Wireshark Exercise

Before you start this lab, go to ANGEL and download the pcap files from the Lecture 4 folder. Open "Wireshark", then use the "File" menu and the "Open" command to open the file "Exercise.pcap". You should see 26 packets listed.

This set of packets describes a 'conversation' between a user's client and a central server. This entire conversation happens automatically, after a user types something and hits enter. Look at the packets to answer the following questions in relation to this conversation.

In answering the following questions, use brief descriptions. For example, "In frame X, the client requests a web page, and in frame Y, the server delivers the content of the page."

a) What is the IP address of the client that initiates the conversation?

b) Use the first two packets to identify the server that is going to be contacted. List the common name, and three IP addresses that can be used for the server.

c) What is happening in frames 3, 4, and 5?

d) What is happening in frames 6 and 7?

e) Ignore frame eight. However, for your information, frame eight is used to manage flow control.

f) What is happening in frames nine and ten? How are these two frames related?

g) What happens in packet 11?

h) After the initial set of packets is received, the client sends out a new request in packet 12. This occurs automatically without any action by the user. Why does this occur? What is occurring in packets 13 through 22?

i) Explain what happens in packets 23 through 26.

j) In one sentence describe what the user was doing (Reading email? Accessing a web page? FTP? Other?).