Forensics : Up can be Down (Before the CTF Hack)

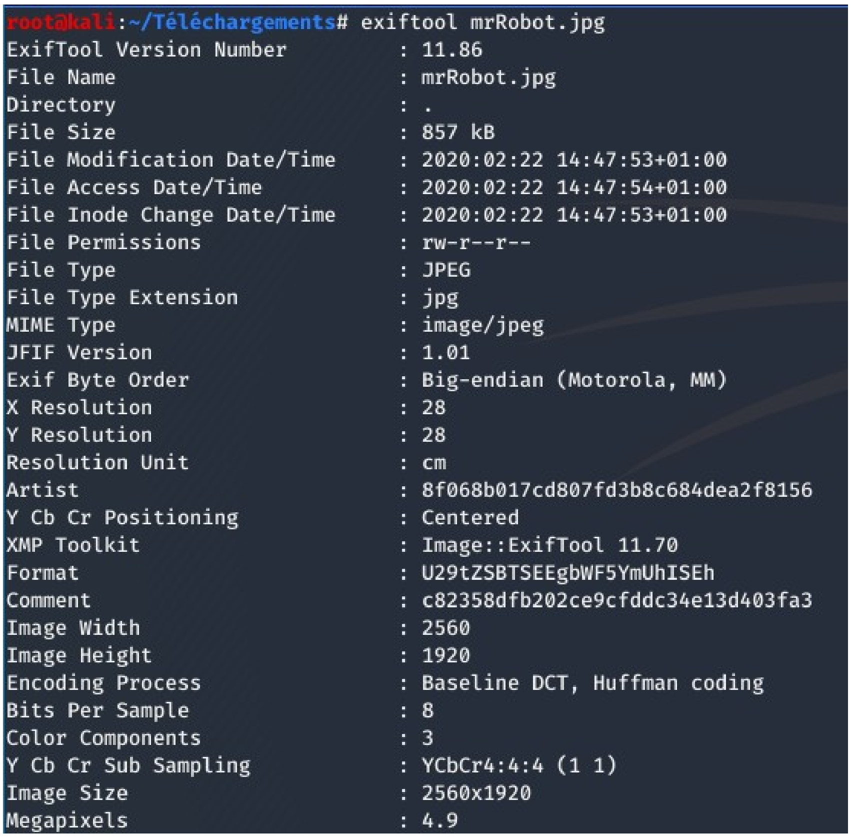
Value : 100 Pts

Description : Mr. Robot is being sent to future. But accidently he lost his passkey which he needs to activate the Time Machine. But he is smart and had already asked Elliot to save the key inside a file to use it in such conditions but safely so that others can't retrieve it easily. Can you help Mr. Robot to find the secret passkey from the file?

Attachment : mrRobot.jpg

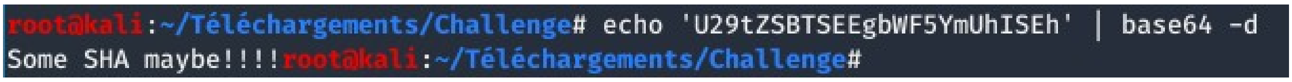
Solution

First download the attachment file «mrRobot.jpg». Using exiftool against the picture i was able to retrieve some interesting informations into «Format» and «Comment». The «Format» seem to be a base64.



```
root@kali:~/Téléchargements# exiftool mrRobot.jpg
ExifTool Version Number         : 11.86
File Name                       : mrRobot.jpg
Directory                       : .
File Size                       : 857 kB
File Modification Date/Time     : 2020:02:22 14:47:53+01:00
File Access Date/Time           : 2020:02:22 14:47:54+01:00
File Inode Change Date/Time     : 2020:02:22 14:47:53+01:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Big-endian (Motorola, MM)
X Resolution                    : 28
Y Resolution                    : 28
Resolution Unit                 : cm
Artist                          : 8f068b017cd807fd3b8c684dea2f8156
Y Cb Cr Positioning             : Centered
XMP Toolkit                     : Image::ExifTool 11.70
Format                          : U29tZSBTSEEgbWF5YmUhISEh
Comment                         : c82358dfb202ce9cfddc34e13d403fa3
Image Width                     : 2560
Image Height                    : 1920
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                      : 2560x1920
Megapixels                      : 4.9
```

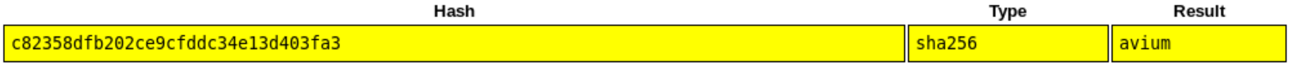
Decode the base64.



```
root@kali:~/Téléchargements/Challenge# echo 'U29tZSBTSEEgbWF5YmUhISEh' | base64 -d
Some SHA maybe!!!!root@kali:~/Téléchargements/Challenge#
```

The decoded output told us it’s maybe some SHA. Go to crackstation website and try to crack the hash.

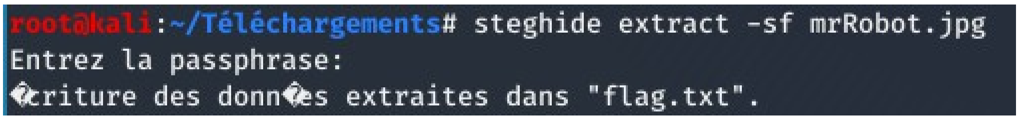
Source : https://crackstation.net/



Hash	Type	Result
c82358dfb202ce9cfddc34e13d403fa3	sha256	avium

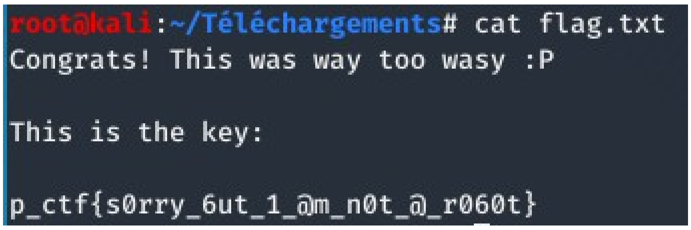
Result : avium

Using steghide for extract potential embed data with the password and we extracted a file «flag.txt».



```
root@kali:~/Téléchargements# steghide extract -sf mrRobot.jpg
Entrez la passphrase:
�criture des donn�es extraites dans "flag.txt".
```

Read the file for get the flag.



```
root@kali:~/Téléchargements# cat flag.txt
Congrats! This was way too wasy :P

This is the key:

p_ctf{s0rry_6ut_1_@m_n0t_@_r060t}
```

Flag : p_ctf{s0rry_6ut_1_@m_n0t_@_r060t}