AUSTIN HALL

1.) The client IP address is 192.168.0.197 and the remote machine address is 146.187.134.7

2.) The client port is 42988 and remote machine is 22

3.) 13, 14, and 15. You can tell tcp is starting a new session because the client sends a SYN message to the server

4.) Client sequence number is 0 relative and raw is 1152689779, remote machine relative sequence number is 0 and raw is 3967195986

5.) Not exactly, there is the synchronization packets that are sent to establish a connection, but no actual data. There is no data field in the initial transmissions

6.) MSS of client is 1460 bytes and MSS of remote is 1380 bytes. MSS is the maximum number of bytes a device can receive in a single TCP segment.

7.) The TCP header contains 20 bytes

8.) The smallest window is 5792. The window size is specified by the receiver to indicate to the sender the amount of data in bytes that it is willing to receive and buffer for the connection.

9.) PSH is the push flag and allows the sending application to start sending the data even when the buffer is not full. With PSH flag set, the data received will be immediately sent to the application. I think the PSH flag is in this trace because its an SSH connection and since theres a window open to another computer it just sends the data there immediately.

10.) No you cant see the ascii commands or the data because SSH establishes an encrypted connection over a possibly unsecure network.

11.) The client sent the first fin packet. It’s not counted as data because there is no data field

12.) This session lasted 24.67 seconds

13.) Around 7,142 bytes were sent from the remote machine

14.) The packets aren’t being sent at a consistent rate. Round trip time average for the client sending packets appears to be around 80 ms. For the remote machine average, it seems to be around 15 ms

15.) The only pattern I found is that the port number from my machine varied between two different ports through most of the session while the remote stayed the same.

16.) The sequence number and acknowledgement number would swap places depending on if the packets were sent from or to me