**hide and split**

***Forensic***

**Challenge:**

Explore this disk image file, maybe you can find something hidden in it.

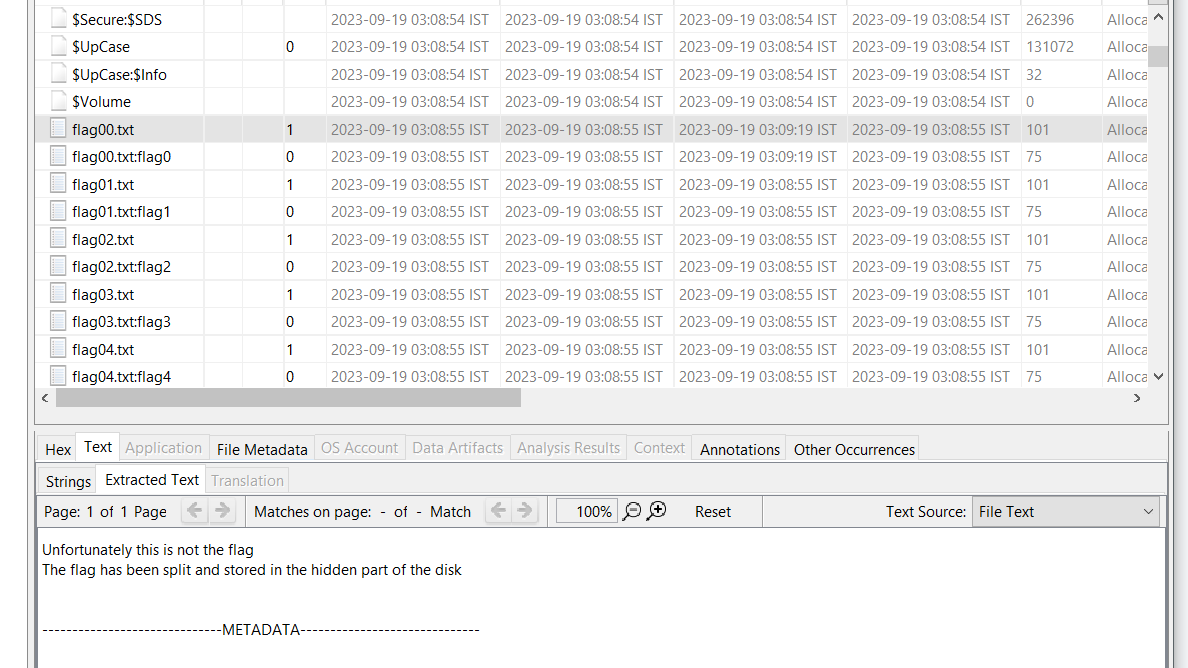
Attached - challenge.zip

**Approach:**

The zip file contained only one file, a challenge.ntfs file, for those who don’t know what NTFS is, I'd recommend you to go read about it first, it’s very cool!

Continuing with the challenge, the question says something about “hidden”, maybe it has hidden files in it?

We open the file in autopsy and see that it has several text files named flag00.txt to flag99.txt, and it all had the same data:

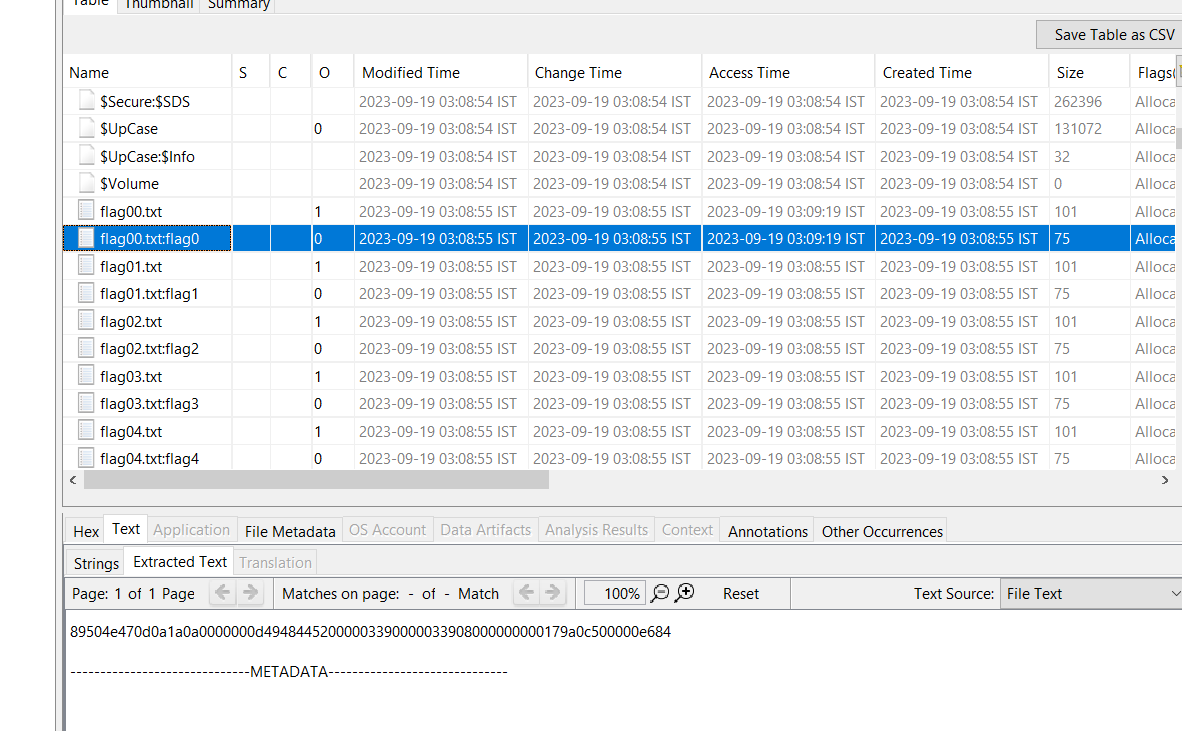


“Unfortunately this is not the flag

The flag has been split and stored in the hidden part of the disk”

We see there are more files, one for each of the text file named as flag00.txt:flag0 to flag99.txt:flag99

…and it had this weird looking data, something like a hex?

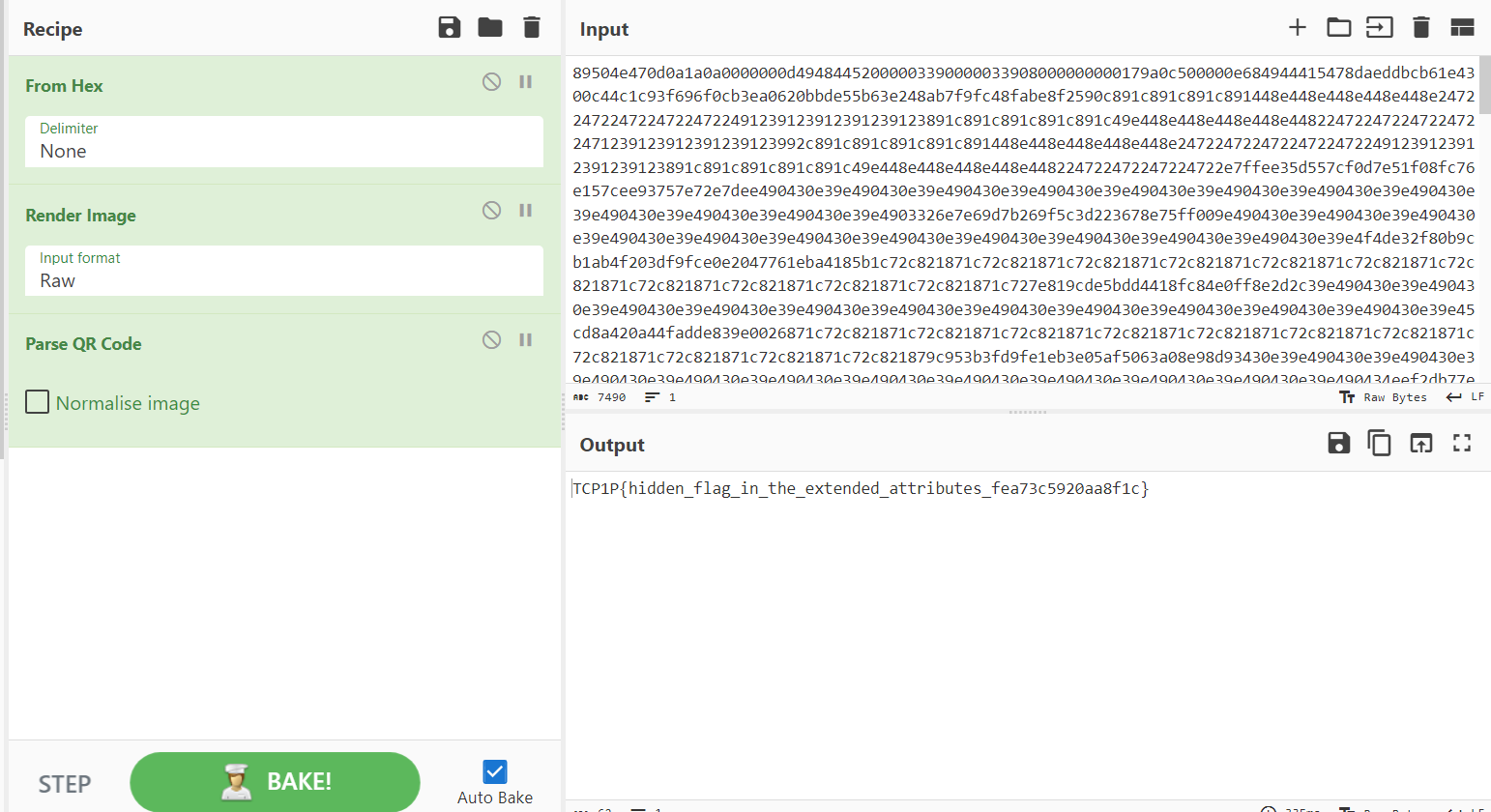


Luckily, i convert the “supposedly” hex in the flag00.txt:flag0 file and got this:

I saw this “PNG” and “IHDR” which hinted maybe?? maybe this is a PNG file??

..and this is what i meant by being lucky, if i would’ve decoded the hex from some other file, it’d have given me some gibberish data and i would’ve discarded this approach.

I copy pasted all the data in cyberchef and it translated into a PNG of a QR code, which further decrypted into the flag:



**Flag: TCP1P{hidden\_flag\_in\_the\_extended\_attributes\_fea73c5920aa8f1c}**

Congrats!!

Happy Hacking!