Hidden in plainsight

kami mendapatkan sebuah file image dengan format jpg, dan kami melakukan analisa menggunakan exiftool untuk membaca metadatanya, dan kami menemukan sebuah text yang di hash menggunakan base64 dan kami melakukan dekode sebanyak 2 kali terhadap text yang di temukan untuk menemukan password yang kami butuhkan untuk melakukan ekstraksi pada image file nya

```
cyberjunkie@shadow:~/ctf/pico$ exiftool img.jpg
ExifTool Version Number         : 12.76
File Name                       : img.jpg
Directory                       : .
File Size                       : 74 kB
File Modification Date/Time     : 2026:01:14 15:20:30+07:00
File Access Date/Time           : 2026:01:14 15:20:42+07:00
File Inode Change Date/Time     : 2026:01:14 15:20:32+07:00
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
Comment                         : c3RlZ2hpZGU6Y0VGNmVuZHZjbVE9
Image Width                     : 640
Image Height                    : 640
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                      : 640x640
Megapixels                      : 0.410
cyberjunkie@shadow:~/ctf/pico$ echo c3RlZ2hpZGU6Y0VGNmVuZHZjbVE9 | base64 -d
steghide:cEF6endvcmQ=cyberjunkie@shadow:~/ctf/pico$ echo c3RlZ2hpZGU6Y0VGNmVuZHZjbVE9 | base
64 -d
cyberjunkie@shadow:~/ctf/pico$ echo cEF6endvcmQ= | base64 -d
pAzzwordcyberjunkie@shadow:~/ctf/pico$
```

kami berhasil menemukan passsword berupa pAzzword, didalam dunia forensic ada konsep yang bernama steganography, dan di dalam stegano graphy kami memiliki tools bernama steghide yang merupakan tools untuk menyisipkan sebuah text atau file kedalam sebuah gambar, yang dimana kami bisa menemukan text atau file di dalam sebuah gambar tersebut menggunakan tools yang sama, jadi kami akan mencoba melakukan ekstraksi file kepada file tersebut

```
cyberjunkie@shadow:~/ctf/pico$ echo cEF6endvcmQ= | base64 -d
pAzzwordcyberjunkie@shadow:~/ctf/pico$ steghide extract -sf img.jpg
Enter passphrase:
the file "flag.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "flag.txt".
cyberjunkie@shadow:~/ctf/pico$ cat flag.txt
picoCTF{h1dd3n_1n_1m4g3_871ba555}
cyberjunkie@shadow:~/ctf/pico$
```

kami berhasil menemukan sebuah file hasil ekstraksi file tersebut dengan menggunakan steghide, dan kami mendapatkan flagnya pada flag.txt