ELE437 Wireshark Assignment

This assignment uses the wireshark capture data from an SMTP session which generates an email message using the previous computer assignment. The capture data, the log of the SMTP session, and the generated email message are available at http://www.ele.uri.edu/courses/ele437/sp07/wireshark.html. The capture data can be loaded into wireshark for analysis. Using this information, please answer the following questions.

1. What is the ethernet address of the SMTP client, and what is the ethernet address of the SMTP server?
2. What is the IP address of the SMTP client, and what is the IP address of the SMTP server?
3. Which frame was used to generate the To: header line in the message? Use the packet numbers 1 to 39 from the capture file.
4. Which frame acknowledged the Subject: header line in the message?
5. Which frames generated the body of the message?
6. What TCP port was used on SMTP client, and what TCP port was used on the SMTP server?
7. Why does wireshark label some of these frames as TCP and some as SMTP?
8. In the first SMTP frame (frame 4), what are the lengths of the frame, the ethernet header, the IP header, the TCP header, and the SMTP header? Give the length in bytes.
9. In the first frame (frame 1), what are the lengths of the frame, the ethernet header, the IP header, and the TCP header?
10. If frames 23 and 24 were missing, what effect would this have on the generated email message?