Kenneth Woodard

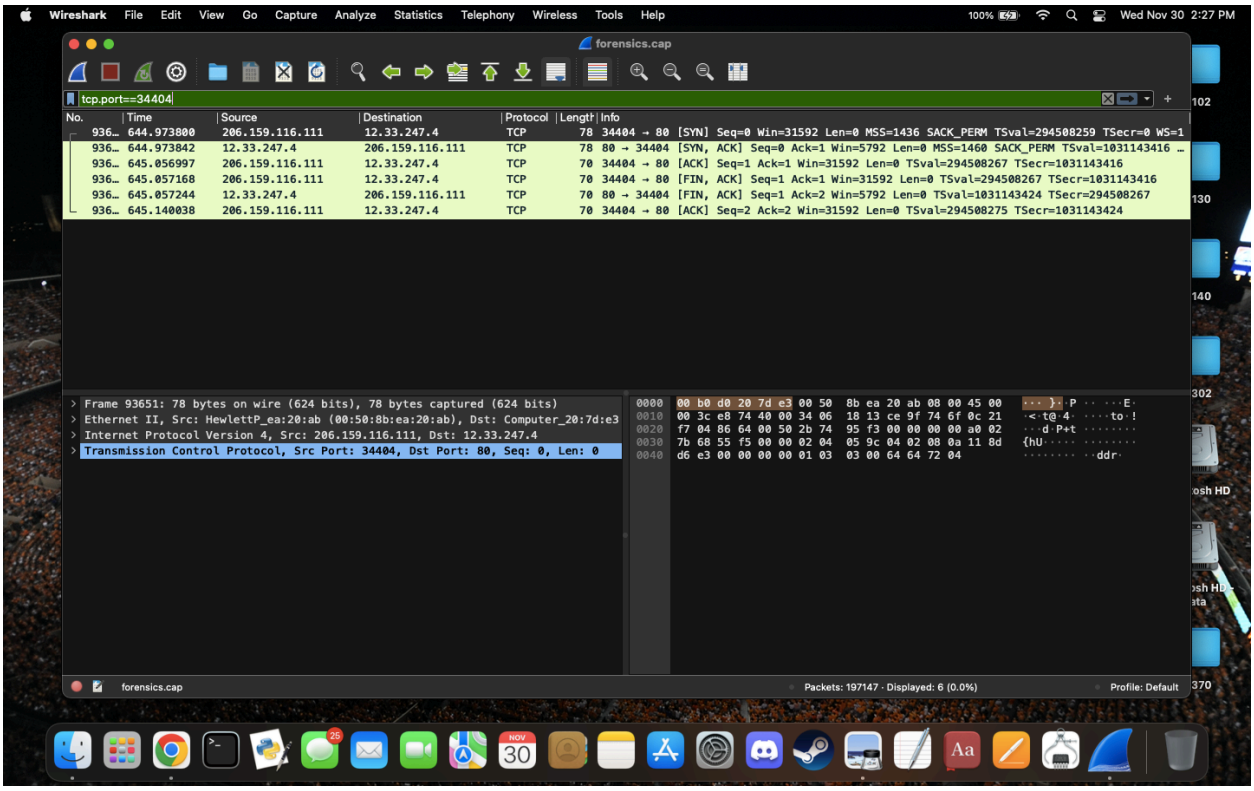
Programming Assignment 2: Report

CS 366

Question 1

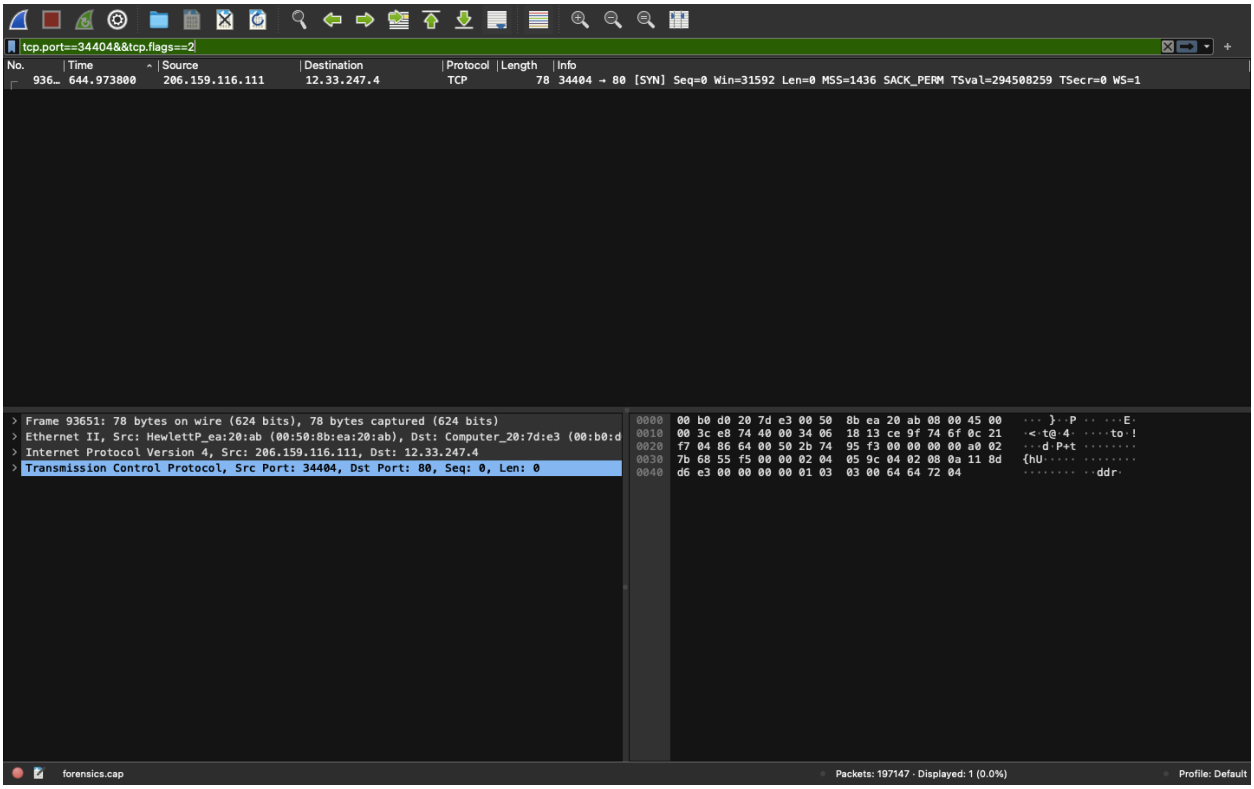
Six packets are printed out. Here's a list of the flags in each one:

- SYN
- SYN, ACK
- ACK
- FIN, ACK
- FIN, ACK
- ACK



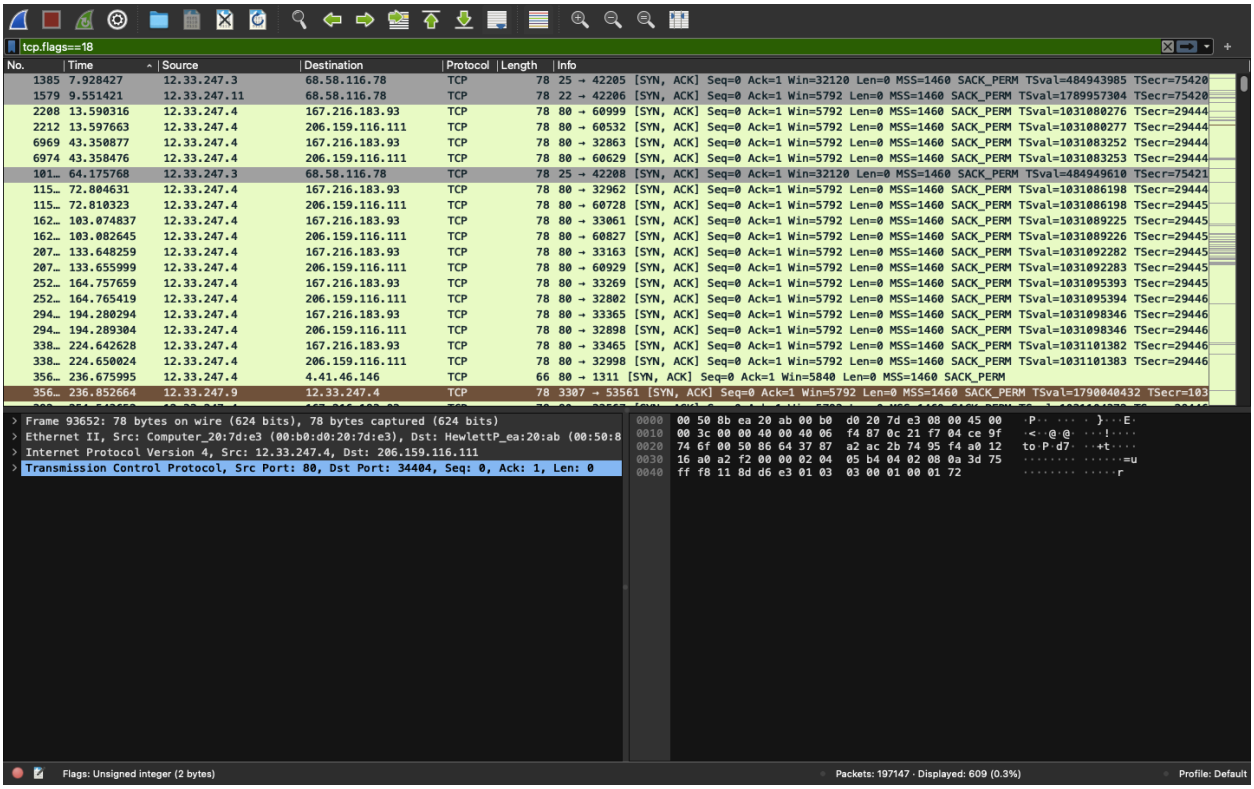
Question 2

Only one packet is printed. Including tcp.flags==2 basically narrows it down to only the packets that have only one flag: SYN.



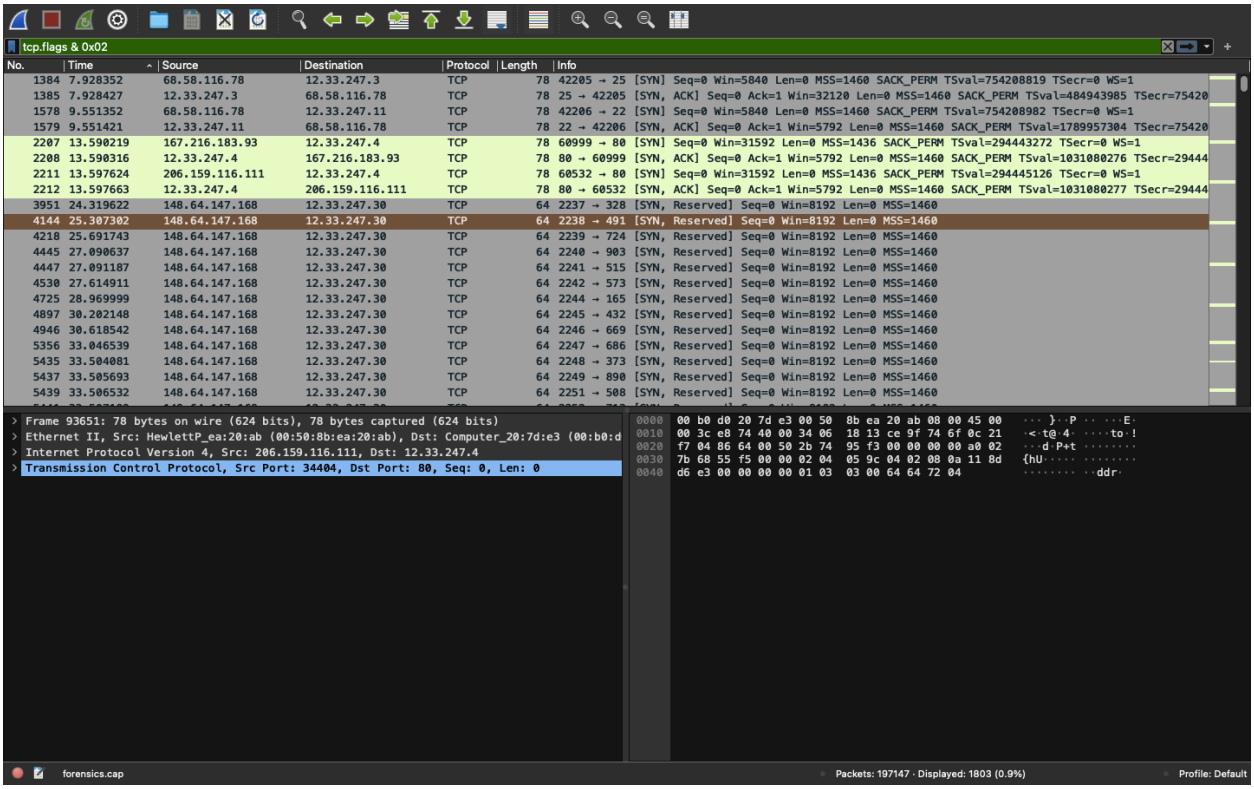
Question 3

609 packets were displayed upon using “tcp.flags==18.”



Question 4

1803 packets are displayed. "tcp.flags & 0x02" is the filter I used.

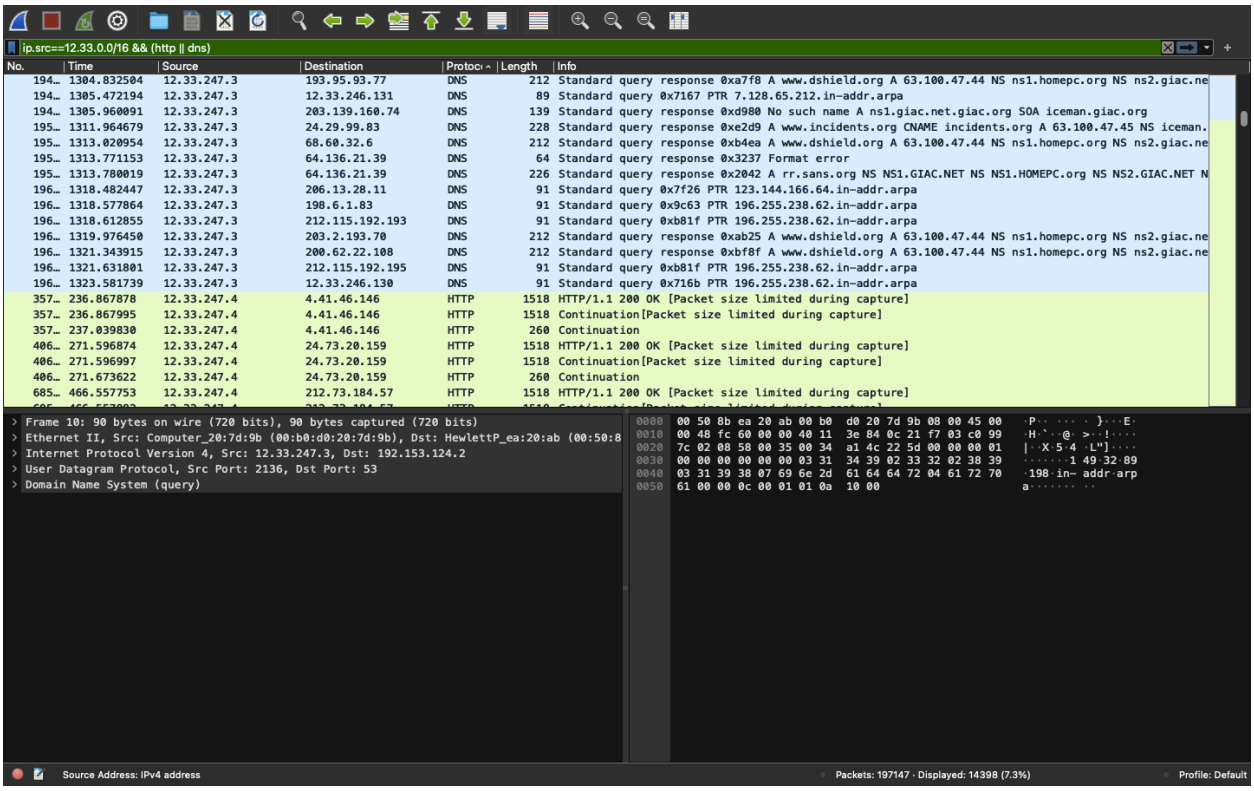


Question 5

My alternative filter for question 4 is “tcp.flags bitwise_and 2.”

Question 6

For the https servers the IP source address was either 12.33.247.2, 12.33.247.4, or 12.33.247.10. The DNS source addresses were either 12.33.247.3, 12.33.247.7, 12.33.247.11, 12.33.247.130, or 12.33.247.131. The method I used was filtering with this string “ip.src==12.33.0.0/16 && (http || dns)” and sorting by protocol. Then, I went through the list and compared IP source addresses. I’m going to include a screenshot for explanation.

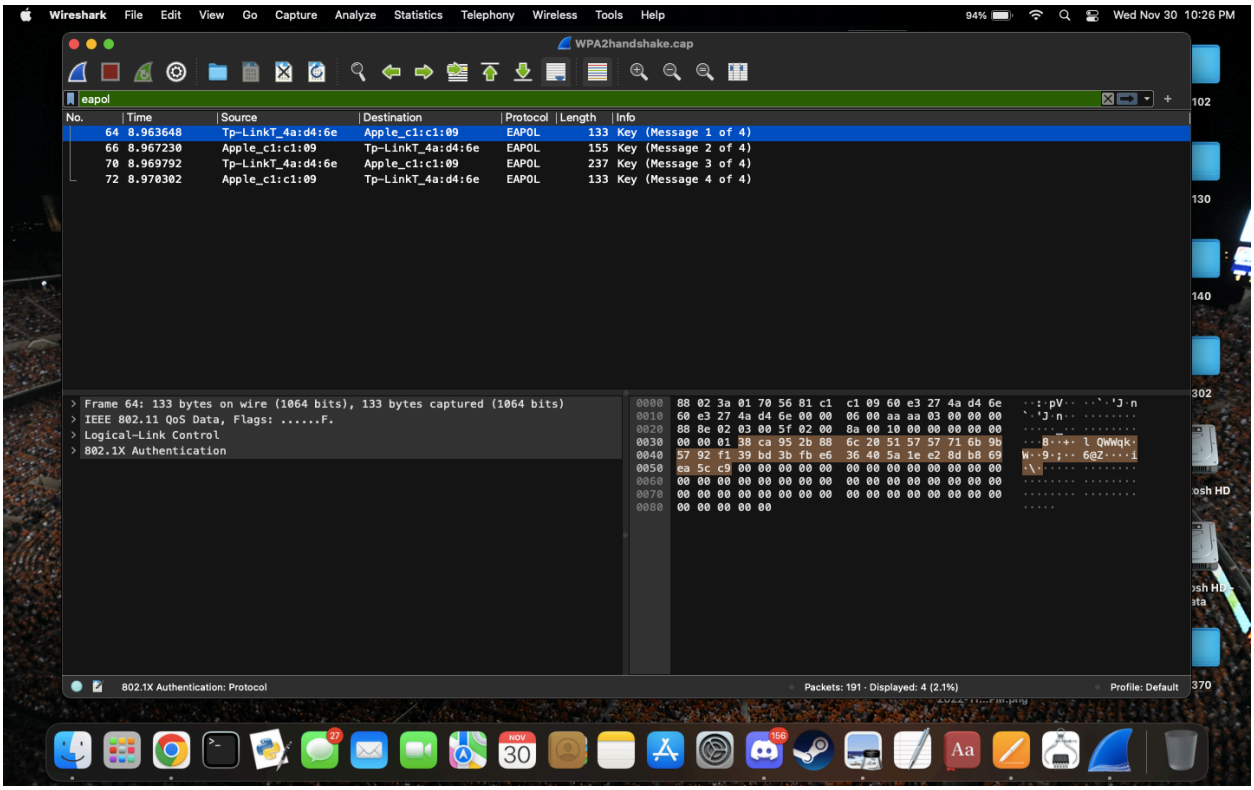


Question 7

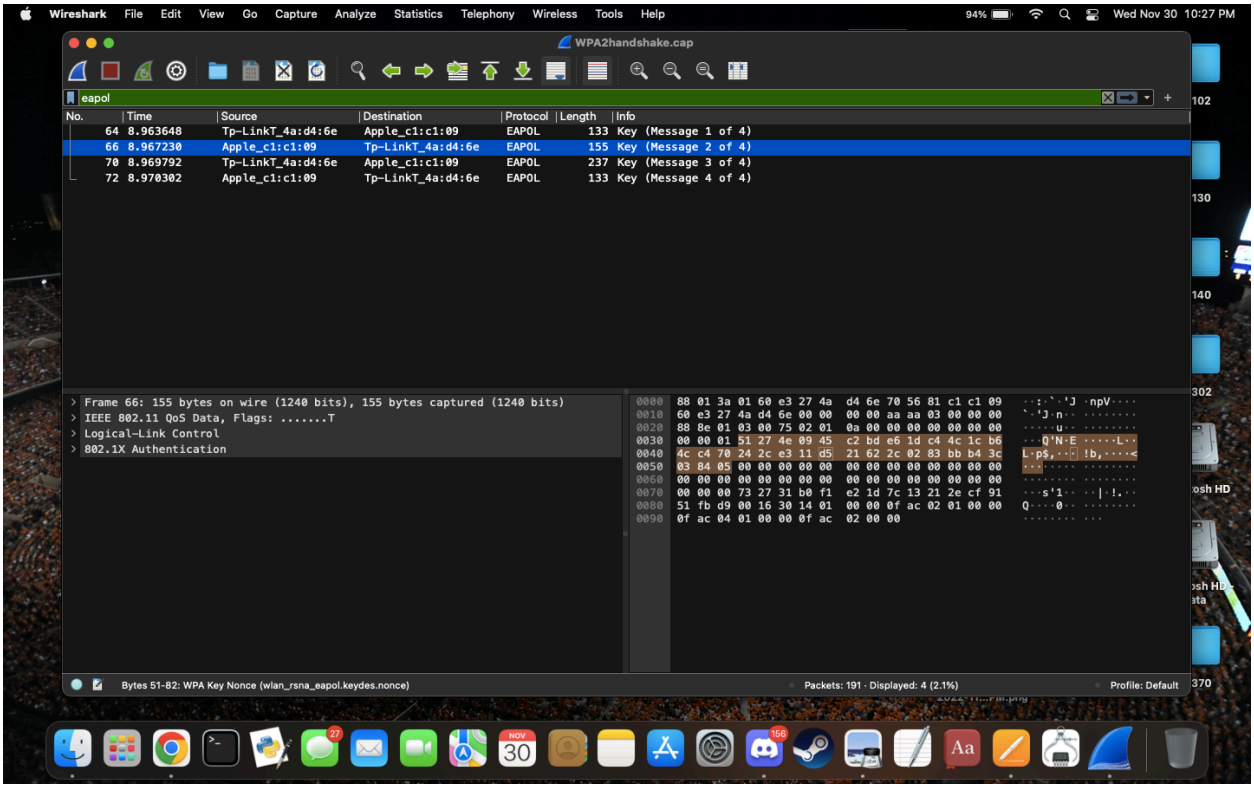
The messages are basically just bytes representing information for encryption/ decryption: addresses, keys, etc.

Question 8

- The ANonce value is 32 bytes, 256 bits long.



- The SNonce value is 32 bytes, 256 bits long.



- I found three non-zero MACs in the messages. They were each 16 bytes, 128 bits long.
- The authenticator sends the ANonce to the receiver. Now the receiver now can make the pairwise key. Then, the client sends the SNonce and the MAC to the host so that the authenticator can have the pairwise key. Now, the authenticator constructs a group key and sends it back with a MAC to protect it.

Question 9

A. Always.

Question 10

B. Only if a weak key/passphrase is used.