Ignite Hacathon {2024}

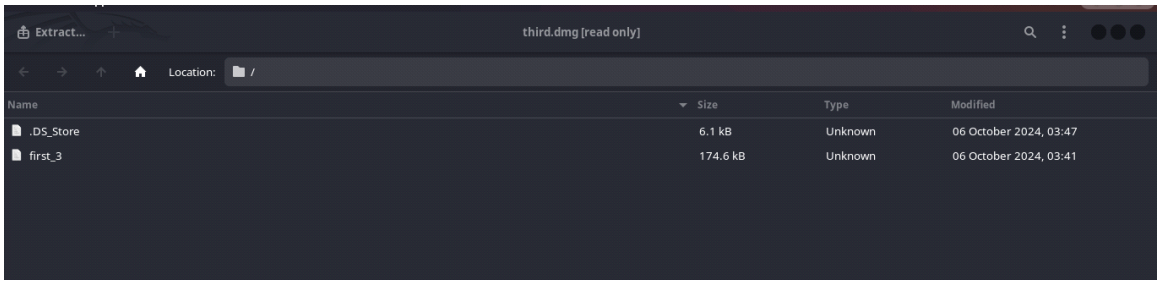
DFIR : -->"Tanker" (50 points)

Sol 1:

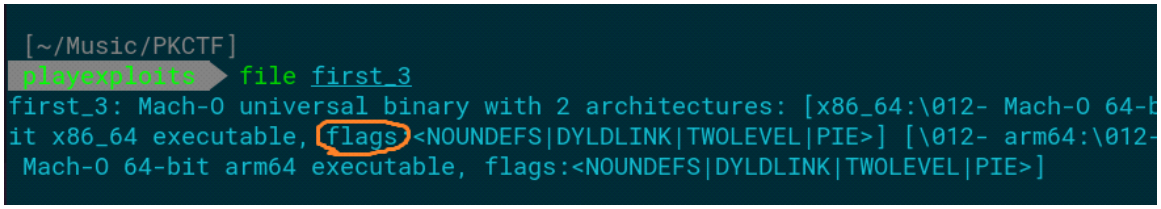
--> This is the tanker challenge, when we read it we simply get that we have to just retrieve the data. So I downloaded the file and check the type of file using this command.

```
[~/Music/PKCTF]
playexploits ▶ file third.dmg
third.dmg: zlib compressed data
```

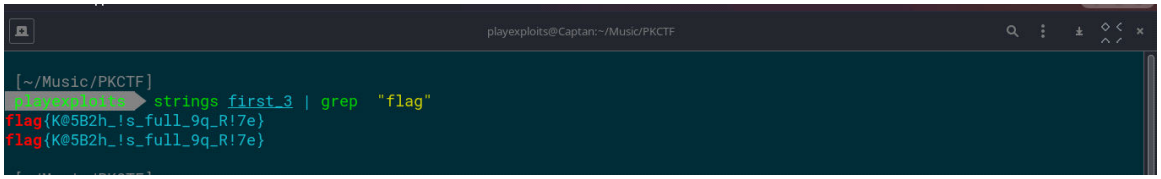
--> Ok, it has compress data. So I simple double click the file and I saw this.



--> Then I just Extracted the both file, then I saw that first_3 is like executable file so i tried to run it but faild, then when i use the file command to see the file type it shows a flag word.



--> Then I simply use the basic command to see the word flag and I get this.

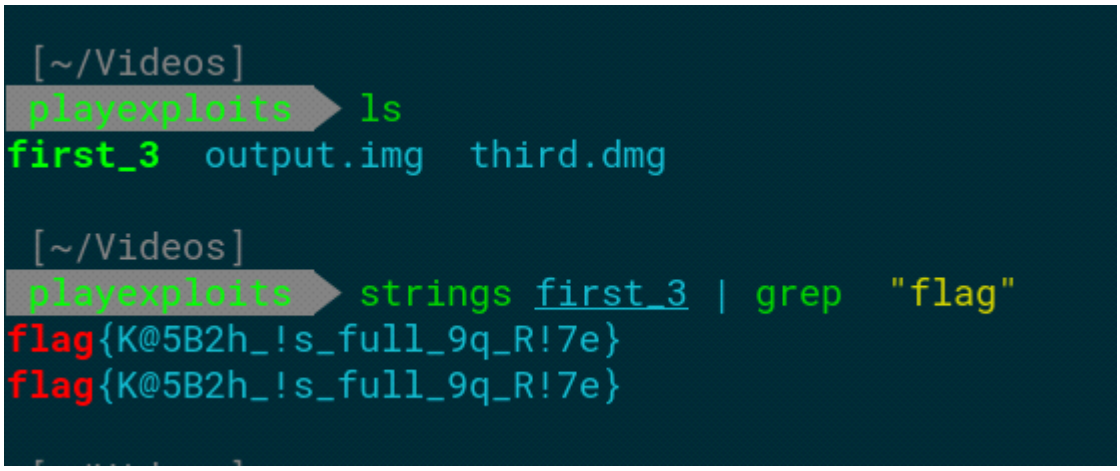


--> Really, I just found the flag but wait there is no one solution I will tell you more for your future DFIR Ctf,s.

Sol 2:

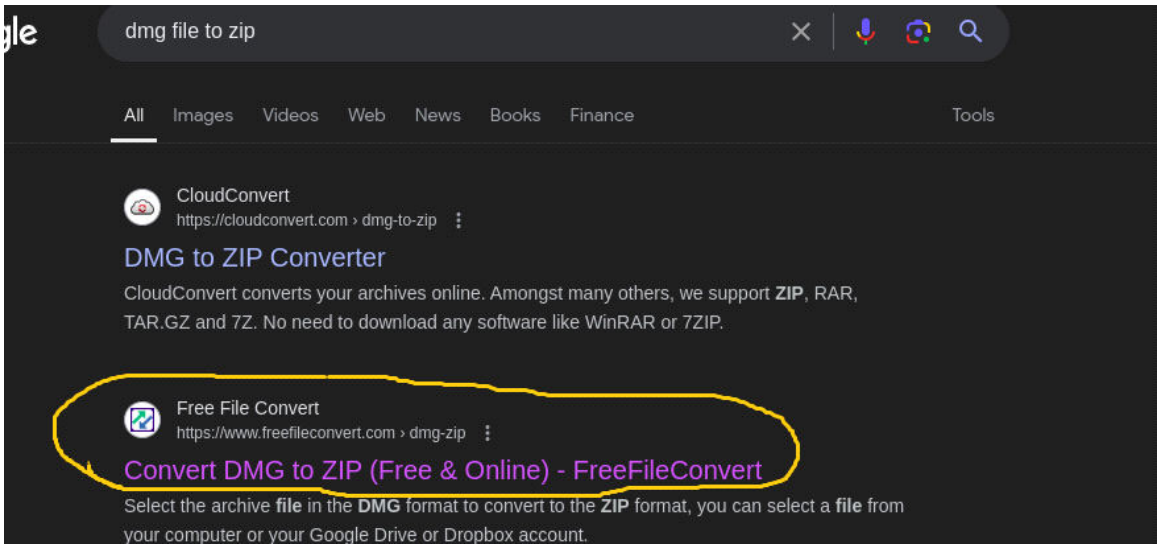
--> In this solution I simply did this.

--> And this I simply found the same first_3 file and I just did this.

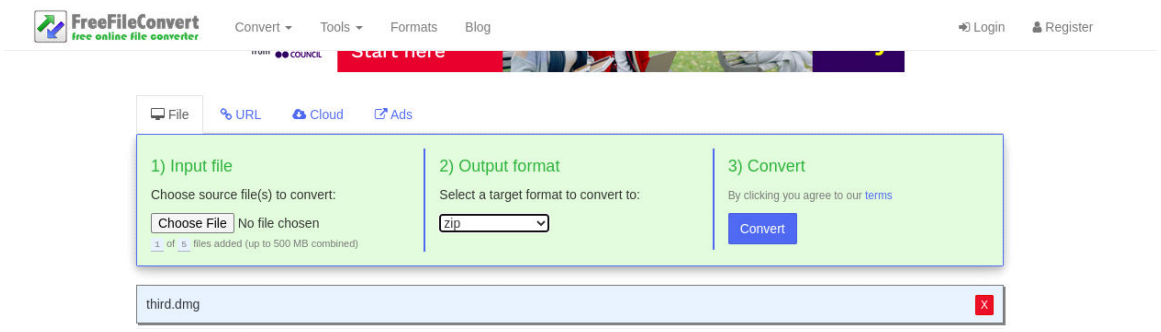


Sol 3 :

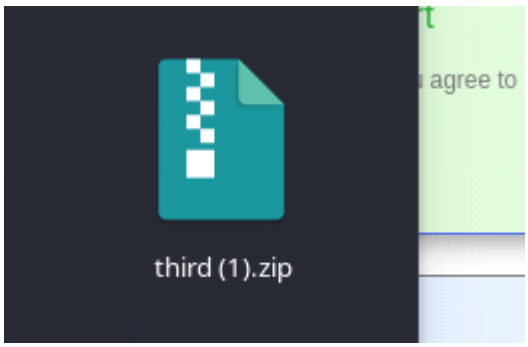
--> In this solution I simple write in web browser that (.dmg convertor into zip) and then I found this one.



-->Then simply I gave input my .dmg file and then in output I changed it to zip. Like this.



--> Then I just download it and this is the zip file.



--> Then i extracted and now this is the main folder.

--> After opening folder, I found these two files.

--> And atlast I use my favourite method, And as aspected. There it is.

```
[~/Music/PKCTF/third]
playexploits ➤ ls
4.cpu16777228  4.x64

[~/Music/PKCTF/third]
playexploits ➤ strings 4.cpu16777228 | grep  "flag"
flag{K@5B2h_!s_full_9q_R!7e}

[~/Music/PKCTF/third]
playexploits ➤ _
```

--> THE FLAGGGGGGGG!!!!

[And The main I want to tell you that I didn,t played or studied any forencics, because I have

taken the andriod catagory ,and just by using my normal ctf skill I found it.]

Thanks alot for reading :)

By PlayExploits...