vishwaCTF

CHALLENGE NAME: [HexCode]

DEV: [Utkarsh Shirsath]

CATEGORY:

[Steganography]

LEVEL: [Easy]

2025

Challenge Description:

Solution:

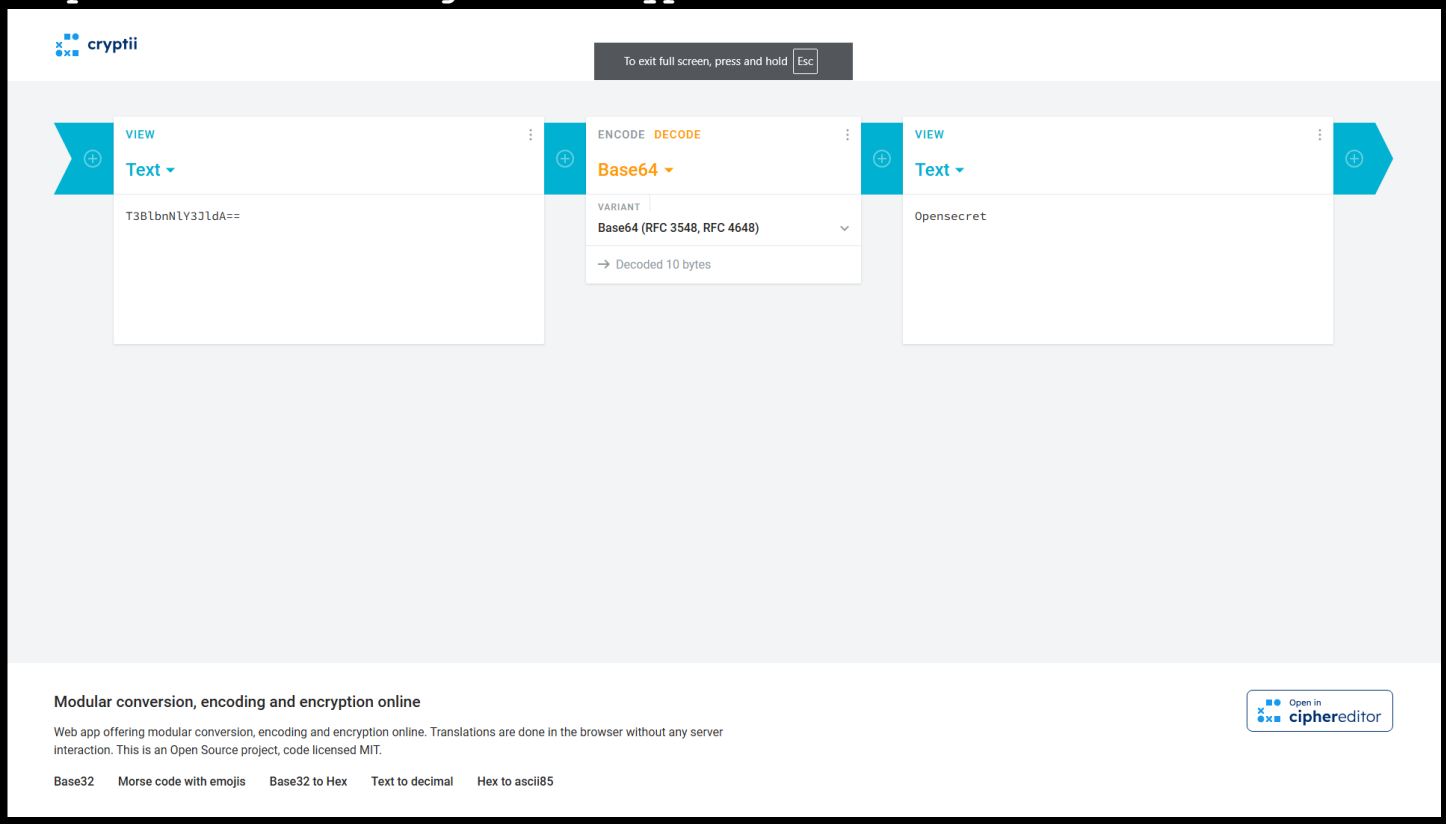
Step 1: - Use exiftool on image

```
kali@Utkarsh: /mnt/c/Users/U
└─(Run: "touch ~/.hushlogin" to hide this message)
┌──(kali㉿Utkarsh)-[/mnt/c/Users/UTKAR/Downloads]
└─$ exiftool HexCode.jpg
ExifTool Version Number         : 13.00
File Name                       : HexCode.jpg
Directory                       : .
File Size                       : 106 kB
File Modification Date/Time     : 2025:02:09 10:07:26+05:30
File Access Date/Time           : 2025:02:13 09:37:50+05:30
File Inode Change Date/Time     : 2025:02:09 10:07:26+05:30
File Permissions                : -rwxrwxrwx
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Comment                         : T3BlbnNlY3JldA==
Image Width                     : 532
Image Height                    : 653
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 532x653
Megapixels                      : 0.347

┌──(kali㉿Utkarsh)-[/mnt/c/Users/UTKAR/Downloads]
└─$
```

Step 2: - Notice the encrypted string in the 'Comment' field

Step 3: - Decode using Base64 cypher



Step 4: - Use this phrase as the passphrase for steghide

```
kali@Utkarsh: /mnt/c/Users/L
└─(Run: "touch ~/.hushlogin" to hide this message)
┌──(kali㉿Utkarsh)-[/mnt/c/Users/UTKAR/Downloads]
└─$ exiftool HexCode.jpg
ExifTool Version Number         : 13.00
File Name                       : HexCode.jpg
Directory                       : .
File Size                       : 106 kB
File Modification Date/Time     : 2025:02:09 10:07:26+05:30
File Access Date/Time           : 2025:02:13 09:37:50+05:30
File Inode Change Date/Time     : 2025:02:09 10:07:26+05:30
File Permissions                : -rwxrwxrwx
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Comment                         : T3BlbnNlY3JldA==
Image Width                     : 532
Image Height                    : 653
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 532x653
Megapixels                      : 0.347

┌──(kali㉿Utkarsh)-[/mnt/c/Users/UTKAR/Downloads]
└─$ steghide extract -sf HexCode.jpg
Enter passphrase:
the file "HexCode.zip" does already exist. overwrite ? (y/n) |
```

Step 5: - Examine the file just extracted.

Observation to be made: - secure.zip requires password and hint.txt contains a riddle/hint.

Name	Date modified	Type	Size
Earlier this week			
HexCode.jpg	09-02-2025 10:07 AM	JPG File	104 KB
Last week			
secure.zip	07-02-2025 12:14 PM	Compressed (zipp...	1 KB
hint.txt	07-02-2025 11:33 AM	Text Document	1 KB

Step 6: - Try decoding the riddle.

Hints riddle provides: -

"In a realm of shades, uncover the truth:"

Hinting to .jpg files, its pixels and RGB that make up pixels.

"(117, 293) R: 89, (463, 503) B: 216, (482, 99) B: 52, (295, 508) G: 96, (67, 580) G: 97, (465, 109) R: 42, (401, 186) B: 26, (413, 174) R:161."

This basically aims to tell x and y coordinates of a pixel hence '(x,y)' and 'R/G/B: number' refer to Red/Blue/Green values of a pixel at then given coordinate.

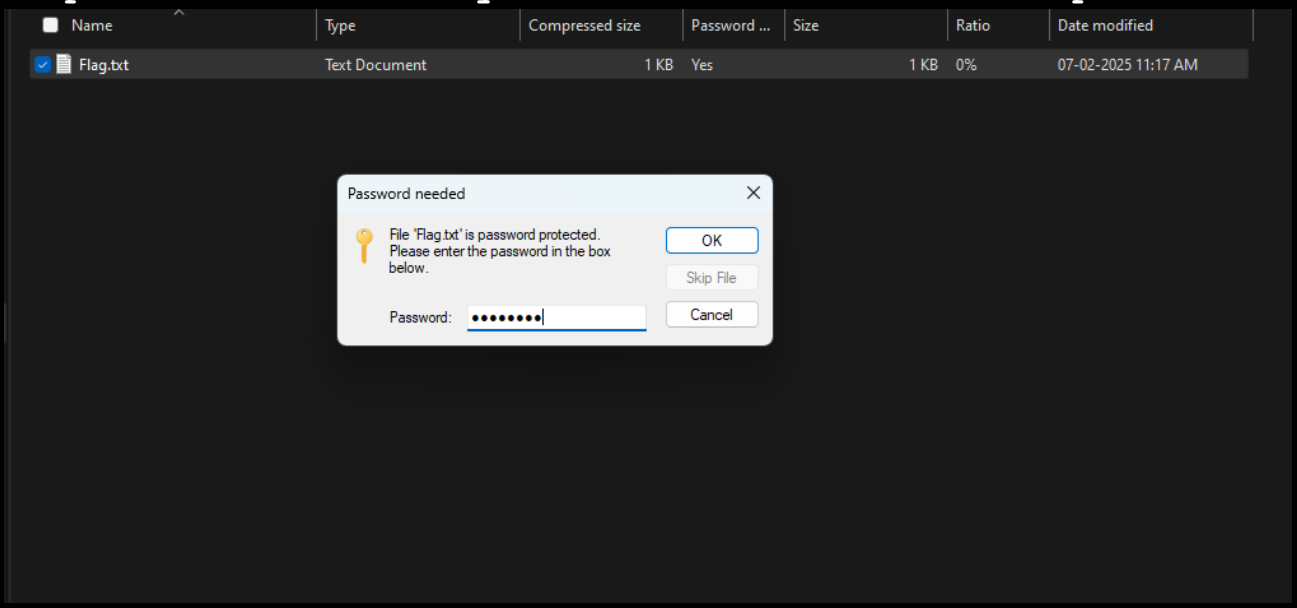
"For each bond, a whisper of 1; for each disconnect, a sigh of 0. Decode the hues to unveil the path."

If the R/G/B values of corresponding to the given coordinates matches with those of the actual image then note down '1' else '0'.

"Binary whispers will reveal what you seek."

Binary number you get after matching values is the password for 'secure.zip'

Step 7: - Use the binary number to unlock 'secure.zip' file.



Note: - In windows 11, dialogue box here mentions 'Flag.txt' but actually the .zip file is password protected.

Step 8: - Open the Flag.txt to get the flag

Flag: VishwaCTF{f9aB3xY7-KdQp52Lm-RtWz84Nv}