NSS Assignment

SAHIL BONDRE U18CO021

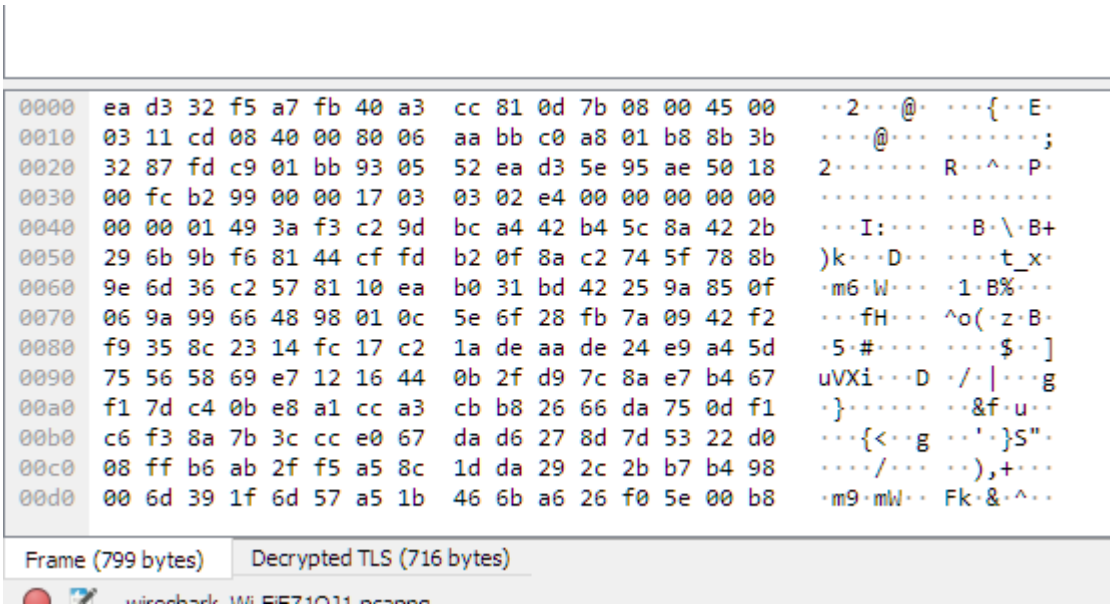
Q1: Decrypting SSL/TLS traffic in Wireshark

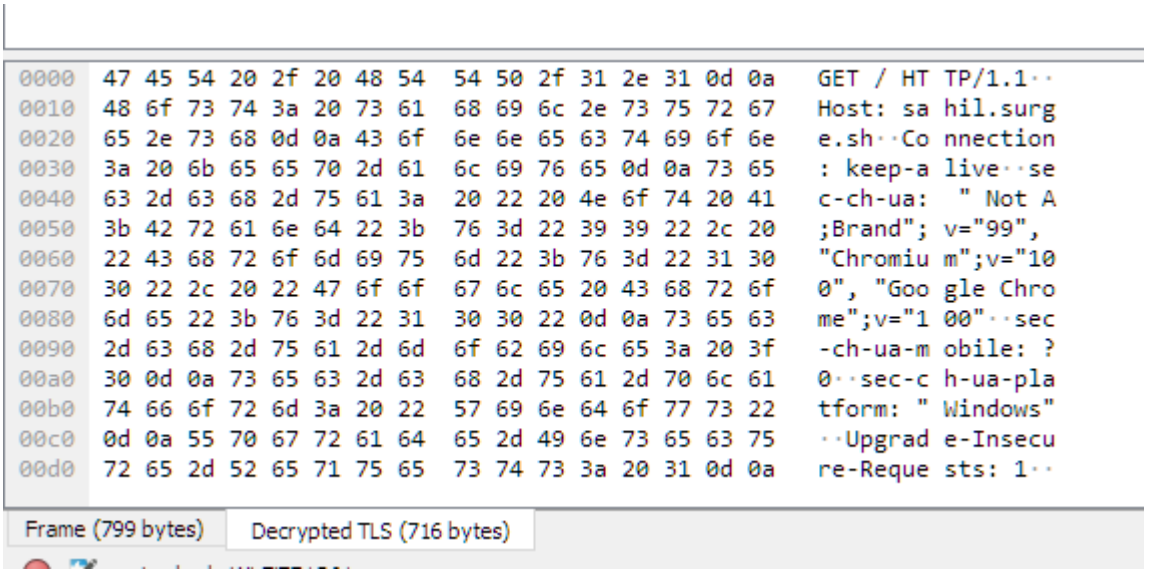
First, we need to add an environment variable so that all the keys for encryption are stored.

Added environment variable:

Now we can add this keylog file to Wireshark to get the decrypted text.

Decrypting Traffic





Q2: In SSL/TLS, "It is possible for the server to reorder SSL record layer packets that arrive out of order". Do you agree with the statement? If yes, explain how reordering can be done. If not, explain why?

Yes, It is possible for the server to reorder SSL record layer packets that arrive out of order. After decrypting, the server can rearrange the packets just like TCP. SSL packets are transmitted with packet numbers. The packet numbers allow the packets to be re-ordered into the proper order if they arrive out of sequence.

Q3: In SSL/TLS, the application-layer payload is compressed first(if compression is applicable) and then encrypted. Can we encrypt the payload first and then compress it?

Yes, it is possible but it's not efficient.

1. Compression techniques work on patterns in the data stream. After encryption, the data becomes a pseudo-random stream reducing the efficiency of compression.
2. Compressed data takes lesser space and will be faster to encrypt.