

CYS REPORT

~ Advait Sathish Kumar
(CH.SC.U4CSE24004)

Task 1: "This garden contains more than it seems"

Methodology:

- I used Notepad to open the image file directly.
- Upon scrolling to the bottom of the file, I found the flag appended as plain text at the end of the file content.

```
všCýNUL!STÄ½jÓýZýNUL°+Ü`ç`Hñ=ÜSÖ'="b0$RSufÊD™SO PăPŢ`ýE[µûç¼iA4Ùçó  
NAK¿/úæýNULu«Y`() ,ó=7g&RS'áv2<³mjx/^û,c!}ØGSÇnkçkSUBÖISOÄ¥trSOHé  
èDELÿÜHere is a flag "picoCTF{more_than_m33ts_the_3y3657BaB2C}"
```

Flag:

picoCTF{more_than_m33ts_the_3y3657BaB2C}

Task 2: "Files can always be changed in a secret way. Can you find the flag?"

Methodology:


- I used a **metadata and EXIF extractor** to retrieve embedded metadata from the image file.
- In the extracted metadata, I found a random string that seemed suspicious.


License

cGljb0NURnt0aGVfbTN0YWRRhdGFfMXNfbW9kaWZpZW9


- Upon decoding the string using a **Base64 decoder**, the flag was revealed.



cGlib0NURnt0aGVfbTN0YWRhdGFfMXNfbW9kaWZpZW99

 For encoded binaries (like images, documents, etc.) use the file upl

UTF-8  Source character set.

☐ Decode each line separately (useful for when you have multiple enti

 Live mode OFF Decodes in real-time as you type or paste (s

 **DECODE**  Decodes your data into the area below.

picoCTF{the_m3tadata_1s_modified}

Flag:

picoCTF{the_m3tadata_1s_modified}

Task 3: "There will always be more than what it seems to contain."

Methodology:

- Using **Command Prompt**, I ran the following command to extract files from the image:

```
tar -xf flag.png
```

- This process extracted a folder containing another image.
- Upon viewing the extracted image, the flag was clearly visible.

```
picoCIF{Hiddinng_An_imag3_within_@n_image_96539bea}
```

Flag:

```
picoCIF(Hiddinng_An_imag3_within_@n_image_96539bea)
```