

NSS Assignment

SAHIL BONDRE U18CO021

Q1: Decrypting SSL/TLS traffic in Wireshark

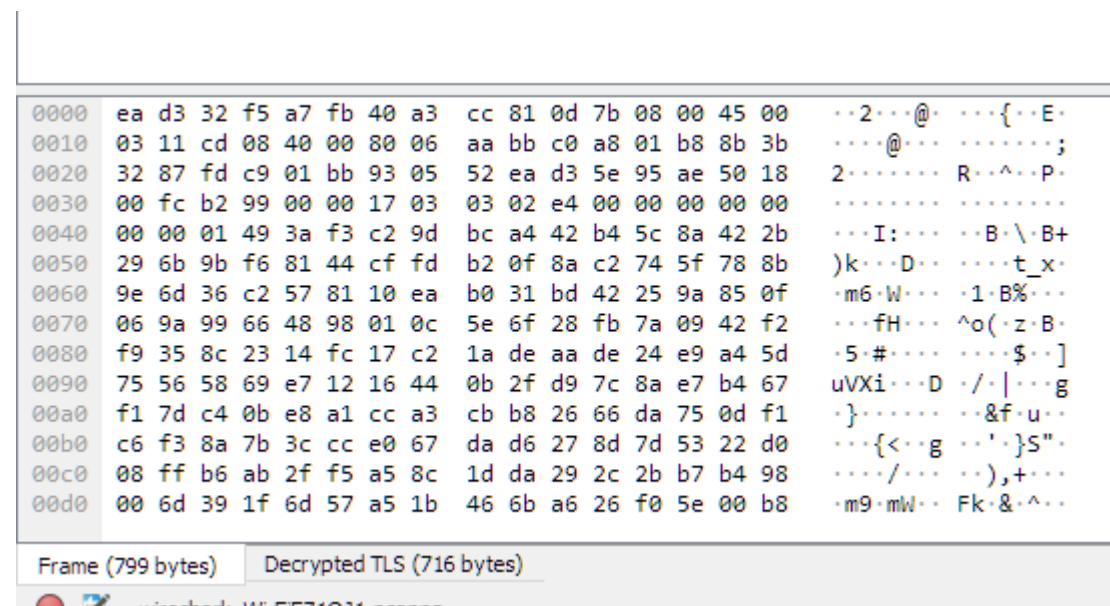
First, we need to add an environment variable so that all the keys for encryption are stored.

Added environment variable:



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

Decrypting Traffic



0000	47 45 54 20 2f 20 48 54	54 50 2f 31 2e 31 0d 0a	GET / HTTP/1.1
0010	48 6f 73 74 3a 20 73 61	68 69 6c 2e 73 75 72 67	Host: sahil.surg
0020	65 2e 73 68 0d 0a 43 6f	6e 6e 65 63 74 69 6f 6e	e.sh...Connection
0030	3a 20 6b 65 65 70 2d 61	6c 69 76 65 0d 0a 73 65	: keep-alive...
0040	63 2d 63 68 2d 75 61 3a	20 22 20 4e 6f 74 20 41	c-ch-ua: "Not A
0050	3b 42 72 61 6e 64 22 3b	76 3d 22 39 39 22 2c 20	;Brand"; v="99",
0060	22 43 68 72 6f 6d 69 75	6d 22 3b 76 3d 22 31 30	"Chromium";v="10
0070	30 22 2c 20 22 47 6f 6f	67 6c 65 20 43 68 72 6f	0", "Google Chro
0080	6d 65 22 3b 76 3d 22 31	30 30 22 0d 0a 73 65 63	me";v="1.00"...sec
0090	2d 63 68 2d 75 61 2d 6d	6f 62 69 6c 65 3a 20 3f	-ch-ua-mobile: ?
00a0	30 0d 0a 73 65 63 2d 63	68 2d 75 61 2d 70 6c 61	0...sec-c h-ua-pla
00b0	74 66 6f 72 6d 3a 20 22	57 69 6e 64 6f 77 73 22	tform: "Windows"
00c0	0d 0a 55 70 67 72 61 64	65 2d 49 6e 73 65 63 75	...Upgrade-Insecu
00d0	72 65 2d 52 65 71 75 65	73 74 73 3a 20 31 0d 0a	re-Requests: 1...

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.