Messy Aes

Problem: We were playing around with AES encryption. We seem to have lost our flag. Can you find it?

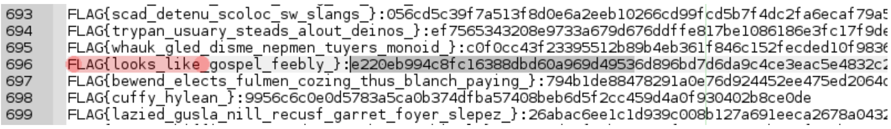
Given:
e220eb994c8fc16388dbd60a969d4953f042fc0bce25dbef573cf522636a1ba3fafa1a7c21ff824a5824c5dc4a376e75

Solution:

We are given a long cipher text and a file of plaintext and ciphertext pairs. Obviously, solving this problem should be based on typical known-plain text attack.

As hinted in the title, the cipher is AES. It is a block cipher, and the block size of plain text and cipher text is 128bits (16 bytes or 32 hex digits). The given cipher text is obviously a hex string and has 96 hex digits. Hence, the cipher text is made of three blocks.

So, we search for the first 32 hex digits "e220eb994c8fc16388dbd60a969d4953" in the given text file. We find the first 16 bytes in the plain text "FLAG{looks_like_".



```
FLAG{scad_detenu_scoloc_sw_slangs_}:056cd5c39f7a513f8d0e6a2eeb10266cd99fcd5b7f4dc2fa6ecaf79a5
FLAG{trypan_usuary_steads_alout_deinos_}:ef7565343208e9733a679d676ddffe817be1086186e3fc17f9de
FLAG{whauk_gled_disme_nepmen_tuyers_monoid_}:c0f0cc43f23395512b89b4eb361f846c152fecded10f983
FLAG{looks_like_gospel_feebly_}:e220eb994c8fc16388dbd60a969d49536d896bd7d6da9c4ce3eac5e4832c
FLAG{bewend_elects_fulmen_cozing_thus_blanch_paying_}:794b1de88478291a0e76d924452ee475ed2064
FLAG{cuffy_hylean_}:9956c6c0e0d5783a5ca0b374dfba57408beb6d5f2cc459d4a0f930402b8ce0de
FLAG{lazied_gusla_nill_recusf_garret_foyer_slepez_}:26abac6ee1c1d939c008b127a691eeca2678a043
```

Follow the same approach and find the rest of the flag…