

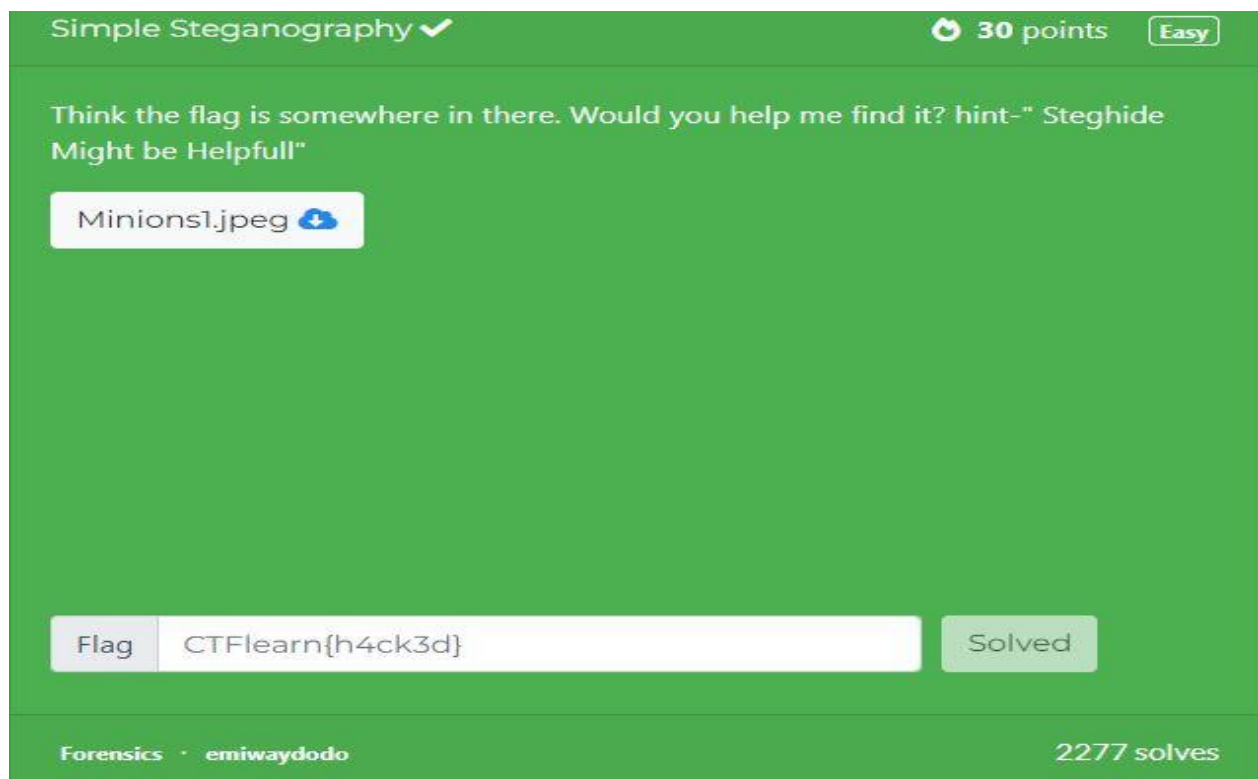
Write Up CTF

Dibuat oleh : Muhammad Mazaya

Nama Challenge : Simple Steganography

Categori : Forensics

Kali ini saya mencoba untuk menyelesaikan sebuah challenge CTF yang bernama Simple Steganography.



Pada challenge ini, diberikan sebuah file bernama Minions1.jpeg yang jika dibuka berisikan sebuah gambar minion lucu.



Karena challenge ini adalah tentang steganography, saya langsung saja menggunakan steghide.

```
kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)-[~/Downloads]
$ steghide extract -sf Minions1.jpeg
Enter passphrase: 
```

Namun, saya menemukan masalah yaitu saya tidak tahu passphrase untuk mendecode file tersebut.

Lalu saya mencoba untuk menggunakan exiftool untuk membaca meta yang terkandung dalam file tersebut.

```
kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)-[~/Downloads]
$ exiftool Minions1.jpeg
ExifTool Version Number      : 12.40
File Name                    : Minions1.jpeg
Directory                   : .
File Size                    : 6.8 KiB
File Modification Date/Time  : 2022:03:27 08:24:27-04:00
File Access Date/Time       : 2022:03:27 08:25:09-04:00
File Inode Change Date/Time  : 2022:03:27 08:24:31-04:00
File Permissions             : -rw-r--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
Current IPTC Digest          : b9e8892a1b55650cf0a6341fe676d194
Keywords                     : myadmin
Application Record Version   : 4
Image Width                  : 225
Image Height                  : 225
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                   : 225x225
```

Saya menemukan sebuah keyword dalam metadata file tersebut. Setelah itu saya coba gunakan keyword tersebut sebagai passphrase.

```
(kali@kali)-[~/Downloads]
$ steghide extract -sf Minions1.jpeg
Enter passphrase:
wrote extracted data to "raw.txt".

(kali@kali)-[~/Downloads]
$
```

Lalu saya buka raw.txt yang berisikan data-data yang terekstrak dari file tersebut.

```
(kali㉿kali)-[~/Downloads]
$ cat raw.txt
AEMAVABGAGwAZQBhAHIAbgB7AHQAaABpAHMAXwBpAHMAXwBmAHUAbgB9
```

Ternyata data yang terekstak merupakan sebuah string yang terlihat acak. String tersebut mengandung huruf-huruf kapital dan kecil dan juga angka-angka. Hal tersebut menyerupai sebuah string yang terenkrpsi dengan base64.

Saya langsung saja mencoba untuk mendecode string tersebut.

```
kali@kali: ~
File Actions Edit View Help

(kali㉿kali)-[~]
$ echo "AEMAVABGAGwAZQBhAHIAbgB7AHQAaABpAHMAXwBpAHMAXwBmAHUAbgB9"
" | base64 --decode
CTFlearn{this_is_fun}

(kali㉿kali)-[~]
$
```

Ternyata memang benar itu merupakan string yang terenkrpsi dengan base64 dan mengoutputkan sebuah flag yang dicari-cari.

Flag = CTFLearn{this is fun}