Andrew Murza

CSE434
Assignment 4 pt 3

(a) How can you identify the packets involved in opening the TCP connection? What is the initial sequence number (ISN) of the TCP client and the TCP server (Hint: there is one ISN on each direction)?

To identify a TCP connection being established you should notice a packet with a SYN (synchronous) packet being sent to the server. When received by the server, a SYN ACK (acknowledgement) is sent back to the client. Then the client sends an ACK to the server once it received the SYN ACK to finalize the connection. The initial ISN of the client is 4012935996 and 3987339890 for the server.

(b) What is the sequence number used in the first byte of application data sent from the TCP client to the TCP server?

The sequence number used in the first byte of the data sent to the server is 4012935997.

(c) Determine the values of the receiving window sizes for the TCP client and the TCP server. How do they change? Note that TCP is full-duplex, there is a receiving window in each direction.

Initially the window size is 5840, but it decreases to 5792 for the SYN ACK then it varies in other sizes throughout the life of this analysis. 7168, 9216, 11584, 14480, 17376, 20272, 23168, 26064.

For the most part, when the client sends something the window is always 5840, but when the server sends something it varies.

(d) How many packets are transmitted by PC1 and how many packets are transmitted by PC2? Is there any retransmission of a TCP segment (with actual data)? Are there any duplicate ACKs?

PC1, in blue (the client), sends 11 packets.

PC2, in red (the server), sends 9 packets.

Every ACK sent by PC1 has an ack# of 987339891

(e) Inspect the TCP headers. How many types of flags do you observe (such as ACK)? What do they mean?

ACK- acknowledgement of an event

SYN- used to imitate connection, synchronous

PSH- indication to let receiver know data is being pushed

FIN- finished, means there is no more data from a sender

(f) How can you identify the packets that are involved in closing the TCP connection? Which end can initiate the close?

The client initiates closing the connection by sending a FIN packet to the server

The server initiates closing the connection by sending a FIN packet to the client

Both client and server initiate closing the connection.

(g) What does it mean for the TCP connection to be full duplex?

For a TCP connection to be full duplex it means that data can be transmitted in both directions simultaneously.