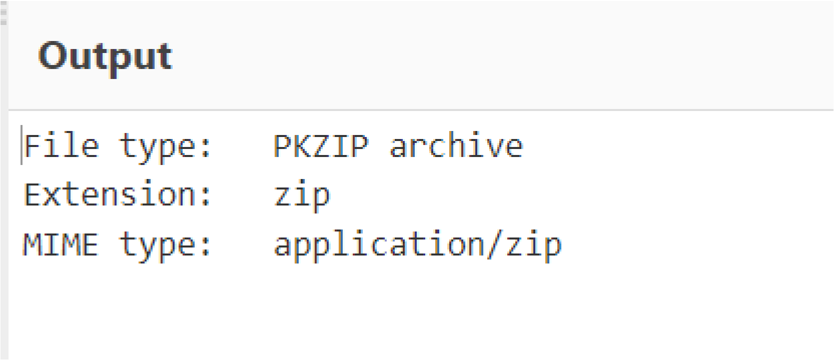
Ahmed Umar Rehman

I221580 Section A

Digital Forensics Lab#1

Task 01: What is wrong with dog.png. Hint Cyberchef

Ans:



```
File type:   PKZIP archive
Extension:   zip
MIME type:   application/zip
```

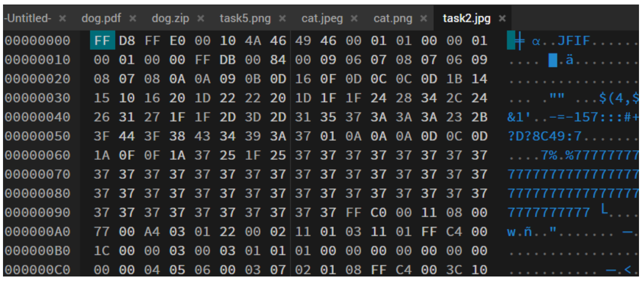
The file name should be PKZIP

Task 02: Can you check Image.jpg and recover the file.

Check for magic bytes in hexed and match them with jpg magic bytes on Gary Kessler’s site.

Ans:

The image.png is recovered



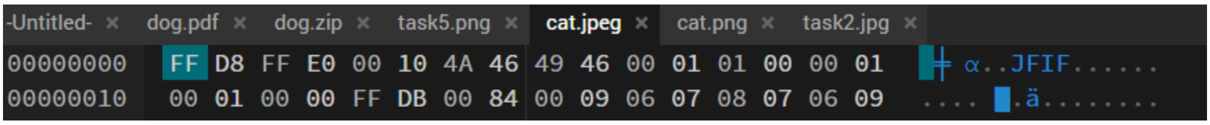
```
00000000  FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01  ╪ α..JFIF......
00000010  00 01 00 00 FF DB 00 84 00 09 06 07 08 07 06 09  .... █.ä........
00000020  08 07 08 0A 0A 09 0B 0D 16 0F 0D 0C 0C 0D 1B 14  ................
00000030  15 10 16 20 1D 22 22 20 1D 1F 1F 24 28 34 2C 24  ... .""  ...$(4,$
00000040  26 31 27 1F 1F 2D 3D 2D 31 35 37 3A 3A 3A 23 2B  &1'..-=-157:::#+
00000050  3F 44 3F 38 43 34 39 3A 37 01 0A 0A 0A 0D 0C 0D  ?D?8C49:7.......
00000060  1A 0F 0F 1A 37 25 1F 25 37 37 37 37 37 37 37 37  ....7%.%77777777
00000070  37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37  7777777777777777
00000080  37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37  7777777777777777
00000090  37 37 37 37 37 37 37 37 37 37 FF C0 00 11 08 00  7777777777 └....
000000A0  77 00 A4 03 01 22 00 02 11 01 03 11 01 FF C4 00  w.ñ..".......  ─.
000000B0  1C 00 00 03 00 03 01 01 01 00 00 00 00 00 00 00  ................
000000C0  00 00 04 05 06 00 03 07 02 01 08 FF C4 00 3C 10  ...........  ─.<.
```

Task 03: Does changing the extension change magic bytes of the file. Try and add screenshots with

explanation.

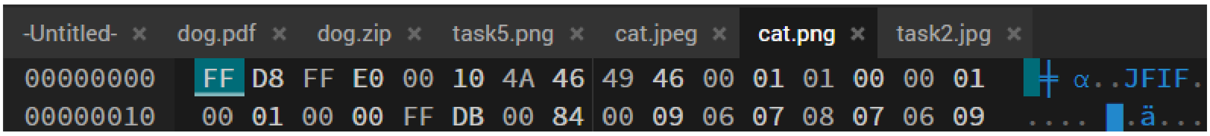
Ans:

No, it doesn't change the magic bytes. The proof of screenshot is given below



```
00000000  FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01  ╪ α..JFIF......
00000010  00 01 00 00 FF DB 00 84 00 09 06 07 08 07 06 09  .... █.ä........
```

Cat.jpeg file



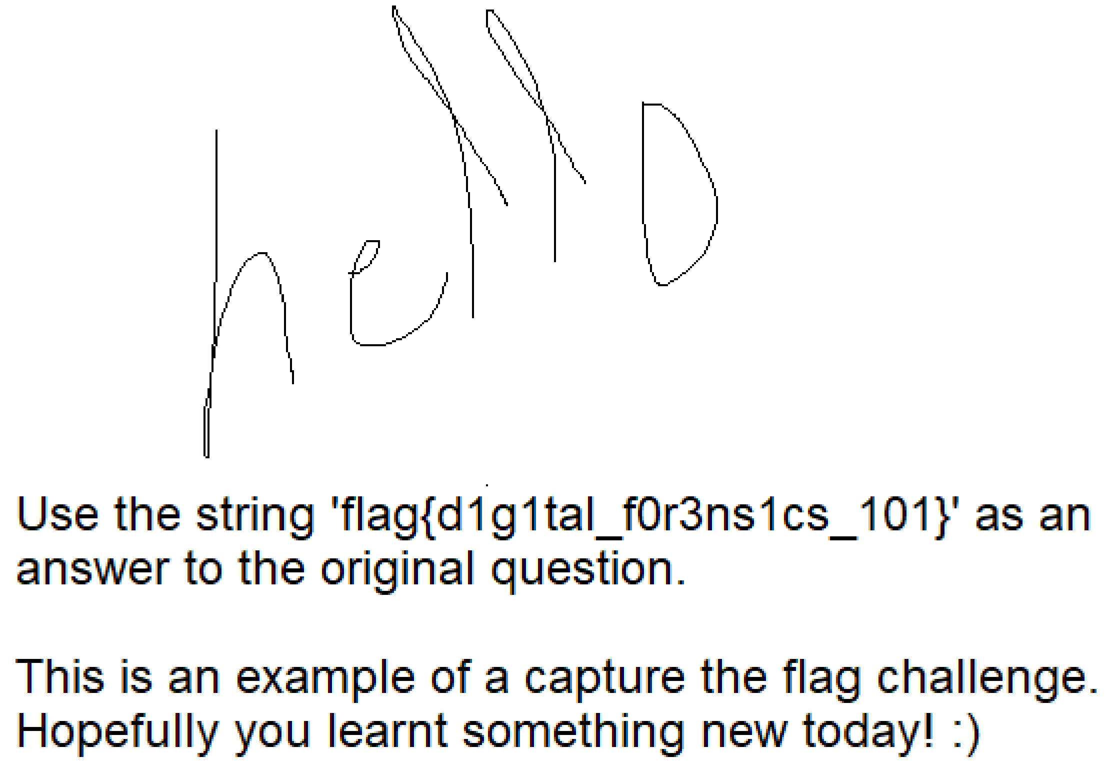
```
00000000  FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01  ╪ α..JFIF.
00000010  00 01 00 00 FF DB 00 84 00 09 06 07 08 07 06 09  .... █.ä...
```

Cat.png file

Task 04: Can you recover the challenge.png file. Flag format flag{}.

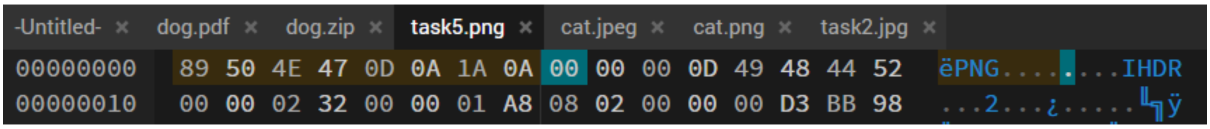
Ans:

Yes, we can recover the file



Use the string 'flag{d1g1tal_f0r3ns1cs_101}' as an answer to the original question.

This is an example of a capture the flag challenge. Hopefully you learnt something new today! :)



```
00000000   89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52   ëPNG........IHDR
00000010   00 00 02 32 00 00 01 A8 08 02 00 00 00 D3 BB 98   ...2...¿.....╙╗ÿ
```

Since the original picture magic bytes was not on the other website gaykessler then search png file in gaykessler and we found the magic bytes

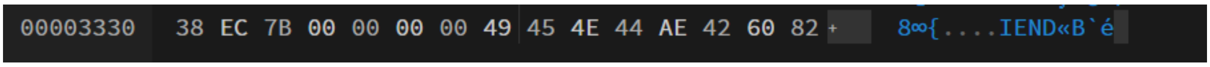
Task 05: What if magic bytes are totally out of place, how can we check for a file type? Hint:

“I have wheels, yet I'm not a car. I am big, but I'm not a star. Pull me along, I'll carry your load.

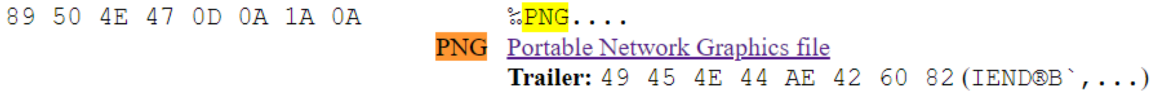
Inside me, stories are often showed.”

Ans:

We can check through the last magic bytes of the challenge.png file and match trailer bytes



```
00003330   38 EC 7B 00 00 00 00 49 45 4E 44 AE 42 60 82     8∞{....IEND«B`é
```



```
89 50 4E 47 0D 0A 1A 0A          ‰PNG....
                            PNG  Portable Network Graphics file
                                 Trailer: 49 45 4E 44 AE 42 60 82 (IEND®B`‚...)
```

Task 06 [Bonus]:

Can you recover Boss.png?

Ans: