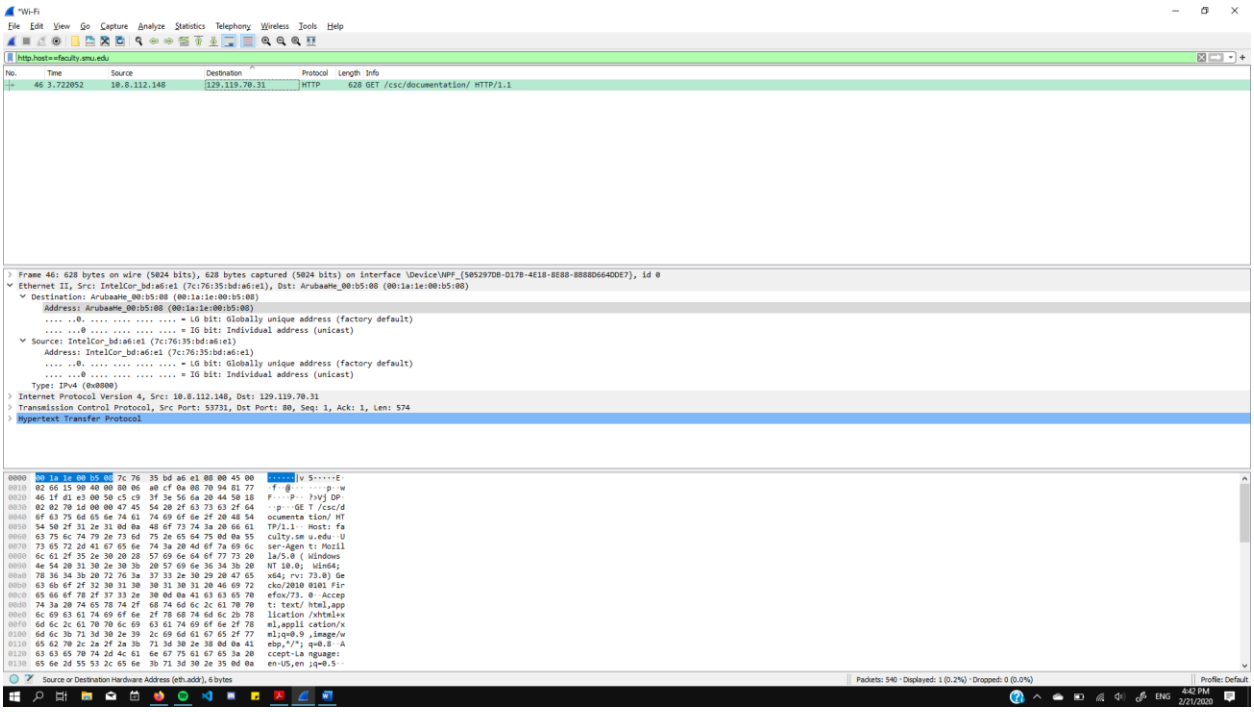
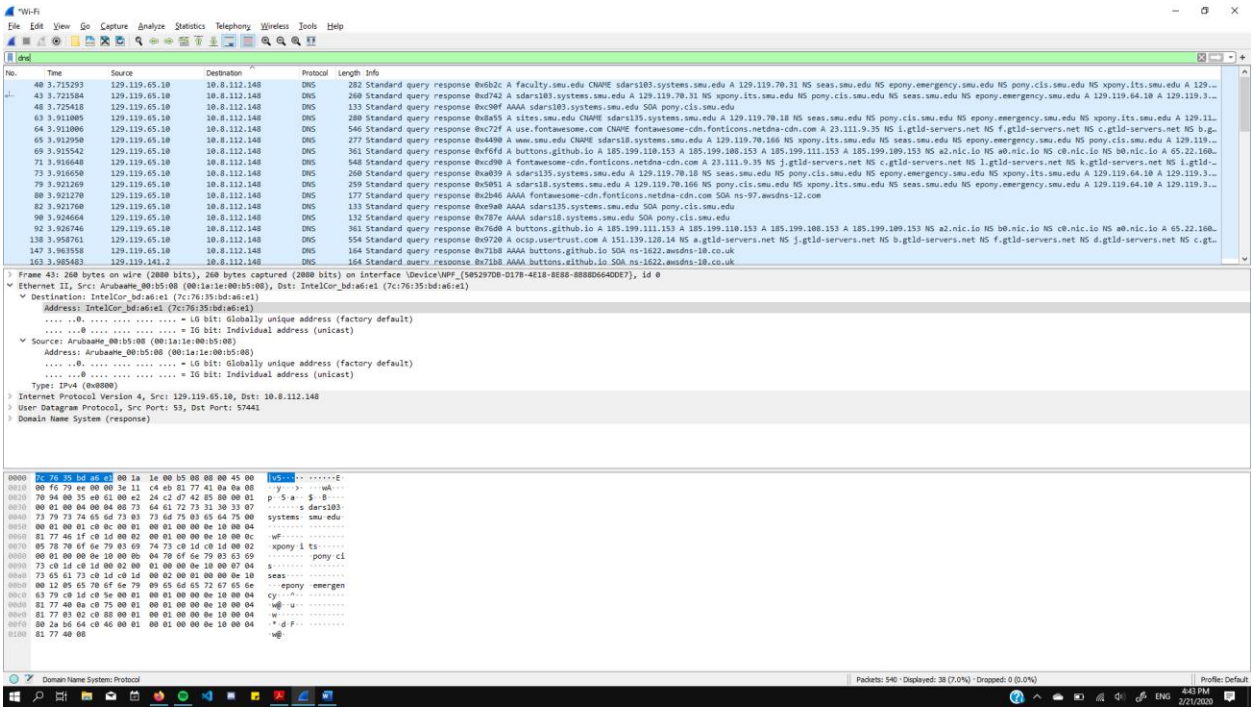
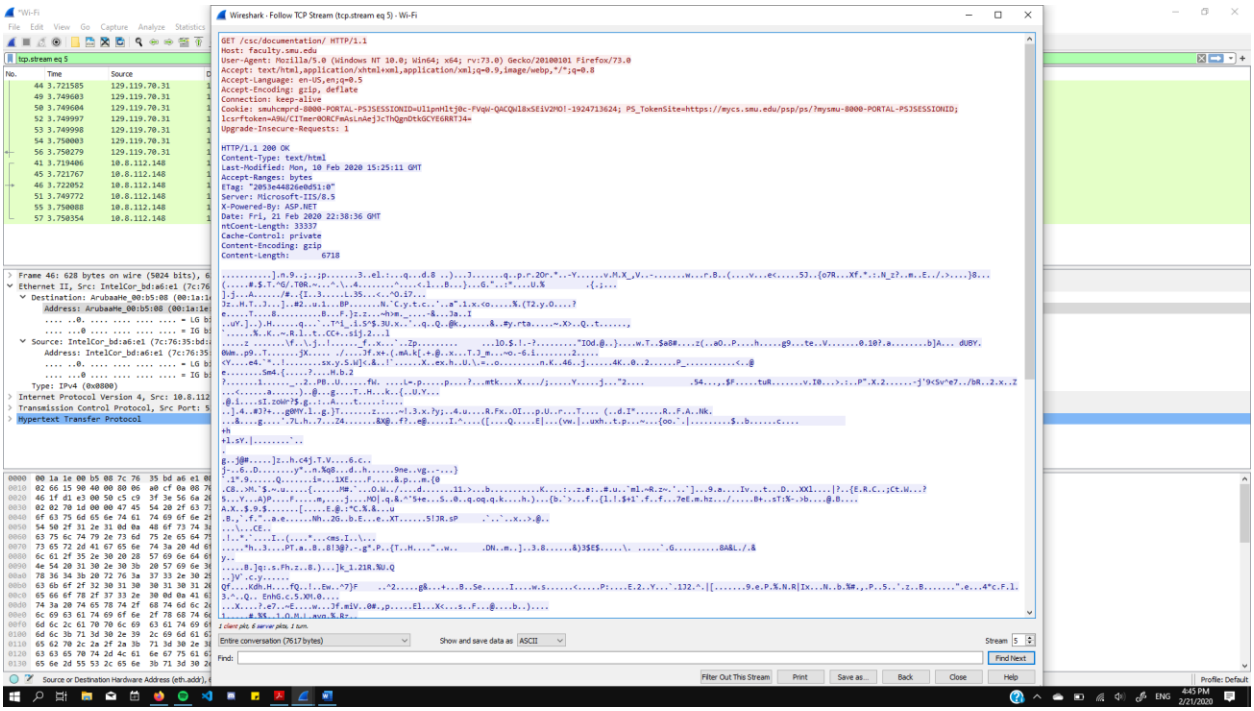
CS 3339 N11

Lab 10

1.







2. Packets highlighted in black are TCP packets that had a problem.
3. To list http traffic, “http” is the command for the filter bar.
4. DNS uses UDP because it is much faster than TCP and can fit DNS requests in each segment.
5. To capture the password used to connect to the FTP server, I had Wireshark capture packets while logging into the server. I filtered through the traffic using “ftp” and found packets with the header USER that contained the username in plaintext. I found another packet with the header PASS with the password in plaintext.
   Sending credentials in plaintext could’ve been prevented by hashing them first. That hash could be checked against the hash of the correct login hash, and access could be denied or granted accordingly.