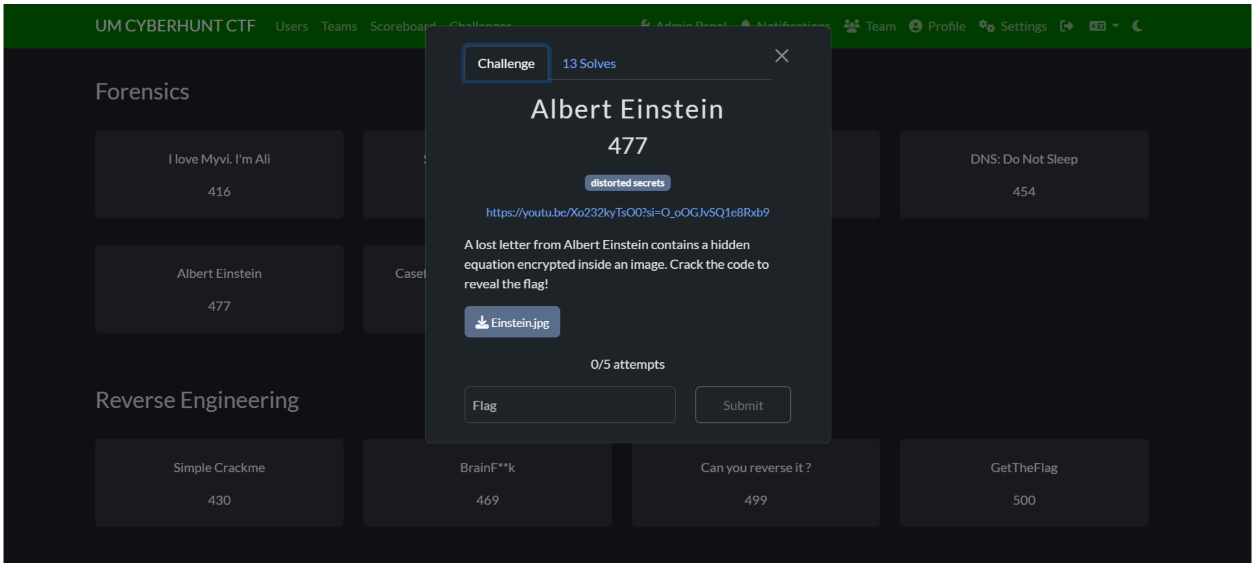
This is how the question looks like



Albert Einstein

477

distorted secrets

https://youtu.be/Xo232kyTsO0?si=O_oOGJvSQ1e8Rxb9

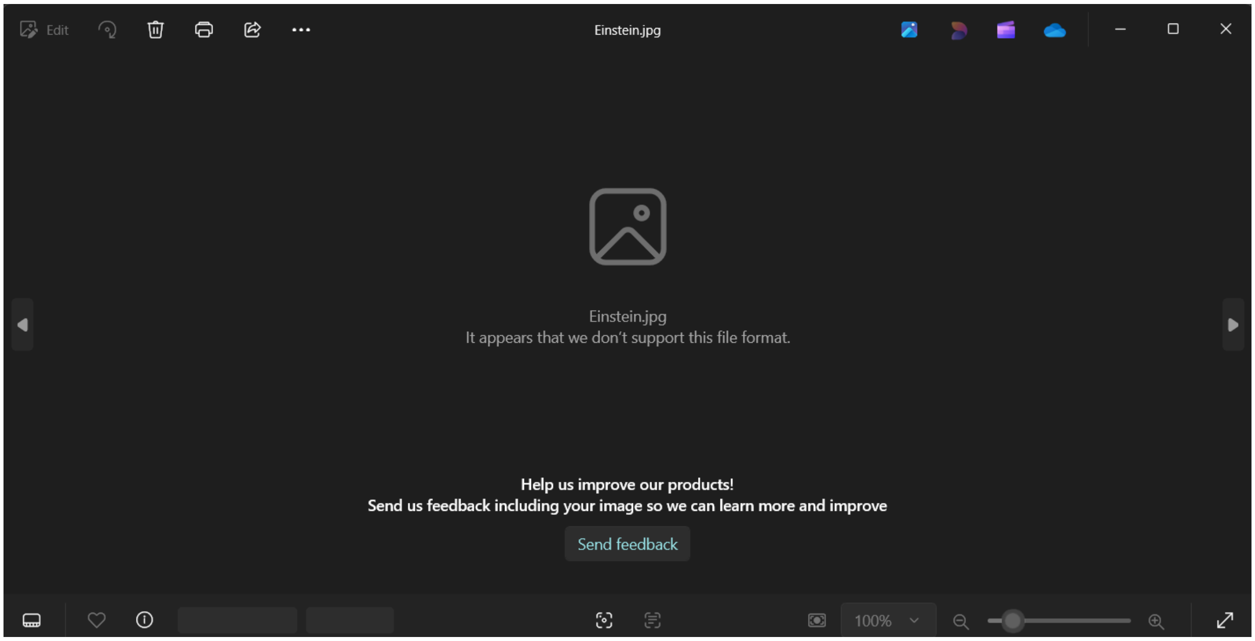
A lost letter from Albert Einstein contains a hidden equation encrypted inside an image. Crack the code to reveal the flag!

0/5 attempts

What we got ?

1. Einstein.jpg
2. Youtube link direct to a video named *The Real Meaning of E=mc²*

Click on the Einstein.jpg :



Einstein.jpg
It appears that we don't support this file format.

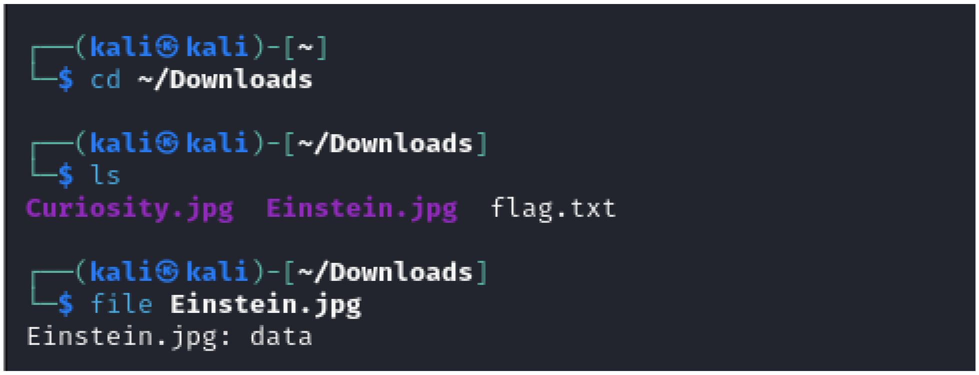
Help us improve our products!
Send us feedback including your image so we can learn more and improve

Hmm… there's some possibility here (but not limited to):

1. Corrupted header
2. Fake extension given (which it's originally with different type of extension like png/zip but renamed with .jpg)
3. It's embedded data, which the file might be a polyglot that containing both a valid image and another file type (like image + ZIP)

Let's try!

Then let's check the type file.



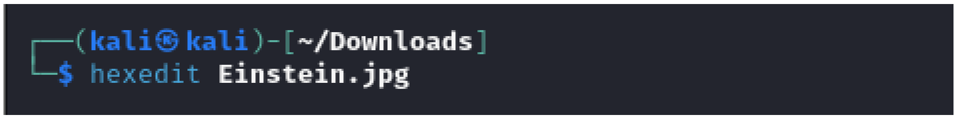
```
┌──(kali㉿kali)-[~]
└─$ cd ~/Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
Curiosity.jpg  Einstein.jpg  flag.txt

┌──(kali㉿kali)-[~/Downloads]
└─$ file Einstein.jpg
Einstein.jpg: data
```

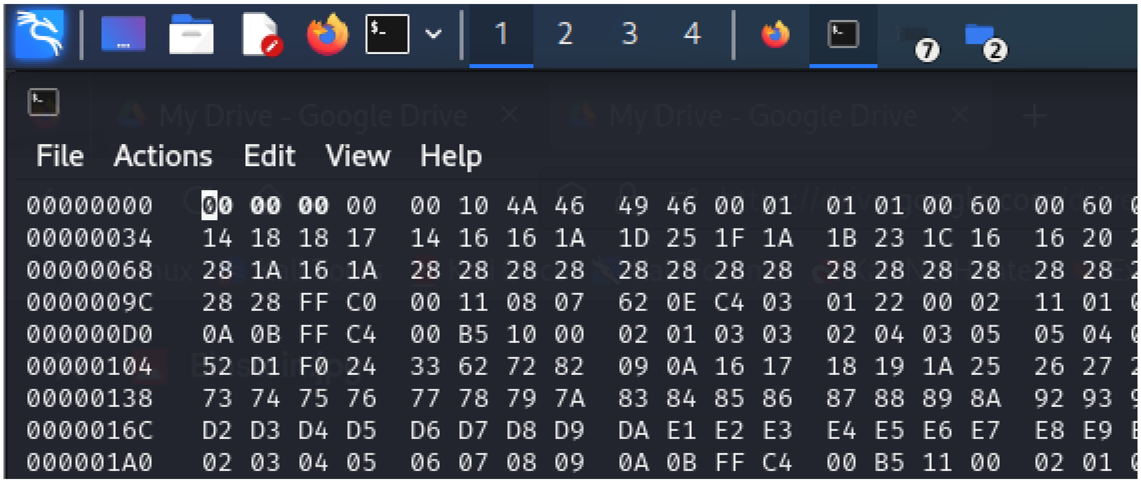
Okay, seems like the header is corrupted. So now, we need to open the hex editor to check on this image's header. As we know:

JPEG files (compressed images) start with an image marker which always contains the marker code hex values FF D8 FF



```
┌──(kali㉿kali)-[~/Downloads]
└─$ hexedit Einstein.jpg
```

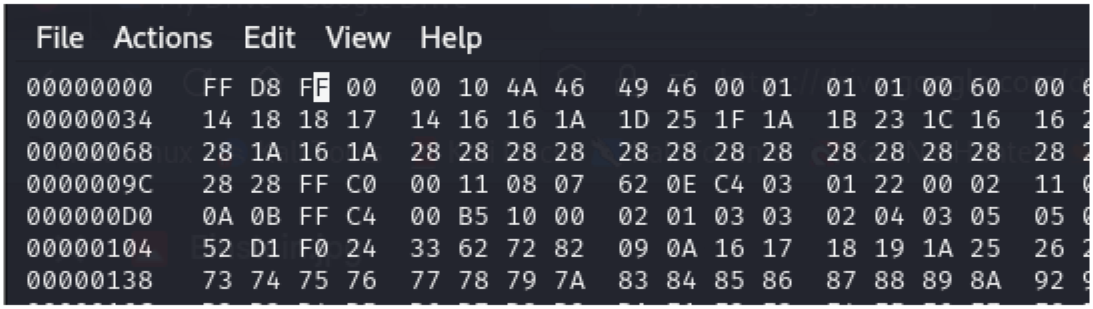
And the current header:



```
00000000   00 00 00 00  00 10 4A 46  49 46 00 01  01 01 00 60  00 60
00000034   14 18 18 17  14 16 16 1A  1D 25 1F 1A  1B 23 1C 16  16 20
00000068   28 1A 16 1A  28 28 28 28  28 28 28 28  28 28 28 28  28 28
0000009C   28 28 FF C0  00 11 08 07  62 0E C4 03  01 22 00 02  11 01
000000D0   0A 0B FF C4  00 B5 10 00  02 01 03 03  02 04 03 05  05 04
00000104   52 D1 F0 24  33 62 72 82  09 0A 16 17  18 19 1A 25  26 27
00000138   73 74 75 76  77 78 79 7A  83 84 85 86  87 88 89 8A  92 93
0000016C   D2 D3 D4 D5  D6 D7 D8 D9  DA E1 E2 E3  E4 E5 E6 E7  E8 E9
000001A0   02 03 04 05  06 07 08 09  0A 0B FF C4  00 B5 11 00  02 01
```

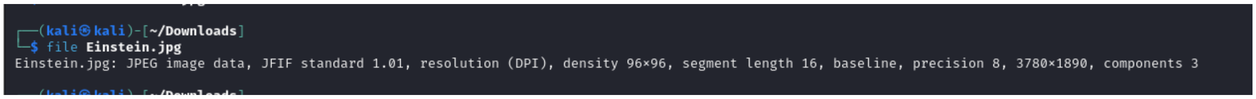
Alright, so the header now is 00 00 00, which is corrupted.

And now, we will change the header to FF D8 FF:



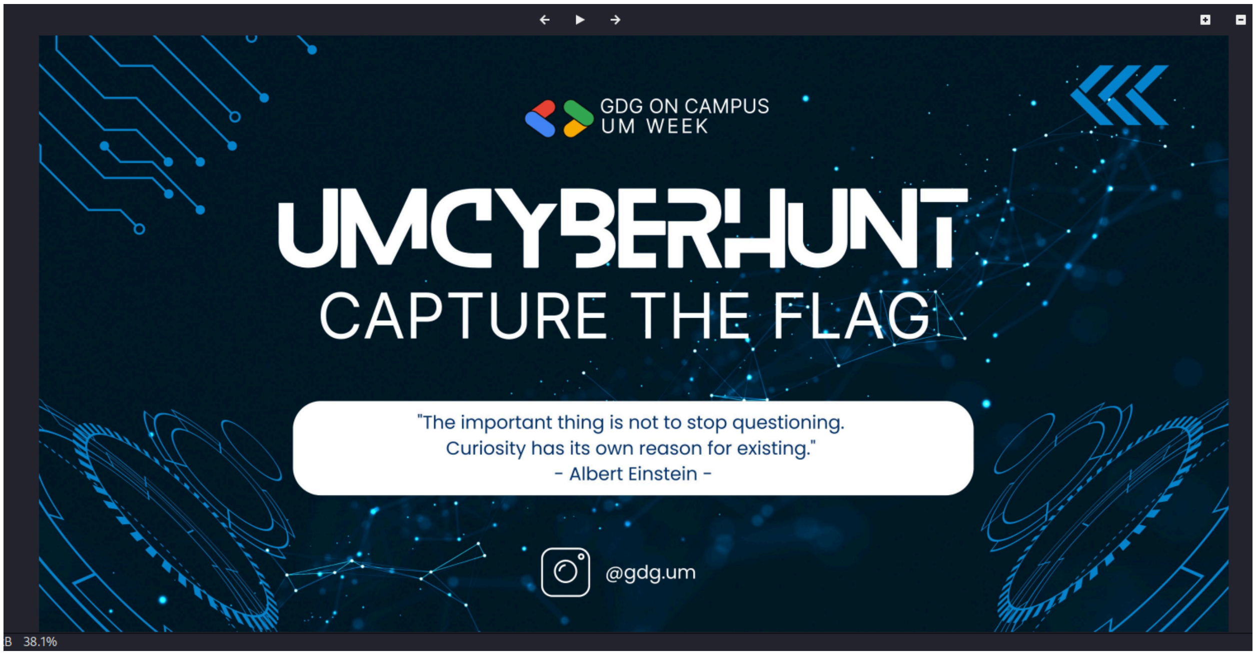
```
00000000   FF D8 FF 00  00 10 4A 46  49 46 00 01  01 01 00 60  00
00000034   14 18 18 17  14 16 16 1A  1D 25 1F 1A  1B 23 1C 16  16
00000068   28 1A 16 1A  28 28 28 28  28 28 28 28  28 28 28 28  28
0000009C   28 28 FF C0  00 11 08 07  62 0E C4 03  01 22 00 02  11
000000D0   0A 0B FF C4  00 B5 10 00  02 01 03 03  02 04 03 05  05
00000104   52 D1 F0 24  33 62 72 82  09 0A 16 17  18 19 1A 25  26
00000138   73 74 75 76  77 78 79 7A  83 84 85 86  87 88 89 8A  92
```

When we check the file type:



```
┌──(kali㉿kali)-[~/Downloads]
└─$ file Einstein.jpg
Einstein.jpg: JPEG image data, JFIF standard 1.01, resolution (DPI), density 96×96, segment length 16, baseline, precision 8, 3780×1890, components 3
```

This shows the file has been fixed.
And now we open the image file.


GDG ON CAMPUS
UM WEEK
UMCYBERHUNT
CAPTURE THE FLAG
"The important thing is not to stop questioning.
Curiosity has its own reason for existing."
- Albert Einstein -
@gdg.um
B 38.1%

Okay seems like there's nothing in the image, but wait hmmm, maybe something is hidden as question mentioned there's a hidden equation in the image.
Now, we will try to extract and see if there's any hidden data under the image file.

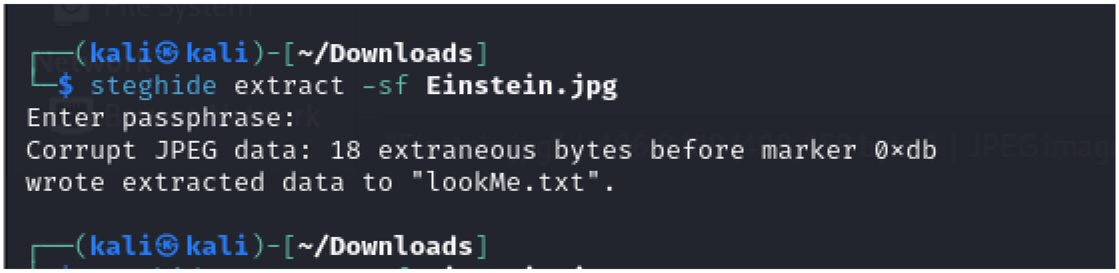
Introduction to tools

Steghide

- Hide secret data inside a cover file (.jpg / .bmp / .wav / .au , but not PNG!!!).
- Extract hidden data from a file (if something was embedded before).

Okay, a passphrase is asked to be entered. Well, let's look again the question. Other than the description that told us there's hidden message. A youtube link is inserted. Ah well, do we need to revise again the physics knowledge? Not really, let's try with the title "The Real Meaning of E=mc²".

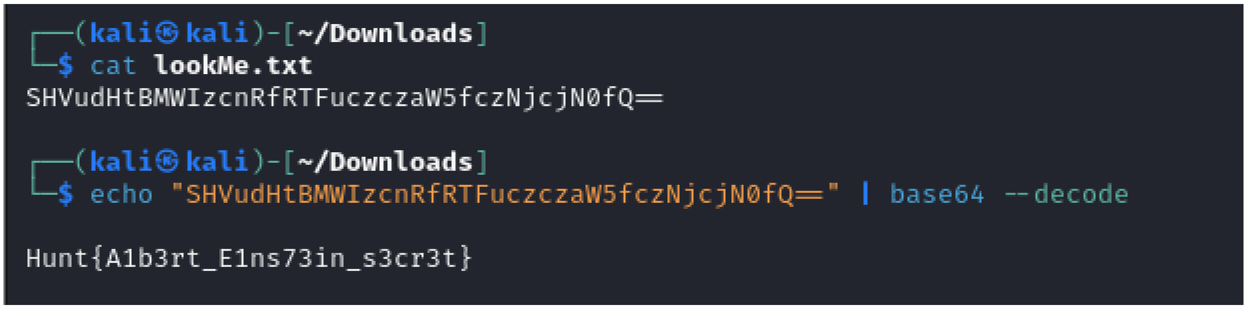
We can try with E=mc2, e=mc2, E=MC2, E=mc^2, E=MC^2, and e=mc^2.



```
┌──(kali㉿kali)-[~/Downloads]
└─$ steghide extract -sf Einstein.jpg
Enter passphrase:
Corrupt JPEG data: 18 extraneous bytes before marker 0xdb
wrote extracted data to "lookMe.txt".

┌──(kali㉿kali)-[~/Downloads]
```

Yay, we got a lookMe.txt. Let’s read it.



```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat lookMe.txt
SHVudHtBMWIzcnRfRTFuczczaW5fczNjcjN0fQ==

┌──(kali㉿kali)-[~/Downloads]
└─$ echo "SHVudHtBMWIzcnRfRTFuczczaW5fczNjcjN0fQ==" | base64 --decode

Hunt{A1b3rt_E1ns73in_s3cr3t}
```

We will get a base 64 strings, then decode it and you will get the flag!!
Yo congrats !