**Michael Sneberger – ASU ID#: 1000001544: Task 3:**

Note that this task is not optional. ANSWERS ARE IN RED TEXT

A Wireshark capture of synthetic TCP traffic between PC1 (10.0.5.11/24) the client, and PC2 (10.0.5.22/24) the server, follows. Use it to answer the following questions.

```
No. Time    Source    Dest.     Protocol Info
 1 0.000000 10.0.5.11 10.0.5.22 TCP 3062>4444 [SYN] Seq=4012935996 Ack=0 Win=5840 Len=0
 2 0.000285 10.0.5.22 10.0.5.11 TCP 4444>3062 [SYN, ACK] Seq=3987339890 Ack=4012935997 Win=5792 Len=0
 3 0.000345 10.0.5.11 10.0.5.22 TCP 3062>4444 [ACK] Seq=4012935997 Ack=3987339891 Win=5840 Len=0
 4 0.000940 10.0.5.11 10.0.5.22 TCP 3062>4444 [PSH, ACK] Seq=4012935997 Ack=3987339891 Win=5840 Len=1024
 5 0.001116 10.0.5.11 10.0.5.22 TCP 3062>4444 [PSH, ACK] Seq=4012937021 Ack=3987339891 Win=5840 Len=1024
 6 0.002851 10.0.5.22 10.0.5.11 TCP 4444>3062 [ACK] Seq=3987339891 Ack=4012937021 Win=7168 Len=0
 7 0.002939 10.0.5.11 10.0.5.22 TCP 3062>4444 [ACK] Seq=4012938045 Ack=3987339891 Win=5840 Len=1448
 8 0.002952 10.0.5.11 10.0.5.22 TCP 3062>4444 [ACK] Seq=4012939493 Ack=3987339891 Win=5840 Len=1448
 9 0.003027 10.0.5.22 10.0.5.11 TCP 4444>3062 [ACK] Seq=3987339891 Ack=4012938045 Win=9216 Len=0
10 0.003051 10.0.5.11 10.0.5.22 TCP 3062>4444 [ACK] Seq=4012940941 Ack=3987339891 Win=5840 Len=1448
11 0.003060 10.0.5.11 10.0.5.22 TCP 3062>4444 [ACK] Seq=4012942389 Ack=3987339891 Win=5840 Len=1448
12 0.008083 10.0.5.22 10.0.5.11 TCP 4444>3062 [ACK] Seq=3987339891 Ack=4012939493 Win=11584 Len=0
13 0.008175 10.0.5.11 10.0.5.22 TCP 3062>4444 [ACK] Seq=4012943837 Ack=3987339891 Win=5840 Len=1448
14 0.008187 10.0.5.11 10.0.5.22 TCP 3062>4444 [FIN, PSH, ACK] Seq=4012945285 Ack=3987339891 Win=5840 Len=952
15 0.008147 10.0.5.22 10.0.5.11 TCP 4444>3062 [ACK] Seq=3987339891 Ack=4012940941 Win=14480 Len=0
16 0.008251 10.0.5.22 10.0.5.11 TCP 4444>3062 [ACK] Seq=3987339891 Ack=4012942389 Win=17376 Len=0
17 0.008646 10.0.5.22 10.0.5.11 TCP 4444>3062 [ACK] Seq=3987339891 Ack=4012943837 Win=20272 Len=0
18 0.011128 10.0.5.22 10.0.5.11 TCP 4444>3062 [ACK] Seq=3987339891 Ack=4012945285 Win=23168 Len=0
19 0.011810 10.0.5.22 10.0.5.11 TCP 4444>3062 [FIN, ACK] Seq=3987339891 Ack=4012946238 Win=26064 Len=0
20 0.011879 10.0.5.11 10.0.5.22 TCP 3062>4444 [ACK] Seq=4012946238 Ack=3987339892 Win=5840 Len=0
```

(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)?

A TCP handshake starts with the client sending a SYN packet asking for a connection. Then the server sends back a SYN-ACK packet, and finally the client completes the connection by sending back a SYN-ACK-ACK packet.

In the Wireshark capture above you can see:

#1 is the client PC1 at 10.0.5.11/24 sending a SYN packet sequence number 4012935996 to the server

#2 is the server PC2 at 10.0.2.22/24 sending a SYN-ACK packet with server sequence number 3987339890 to the client in response to client sequence number 4012935996 (you can tell because it sends back as ack=4012935997 which is one more than the SYN Seq number)

#3 is the client sending a SYN-ACK-ACK packet back to the server – you can tell this is the SYN-ACK-ACK as it is the sequential sequence number 4012935997 from the client sent in response to the server's sequence number 3987339891

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

4012935997 but then the server does not ACK until client resends as 4012937021

(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.
The client receiving window size = 5840 as announced in the #1 SYN packet

The server receiving window size initially = 5792 as announced in the #2 SYN-ACK but then it gets larger which indicates that there is more server receive buffer space available.

(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 transmits 11 packets

PC2 transmits 9 packets

(e) Inspect the TCP headers. How many types of flags do you observe (such as ACK)? What do they mean?
SYN = synchronize
SYN-ACK = synchronize request acknowledged
SYN-ACK-ACK = TCP handshake completed
PSH = an indication by the sender that, if the receiving machine's TCP implementation has not yet provided the data it's received to the code that's reading the data (program, or library used by a program), it should do so at that point.
FIN = I have nothing more to say which is an invitation to end the connection
FIN-ACK = connection terminated

(f) How can you identify the packets that are involved in closing the TCP connection? Which end can initiate the close?
#14 is a FIN, PSH, ACK packet from the client to server so it is an invitation to close the connection
#19 is a FIN, ACK packet from the server to the client so it is an agreement to close the connection
#20 is a final ACK packet by which the client closes the connection

(g) What does it mean for the TCP connection to be full duplex?
The server and the client can send data to each other simultaneously.

Deliverables:

1. Please briefly answer each question.
2. Please submit a PDF file containing the answers on Canvas, like that in assignment 1.

Grading rubrics:

There are two points for this task.