CS2910 Exercise: Email and SMTP

Names: ____

Email Protocols

1. Historically, there could be several servers involved in transferring a message from one client to another. Today, the number of servers between the sending and receiving client is reduced to two. Could this be reduced to one? Why or why not?

2. Imagine reducing it to zero – that is, imagine sending email directly from client to client. What advantages or problems would this have?

3. The Stored Communications Act is often interpreted as saying that unopened mail held on a server for less than 180 days requires a search warrant to receive. On the other hand, email held on a server for more than 180 days, or email that has been opened can be obtained (more easily) with a court order. In light of this, which of POP, IMAP, or HTTP provides the best legal protection? Explain your answer.

4. Why is POP difficult to use with multiple clients?

SMTP

1. Download and install Mozilla Thunderbird (25 MB download, 56 MB on disk). This is the email client from the maker of the web-browser Firefox. With it, you can send email using SMTP. If you get an error saying "this program is blocked by group policy," unzip the file (e.g. with 7-zip) and run the exe inside the extracted folder.

2. Configure Thunderbird to send email through your MSOE account. For the incoming server, use outlook.office365.com, with the default port 993 for IMAP. (Don't use POP – Why might I say this?) For the outgoing server, use **smtp**.office365.com and the default port of 587 (with "IMAP", though really SMTP is used for sending email). You can use the default security settings. (MSOE HUB documentation of how to do this – you may need to log in twice.) Once configured, you should be able to view your on-server messages either in Outlook or Thunderbird. (You can also use IMAP with gmail if you would like.)

3. Fire up Wireshark. Filter on "smtp". Send a friend (or yourself) an email using Thunderbird. Look at the captured packets.
    a. Which messages between your client and the server do you see in the wireshark trace?

    b. The 250 message is sent multiple times in one of the replies from the server. How does the client know when the server is done sending messages? Can you confirm your hunch by reading the specification? (RFC 5321)

    c. What messages are missing in your Wireshark trace? Why are they missing?

    d. What else can you discover by looking at the sent message? Can you confirm this from the specification?