**Flag 1:**

Don’t be fooled by two 0xffd9 markers



It is important to know 0xffd9 markers represent the end of the file. The description hints that there may be two 0xffd9 markers. I’m using [Hexed](https://hexed.it/), you can use the tool of your choice.

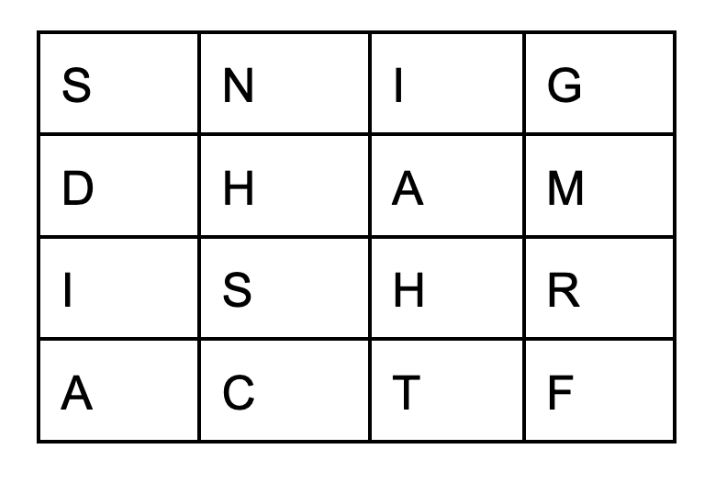
By looking at the end of the file, we can validate there are actually two EOI (End of Image) markers. The actual true end of the JPEG file is the first one. The second one is only there to fool us into thinking that this one is the actual end, which it isn’t. Notice there is data between those markers, let’s extract it and decrypt it.

“XOR and cb are your friends”

We have found data that doesn’t seem to decode in any readable way. You can use [this](https://gchq.github.io/CyberChef/#recipe=From_Hex('Auto')XOR(%7B'option':'Hex','string':'cb'%7D,'Standard',false)) link to decode it or XOR using cb as the key.

**Flag 2:**

Hello! I received this suspicious message: 'HKO{3Fk186r4-CkR9-11Fn-cOf1-0242Mh120002torN2}' and this image. Help me decrypt this



Use [this](https://www.boxentriq.com/code-breaking/cipher-identifier) website to find out the right cipher to use. On using the raw cipherText it will not detect anything. This may be due to some characters not being in the cipher’s alphabet.If you notice the image, only letters are used.

Thus, we could select the Letters Only option in Text Options to remove every character other than letters. This could solve our problem. It gave Base64 Encoding. On trying that out the result doesn’t look like simply Base64 Encoding.

If you look into the image further you’ll see only uppercase letters are used. This could mean that the case doesn’t matter in that cipher, thus we could try putting all letters in the ciphertext in uppercase too. We can achieve this by using the UPPER option in Text Options. This time it returns a list of possibilities. If you know PlayFair Cipher uses a grid similar to the image as the key. This can be used to decode the flag.

**Flag 3**

You have the zip file. If you unzip it you’ll see that it’s a GIT repository containing only one file which once contained the flag but is now redacted.

We will take a deeper look at the repository by using GitHub Desktop or the command-line or any Git Tool of your choice.

For GitHub:

You can just add the repository by giving the project's local path on your machine.

For CommandLine:

You can use *git log -p*

Using Either go through the commits and one of them will have the original Flag.