Homework 3

Due: 26 April 2022, 11:59pm

1 TCP Sliding window (15 pts)

Suppose A and B create a TCP connection with initial sequence numbers 20000 and and 5000, respectively, and an initial window of 8000 bytes. The table on the next page depicts the flow of the connection, which has 3 main events:

a. A sends three 100-byte segments, (Which we will name DataA1, DataA2, and DataA3), and B sends ACKs for each.

b. Between segments Data2A and DataA3, the application on B calls `read()` on the socket associated with this connection, which returns 200 bytes.

c. B sends a 100-byte segment DataB1 to A and begins the connection termination process with a FIN.

In the table on the next page, fill in the SEQ, ACK, and WIN fields for each packet shown, given the initial sequence numbers and window sizes.

Hint: Try to create a similar connection flow using the TCP reference, while looking at the packets sent in Wireshark—this should allow you to view the changes in sequence numbers, and window sizes. Another reference that may be useful is Section 17.3 of the Dordal textbook[1].

[1] http://intronetworks.cs.luc.edu/

t	**Packets sent by A**	**Packets sent by B**
0	SYN, seq=20000, win=8000	
1		SYN,ACK, seq=5000, ack=_____, win=8000
2	ACK, seq=_____, ack=_____, win=8000	
3	ACK, seq=_____, ack=_____, win=_____, data=DataA1	
4		ACK, seq=_____, ack=_____, win=_____
5	ACK, seq=_____, ack=_____, win=_____, data=DataA2	
6		ACK, seq=_____, ack=_____, win=_____
7		[*B calls* `read()`*, which returns 200 bytes*]
8	ACK, seq=_____, ack=_____, win=_____, data=DataA3	
9		ACK, seq=_____, ack=_____, win=_____
10		ACK, seq=_____, ack=_____, win=_____, data=`DataB1`
11	ACK, seq=_____, ack=_____, win=_____	
12		FIN,ACK, seq=_____, ack=_____, win=_____
13	. . .	

2 DNS (10 pts)

I issued two queries a few seconds apart to resolve `www.google.com`, and got the following responses:

Query 1:

```
;; QUESTION SECTION:
;www.google.com. IN A

;; ANSWER SECTION:
www.google.com.     300 IN  A   172.217.12.164
www.google.com.     300 IN  A   172.217.30.100

;; Query time: 44 msec
```

Query 2:

```
;; QUESTION SECTION:
;www.google.com. IN A

;; ANSWER SECTION:
www.google.com.     294 IN  A   172.217.30.100
www.google.com.     294 IN  A   172.217.12.164

;; Query time: 1 msec
```

Based on this information, answer the questions below. Your answers can be short (no more than 1–2 sentences).

a. How much time elapsed between queries 1 and 2, and how do you know?

b. Why did the second query take so much less time than the first zone?

c. Why are the two answers in different orders in the responses to queries 1 and 2?

d. If you run the authoritative DNS server for a website that has lots of geographically-distributed webservers, how could you use DNS to send users to the webserver closest to them?

e. Briefly explain how, if you control an ISP, you can attempt to leverage DNS to block access to sites you don't want your customers to access.

f. (**Bonus**, 2pts) Google uses a maximum TTL value of 300. `cs.brown.edu` uses a maximum of 86400. Why might Google want a very short TTL?