Writeup : The Mystery of the MAGIC Christmas Card

Pour ce challenge, j'ai téléchargé le fichier santa.pdf. Cependant, lorsque je l'ai ouvert, j'ai rencontré des erreurs. Après quelques vérifications, j'ai compris qu'il fallait changer l'extension .pdf en .jpg.

```
└─$ file santa.pdf
santa.pdf: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segme
nt length 16, baseline, precision 8, 640x640, components 3

┌──(kali㉿kali)-[~/Bureau/Pere_Noel]
```

Au départ, j'avais ouvert l'image directement sans y prêter attention, mais j'ai fini par obtenir la bonne image.

Étape 1 : Analyse initiale avec strings

En utilisant la commande strings, j'ai remarqué à la troisième ligne qu'il y avait un fichier caché dans l'image. Cela m'a mis sur la piste d'une stéganographie.

```
└─$ strings santa.jpg
JFIF
$3br
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
        #3R
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
@OjW
```

Étape 2 : Extraction du fichier caché

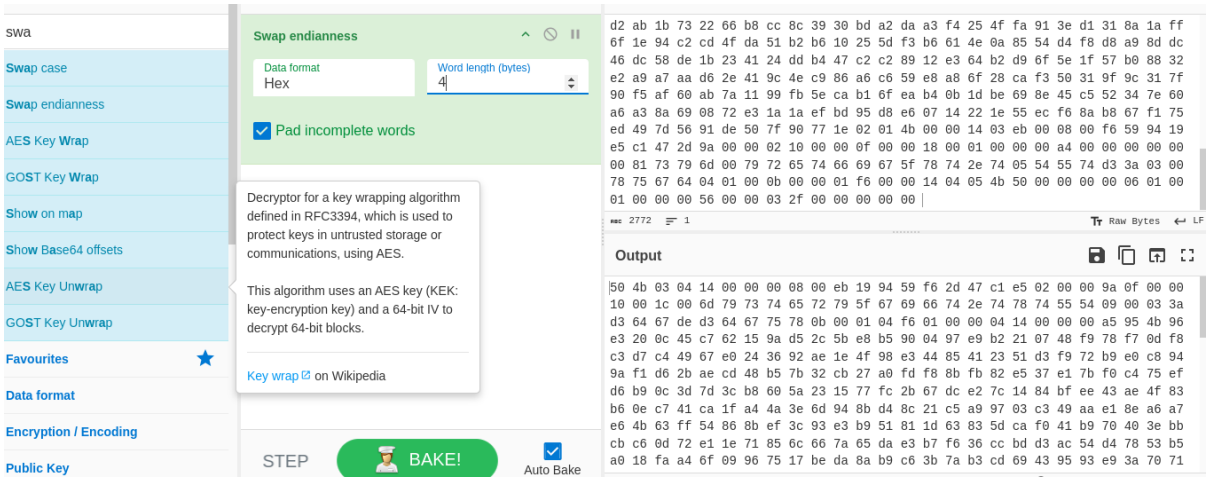
Pour extraire ce fichier, j'ai essayé avec steghide, mais cela nécessitait un mot de passe. J'ai donc utilisé mon outil préféré, **StegSeek**, qui a réussi à extraire un fichier nommé mystery.txt.

```
└─$ stegseek santa.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "@24Roxalan10@"
[i] Original filename: "mystery.txt".
[i] Extracting to "santa.jpg.out".
```

Étape 3 : Analyse du fichier extrait

En ouvrant mystery.txt, j'ai constaté que les données étaient en hexadécimal, mais inversées. Après correction, cela s'est révélé être un fichier ZIP.



Vous mon code python pour avoir le zip

```python
# Given the hex data, let's convert it into binary and save it as a ZIP file

hex_data = "50 4b 03 04 14 00 00 00 08 00 eb 19 94 59 f6 2d 47 c1 e5 02 00 00 9a 0f 00 00 10 00 1c 00 6d 79 73 74 65 7

# Convert the hex string into bytes
binary_data = bytes.fromhex(hex_data)

# Save the binary data to a file
zip_filename = 'mystery_gift.zip'
with open(zip_filename, 'wb') as f:
    f.write(binary_data)

zip_filename

```

Étape 4 : Recherche d'informations supplémentaires

En ouvrant ce fichier texte, j'ai d'abord pensé à une stéganographie utilisant des espaces ou des caractères invisibles (whitespace). Cependant, après plusieurs tests, cela ne donnait rien.

```
i want to say... merry christmas to you
i want to wish you... happiness and joy
but as i look around and see a whole world that's hurting
i can feel the pain... as i see it in their eyes

i want to say... merry christmas to you
i want to wish you... happiness and joy
but as i look around and see the faces staring blindly
i don't have the answers that can wash away their tears

i know a man who came and died for them
he suffered grief and pain beyond compare
born a simple child without a home to call his own
born to be a savior of the world...

can you see me ?
```

The Mystery of the MAGIC Christmas Card

500

Nicolas, the apprentice Santa Claus, received a mysterious digital greeting card. The image shows a SNOWY landscape sparkling with a thousand lights, with who seems to be offering him a gift. In a corner, we see other gifts at the foot of a magnificent Christmas tree. The card is signed "From all the elves". However, the elves claim they never sent this card. Nicolas suspects that a secret message is hidden there, perhaps linked to the list of toys for good children or the secret recipe for magic eggnog.

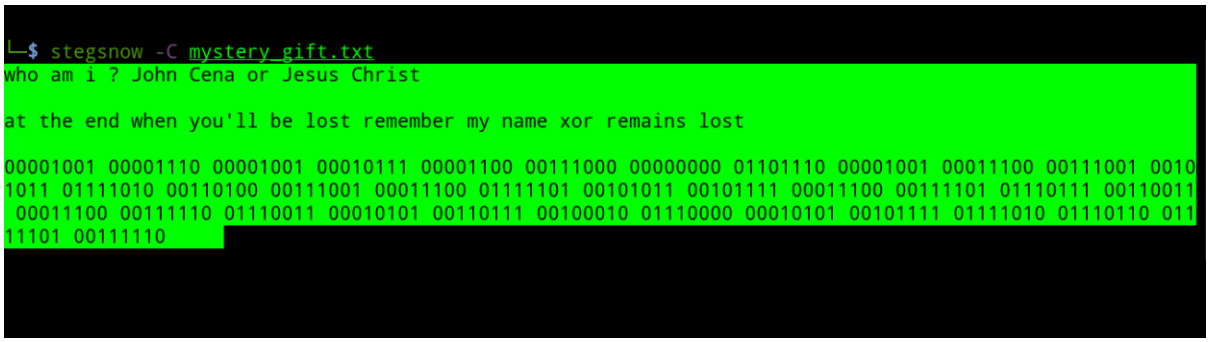
Flag format: CMCTF{REDACTED}

Author: t4f3

▶ Unlock Hint for 50 points

santa.pdf

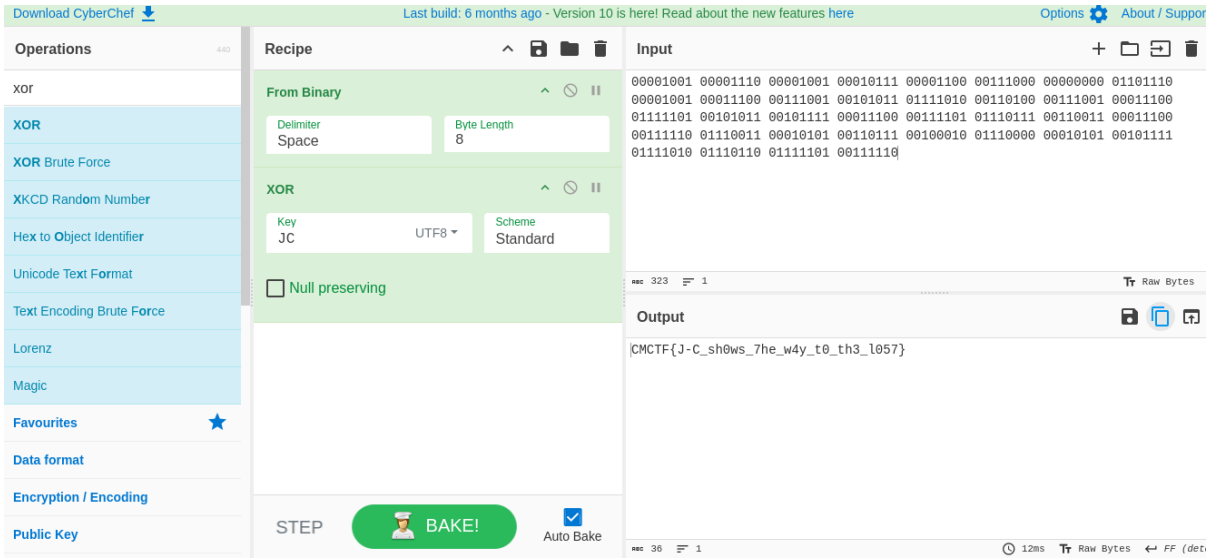
Après avoir relu attentivement le texte du fichier, j'ai remarqué un mot écrit en **majuscules**. Cela m'a semblé étrange et m'a donné l'idée de rechercher ce mot sur Google. À ma grande surprise, cela faisait référence à un outil nommé **StegSnow** (lien officiel).



Étape 5 : Utilisation de StegSnow

L'outil mentionnait qu'il fallait appliquer un **XOR** sur les données binaires. En haut du fichier texte, j'avais remarqué des mots comme "John Cena" ou "Jesus Christ". J'ai alors supposé que la clé pouvait être liée à "JC".

En utilisant **JC** comme clé pour le XOR, j'ai obtenu le flag :



CMCTF{J-C_sh0ws_7he_w4y_t0_th3_l057}

Writeup:overhack