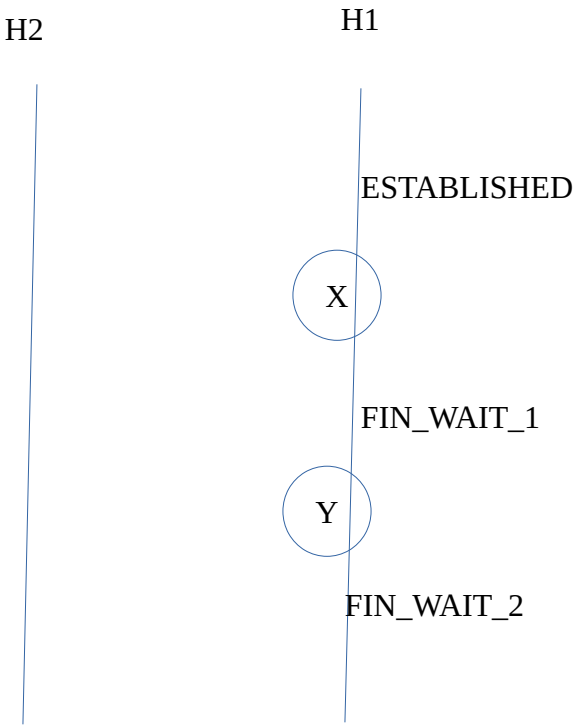
TEST 2 – 4/3/2023

Submit a single PDF file with your answers, and a pcapng Wireshark packets file.

No other files or file types will be graded.

1. The following figure shows the state transition diagram of a **host H1's TCP connection** to host H2. X and Y stand for TCP exchanges between the two hosts.



Indicate whether each of the following scenario is possible or not. If not possible, write a very brief reason. Your answers should be one-liners like *No – at this stage H2 can only send ACKs, no data*, or a simple *Yes*.

a. X could be H1 sending FIN flag to H2._____

b. X could be H1 sending FIN with PUSH flag to H2. _____

c. X could denote H1 receiving FIN from H2. _____

d. Y could be H1 receiving FIN from H2. _____

e. Y could be H1 receiving ACK of its FIN from H2. _____

f. Y could denote data transfer from H1 to H2. _____

g. Y could denote H1 sending H2 an ACK of H2's FIN. _____

2. Load the capture file attached into wireshark. Filter out the ssh session between 137.140.8.106 and 50.74.239.202

a. What are the client and server sockets for this ssh session?

b. Draw a flow diagram (flow graph) showing the first 4 and last 4 TCP exchanges in this session. (DO NOT Use Wireshark to draw the flow graph – Wireshark produces all exchanges between the hosts, which you need not show). Clearly marks the **TCP flags, Seq #, Ack #** in each of the displayed exchanges.

c. How long did the session last?

d. How many bytes of data were exchanged from each host in this session, not counting flags and headers? Give separate counts for data from each host.

e. Which host went through the CLOSE_WAIT state in this session?

f. Which host went through the TIME_WAIT1 state in this session?

3. In the following figure, if If x=140721 and y=221817, fill in the values of z, p, q, r and s