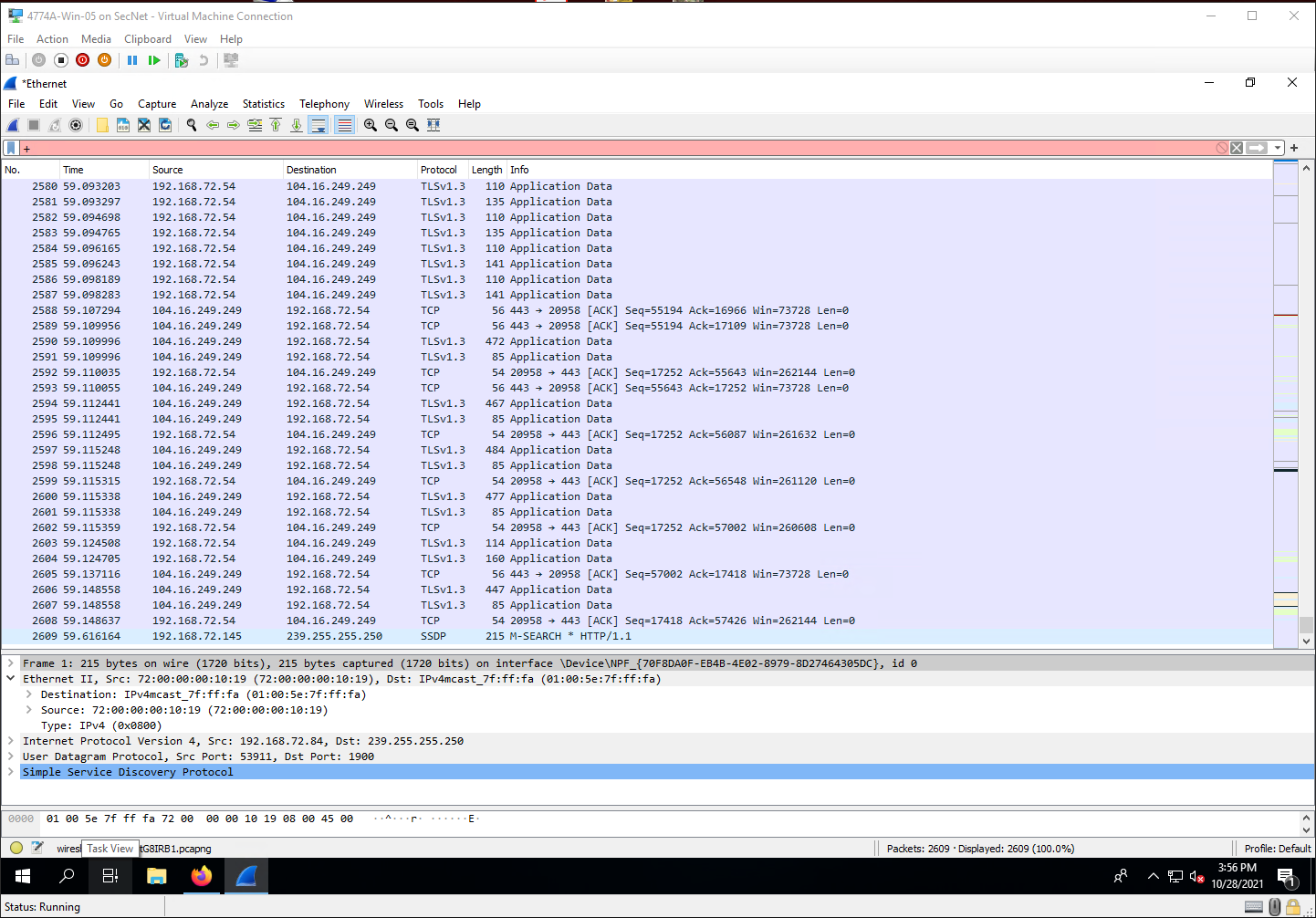
Thought Questions

1. Computers break up information into packets to send them because that is the most efficient way to transfer data. Sending data as one big packet could eat up all the available bandwidth.
2. SYN is used to initiate a connection. ACK is used to confirm that other side has received SYN. FIN is used to terminate connections. GET is an HTTP method that requests the specified resource.
3. Sequence numbers allow packets to be reconstructed in order if they were received out of order
4. My computer sends a packet to the webserver to establish a connection with it. It would also send a packet to request a certain resource, which in this case could be a home page.

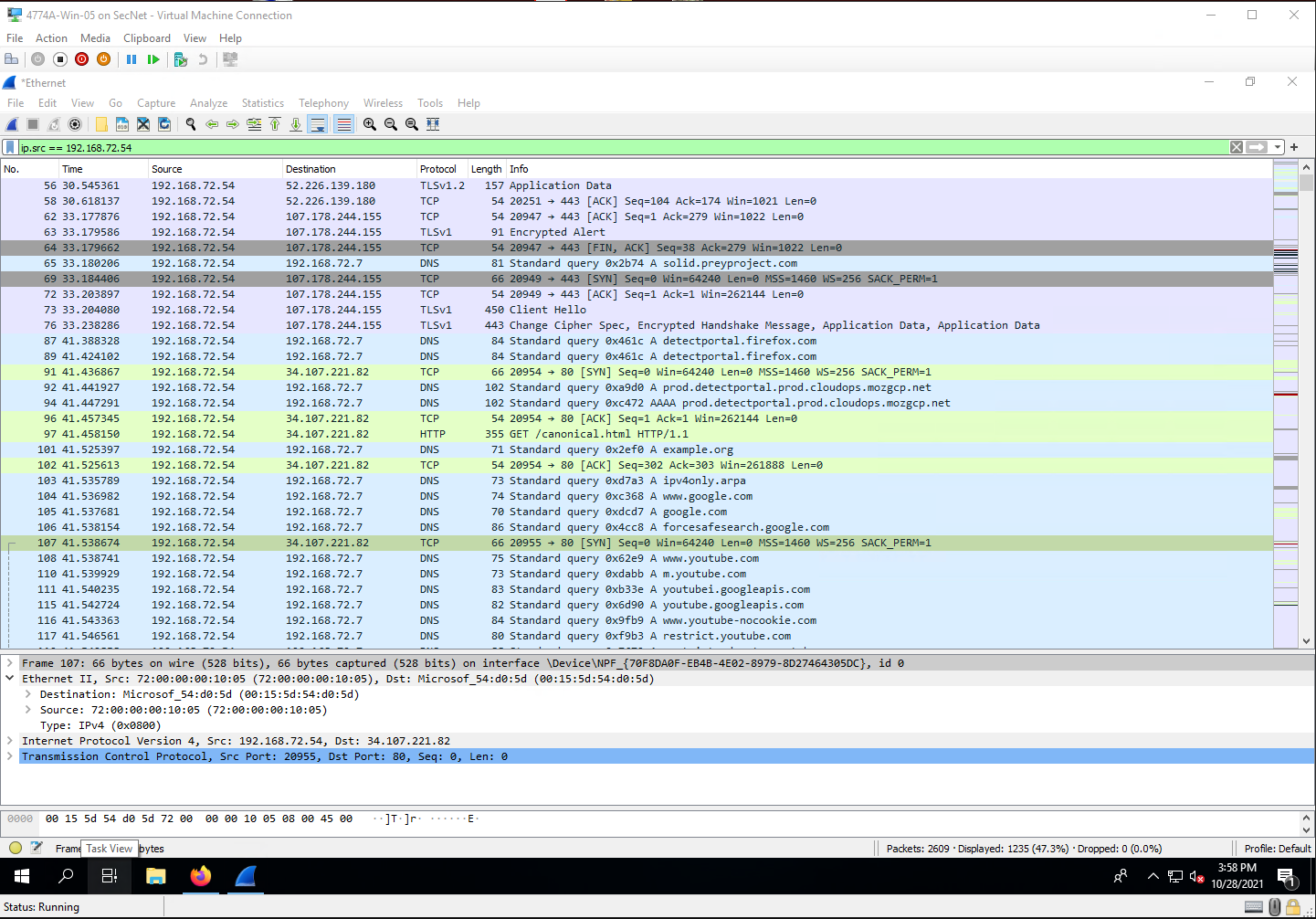
4 Wireshark IV

Screenshots

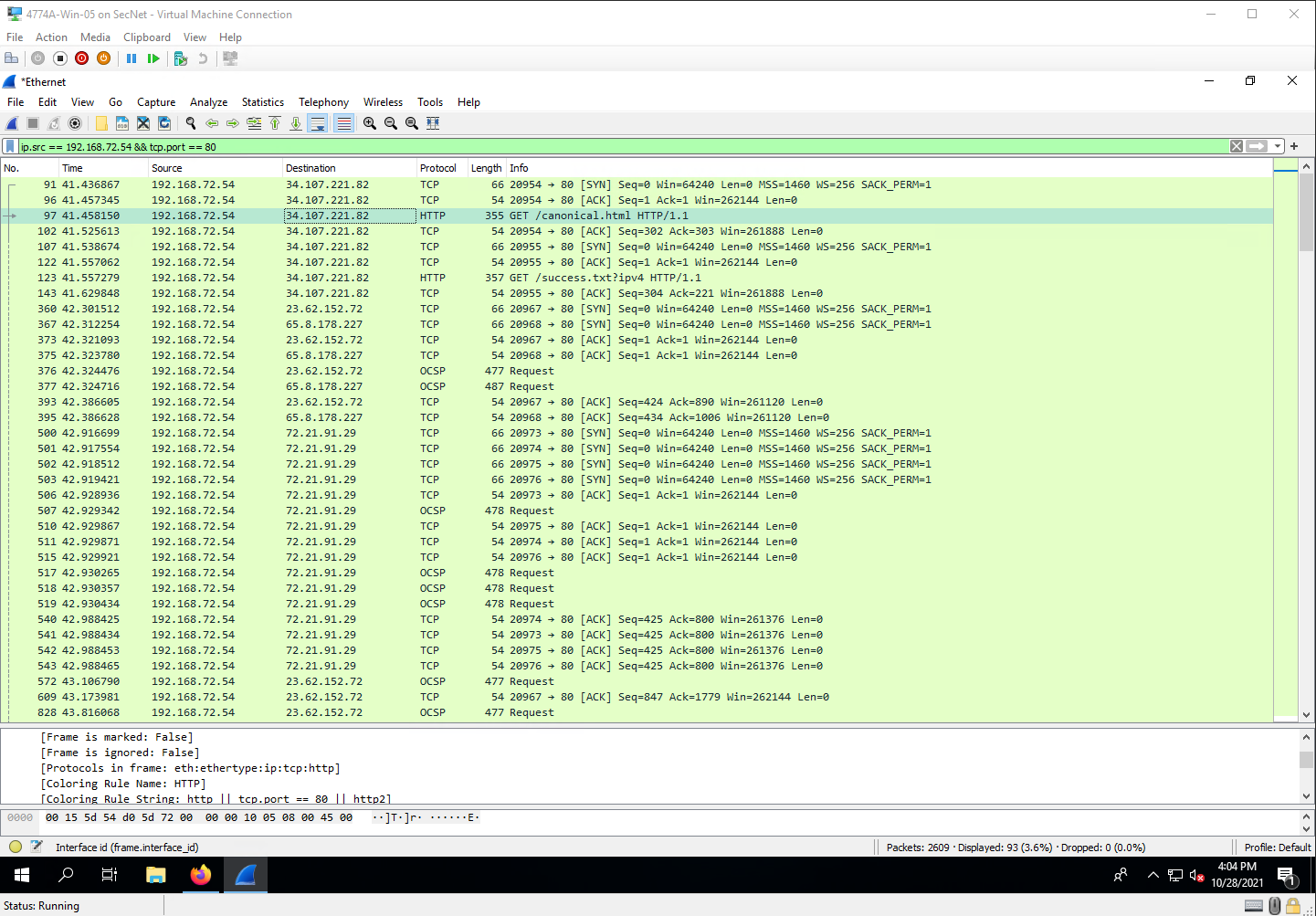
Step 10



Step 14



Step 24



Project Questions

1. My IP address is 192.168.72.54
2. I captured 2609 packets.
3. With the filters there were only 93 packets, meaning that 2516 packets were removed.
4. The most common destination IP address was 72.21.91.29.

Thought Questions

1. Yes, you would be able to filter a person’s traffic if you know their IP address and the type of packet that you are looking for.
2. There are many fields to filter because there are many different protocols, each having their own specific metadata that could be filtered out.
3. Another protocol used to manage traffic across networks is UDP.
4. The endpoint 104.16.249.249 was sent/received 794 packets during the scan.