Something with an E

```
┌──(debangshu㉿localhost)-[~/Downloads] └─$ steghide embed -cf
WhatsApp_Image_2024-12-10_at_19.15.36.jpeg -ef flag.enc -p "StegPass123"

embedding "flag.enc" in "WhatsApp_Image_2024-12-10_at_19.15.36.jpeg"... done

┌──(debangshu㉿localhost)-[~/Downloads] └─$ steghide extract -sf
WhatsApp_Image_2024-12-10_at_19.15.36.jpeg -p "StegPass123"

the file "flag.enc" does already exist. overwrite ? (y/n) t steghide: did not write to file
"flag.enc".

┌──(debangshu㉿localhost)-[~/Downloads] └─$ steghide extract -sf
WhatsApp_Image_2024-12-10_at_19.15.36.jpeg -p "StegPass123"

the file "flag.enc" does already exist. overwrite ? (y/n) y wrote extracted data to
"flag.enc".

┌──(debangshu㉿localhost)-[~/Downloads] └─$ openssl enc -aes-256-cbc -d -in
flag.enc -out flag_decrypted.txt -pass pass:CTFChallengeKey -pbkdf2

┌──(debangshu㉿localhost)-[~/Downloads] └─$ cat flag_decrypted.txt
```

The war prowls at night

```
┌──(debangshu㉿localhost)-[~/Downloads] └─$ exiftool WhatsApp_Image_2024-
12-10_at_19.15.36_1_with_flag.jpeg

ExifTool Version Number : 13.00 File Name : WhatsApp_Image_2024-12-
10_at_19.15.36_1_with_flag.jpeg Directory : . File Size : 24 kB File Modification
Date/Time : 2024:12:26 05:52:19+00:00 File Access Date/Time : 2024:12:26
05:52:19+00:00 File Inode Change Date/Time : 2024:12:26 05:52:19+00:00 File
Permissions : -rw-rw-r-- File Type : JPEG File Type Extension : jpg MIME Type :
image/jpeg JFIF Version : 1.01 Resolution Unit : None X Resolution : 1 Y Resolution
: 1 XMP Toolkit : Image::ExifTool 13.00 Description : Cipher: U2VjcmV0UGFzcw==
Image Width : 198 Image Height : 254 Encoding Process : Baseline DCT, Huffman
coding Bits Per Sample : 8 Color Components : 3 Y Cb Cr Sub Sampling :
YCbCr4:4:4 (1 1) Image Size : 198x254 Megapixels : 0.050

┌──(debangshu㉿localhost)-[~/Downloads] └─$ echo "U2VjcmV0UGFzcw==" |
base64 -d

SecretPass
```

```
┌──(debangshu㉿localhost)-[~/Downloads] └─$ steghide extract -sf
WhatsApp_Image_2024-12-10_at_19.15.36_1_with_flag.jpeg -p "SecretPass"

the file "flag.txt" does already exist. overwrite ? (y/n) y wrote extracted data to
"flag.txt".

┌──(debangshu㉿localhost)-[~/Downloads] └─$

┌──(debangshu㉿localhost)-[~/Downloads] └─$ cat flag.txt
Flag{R3c0v3r_Th3_Flag}
```

Seems off doesnt it?

Step 1: Examine the file to see its type

```
file final_challenge.txt
```

Step 2: Remove the first few lines containing the instructions and extract the encrypted data

```
sed '1,3d' final_challenge.txt > encrypted_data.bin
```

Step 3: Attempt decryption using OpenSSL with the given passphrase (SecretPass)

```
openssl enc -d -aes-256-cbc -in encrypted_data.bin -out decrypted.tar.gz -pass
pass:SecretPass -pbkdf2
```

Step 4: If OpenSSL fails (bad magic number), try other decryption methods or investigate further

```
xxd encrypted_data.bin | head -n 10
```

Step 5: Check for hidden files or archives within the encrypted binary using binwalk

```
binwalk encrypted_data.bin
```

Step 6: If any embedded files are found, extract them using binwalk

```
binwalk -e encrypted_data.bin
```

Step 7: Once extracted, try to extract the tarball file (if decrypted successfully)

```
tar -xzvf decrypted.tar.gz
```

Step 8: If the extracted file contains the flag, you'll find it inside the text file

```
cat extracted_file.txt
```

Flag should now be revealed: Flag{school game for the file}

Sigma Sigma on the wall

1. Mount the Disk Image:

```
sudo mount disk.img /mnt/disk
```

1. List the Files on the Mounted Disk:

```
sudo ls -la /mnt/disk
```

Look for the encrypted_flag.txt file or any hidden files. 3. Inspect the Content of the Encrypted Flag:

If encrypted_flag.txt is found, check its contents to confirm it is encrypted:

```
sudo cat /mnt/disk/encrypted_flag.txt
```

It will likely be unreadable, as it's encrypted. 4. Decrypt the Flag:

Use OpenSSL to decrypt the file. The decryption password is CTF2024:

```
openssl enc -d -aes-256-cbc -in /mnt/disk/encrypted_flag.txt -out
/mnt/disk/decrypted_flag.txt -pass pass:CTF2024
```

1. Verify the Decrypted Flag:

Check the decrypted file to see the flag:

```
sudo cat /mnt/disk/decrypted_flag.txt
```

The flag should appear as:

```
CTF{hidden_forensic_challenge}
```

1. Clean Up:

Once you've recovered the flag, unmount the disk image:

```
sudo umount /mnt/disk
```