

Information

Forensics

Description:

Files can always be changed in a secret way. Can you find the flag? [cat.jpg](#)

Hints:

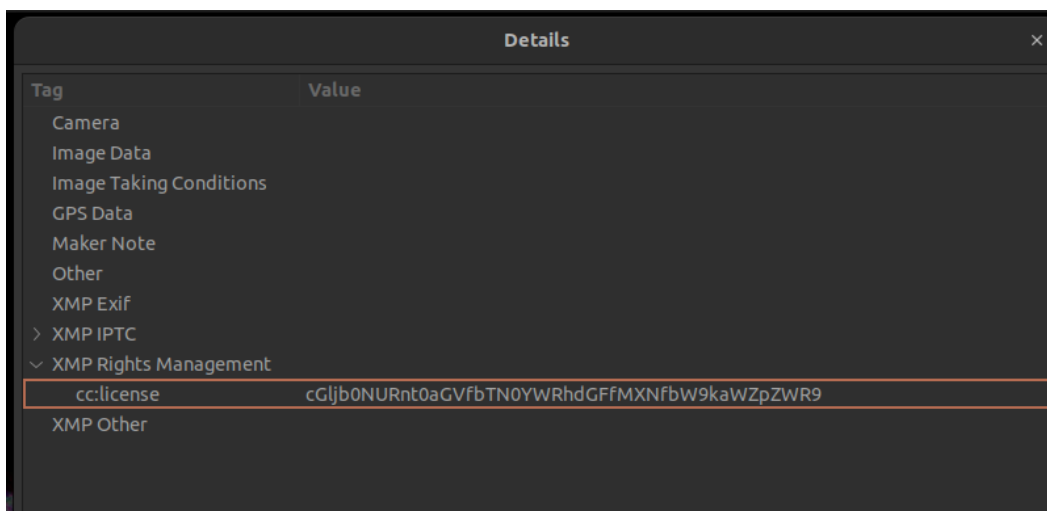
- 1) Look at the details of the file.
- 2) Make sure to submit the flag as picoCTF{XXXXXX}

Solution:

- 1) Identify the file type and get details of the image.

```
shouvik028@shouvik028-Aspire-A715-75G:~/Downloads$ identify cat.png
identify-im6.q16: unable to open image 'cat.png': No such file or directory @ error/blob.c/
OpenBlob/2924.
shouvik028@shouvik028-Aspire-A715-75G:~/Downloads$ identify cat.jpg
cat.jpg JPEG 2560x1598 2560x1598+0+0 8-bit sRGB 878136B 0.000u 0:00.000
shouvik028@shouvik028-Aspire-A715-75G:~/Downloads$ identify -vverbose cat.jpg
identify-im6.q16: unrecognized option '-vverbose' @ error/identify.c/IdentifyImageCommand/89
8.
shouvik028@shouvik028-Aspire-A715-75G:~/Downloads$ identify -verbose cat.jpg
Image:
  Filename: cat.jpg
```

- 2) Open image in some image editing software to get more details.
- 3) Under the XMP rights management we see a string that looks like its encoded in Base64.




4) Use a decoder to find the flag.

Decode from Base64 format

Simply enter your data then push the decode button.

cGlib0NURnt0aGVfbTN0YWRhdGFfMXNfbW9kaWZpZW99

 For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8

Source character set.

☐

Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF

Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE >

Decodes your data into the area below.

picoCTF{the_m3tadata_1s_modified}

Flag: picoCTF{the_m3tadata_1s_modified}