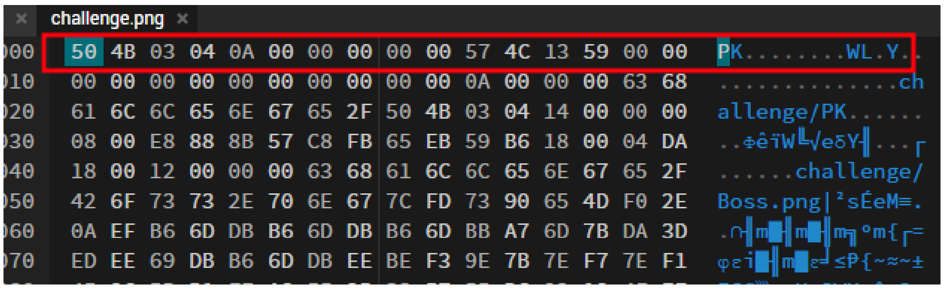
Digital Forensics-Lab 01 Report

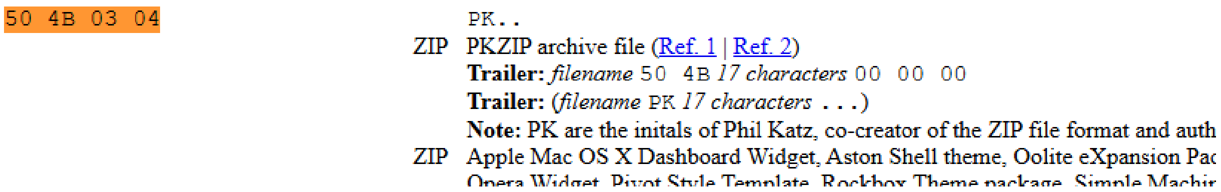
I22-1609_Ahmad-Abdullah

Task 01: **What is wrong with challenge.png.** Hint Cyberchef

Ans: The file's extension was changed which was different from the header defined in its hex.



```
challenge.png
000   50 4B 03 04 0A 00 00 00 00 00 57 4C 13 59 00 00   PK........WL.Y..
010   00 00 00 00 00 00 00 00 00 00 0A 00 00 00 63 68   ..............ch
020   61 6C 6C 65 6E 67 65 2F 50 4B 03 04 14 00 00 00   allenge/PK......
030   08 00 E8 88 8B 57 C8 FB 65 EB 59 B6 18 00 04 DA   ..ΦêïW╚√eδY╢...┌
040   18 00 12 00 00 00 63 68 61 6C 6C 65 6E 67 65 2F   ......challenge/
050   42 6F 73 73 2E 70 6E 67 7C FD 73 90 65 4D F0 2E   Boss.png|²sÉeM≡.
060   0A EF B6 6D DB B6 6D DB B6 6D BB A7 6D 7B DA 3D   .∩╢m█╢m█╢m╗ºm{┌=
070   ED EE 69 DB B6 6D DB EE BE F3 9E 7B 7E F7 7E F1   φεi█╢m█ε╛≤₧{~≈~±
```



`50 4B 03 04`

PK..

ZIP PKZIP archive file (Ref. 1 | Ref. 2)

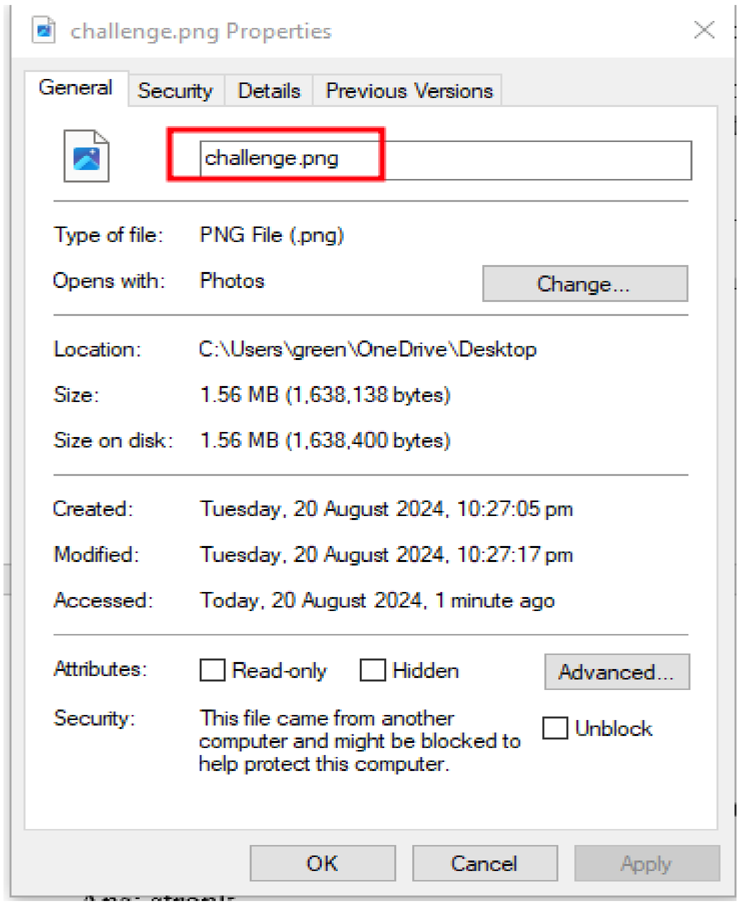
Trailer: *filename* 50 4B *17 characters* 00 00 00

Trailer: (*filename* PK *17 characters* . . .)

Note: PK are the initals of Phil Katz, co-creator of the ZIP file format and auth

ZIP Apple Mac OS X Dashboard Widget, Aston Shell theme, Oolite eXpansion Pac

Opera Widget, Pivot Style Template, Rockbox Theme package, Simple Machir



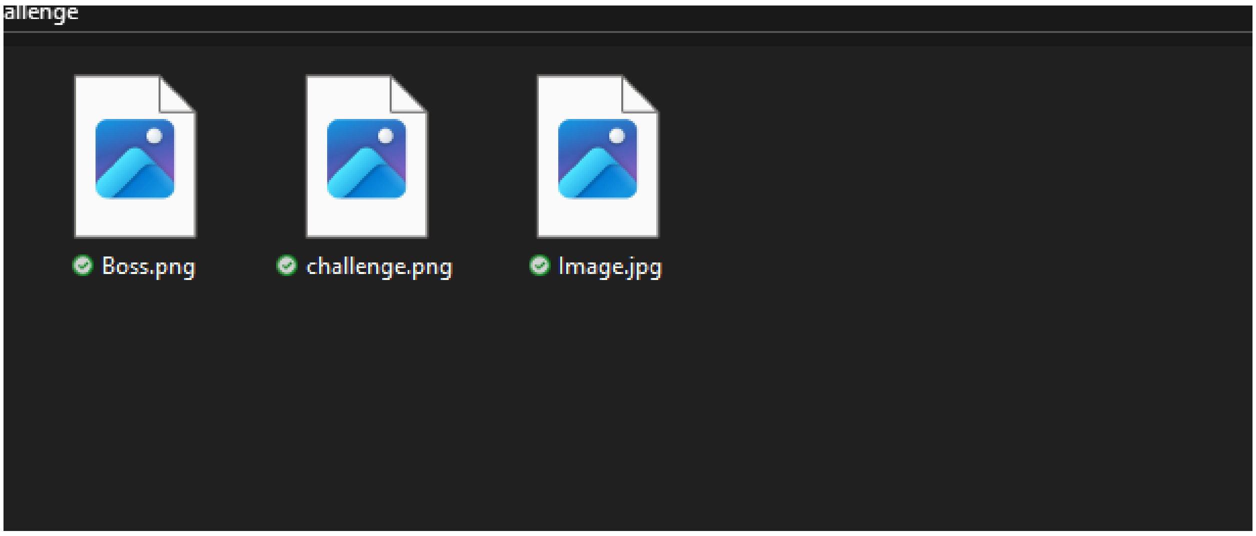
challenge.png Properties

General | Security | Details | Previous Versions

challenge.png

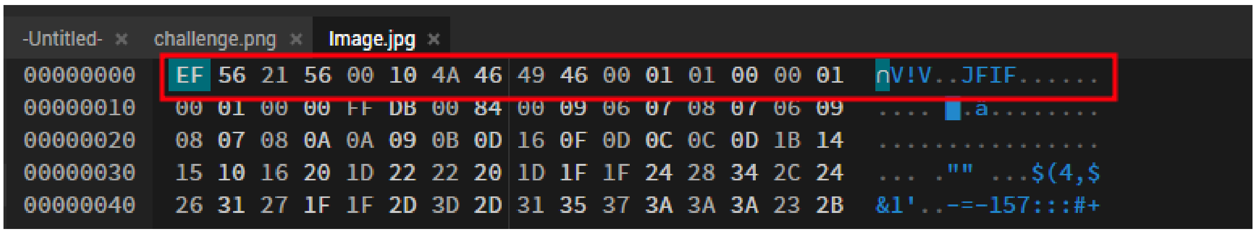
Type of file:	PNG File (.png)
Opens with:	Photos
Location:	C:\Users\green\OneDrive\Desktop
Size:	1.56 MB (1,638,138 bytes)
Size on disk:	1.56 MB (1,638,400 bytes)
Created:	Tuesday, 20 August 2024, 10:27:05 pm
Modified:	Tuesday, 20 August 2024, 10:27:17 pm
Accessed:	Today, 20 August 2024, 1 minute ago
Attributes:	☐ Read-only ☐ Hidden
Security:	This file came from another computer and might be blocked to help protect this computer. ☐ Unblock

- Changing the extension of the file from *PNG* to *zip* runs the file in its original state which shows us that there are 3 more *PNG* files compressed in *challenge.zip*.



Task 02: Can you check Image.jpg and recover the file? Flag format FLAG{text_in_image}.
Hint: Check for magic bytes in hexed and match them with jpg magic bytes on Gary Kessler's site.

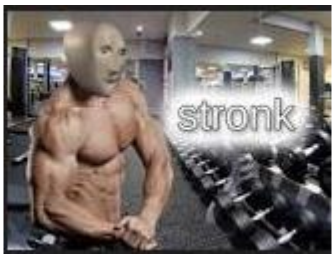
__Ans:__ Upon opening the Image.jpg we are welcomed with an error that the image is not supported. So we open the image in Hex Editor and instantly see that the image is not a jpg format file.



```
00000000  EF 56 21 56 00 10 4A 46 49 46 00 01 01 00 00 01  nV!V..JFIF......
00000010  00 01 00 00 FF DB 00 84 00 09 06 07 08 07 06 09  .... █.a........
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:::#+
```

Our next step is to identify what is the actual file type of the image.jpg using the Garykessler website. The hex *EF 56 21 56* is not defined as an extension in the Garykessler website so another approach is to change the hex of the image.jpg to the actual jpg hex which we can easily find on the same website.
This approach works and gives us the image below having text __*STRONK.*__

FLAG{stronk}.

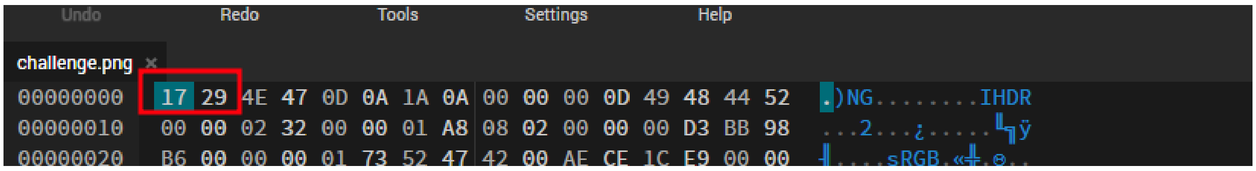


Task 03: Does changing the extension change the magic bytes of the file? Try to add screenshots with explanations.

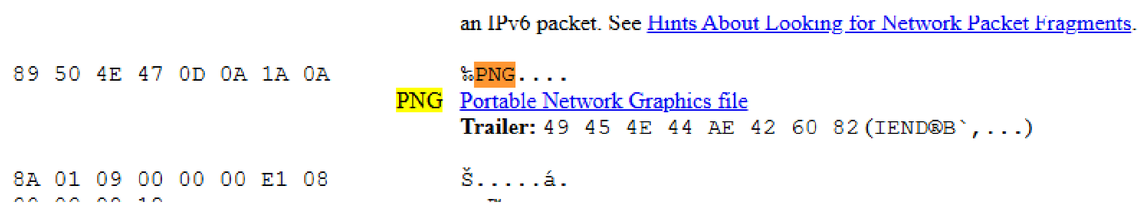
Ans: Changing the extension does not change the header HEX of the file the OS just tries to run the file with the user-defined extension which does not load the file type defined in the header.

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

Ans: This task was easier to than the above tasks as the we just needed to change the first 2 HEX of the header to make it complete *PNG* file



```
00000000  17 29 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52  .)NG........IHDR
00000010  00 00 02 32 00 00 01 A8 08 02 00 00 00 D3 BB 98  ...2...¿.....╚╗ÿ
00000020  B6 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00  ╢....sRGB.«╬.Θ..
```

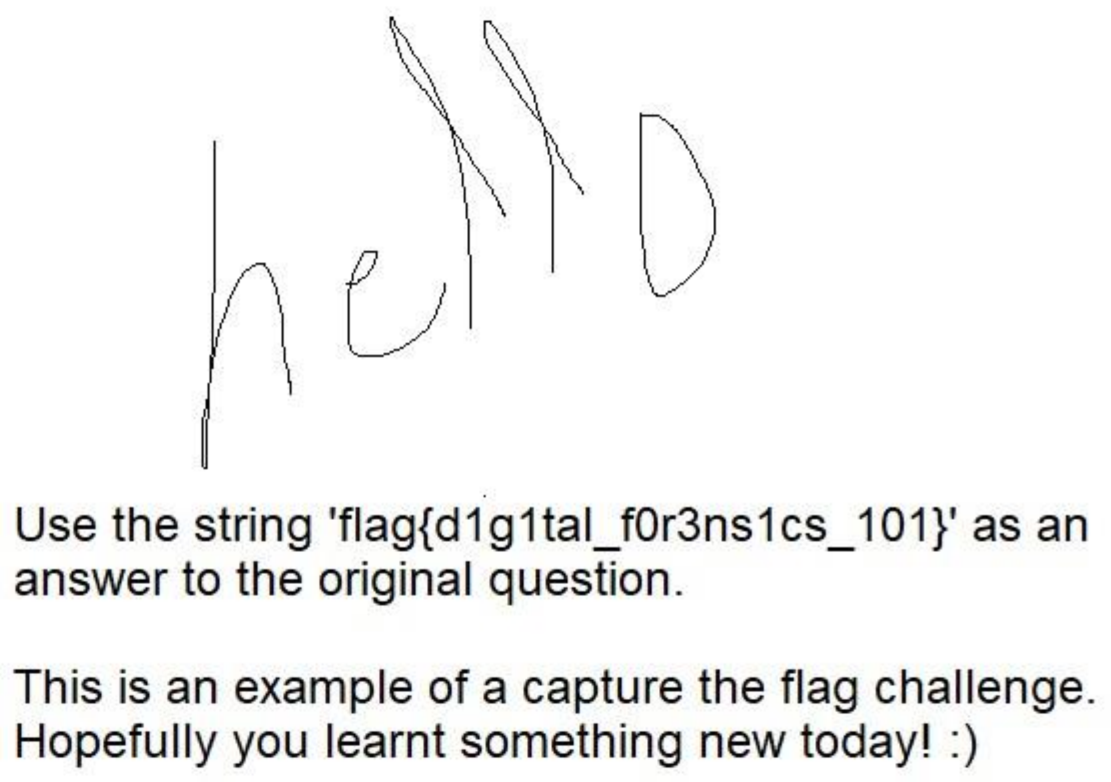


an IPv6 packet. See Hints About Looking for Network Packet Fragments.

```
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`,...)

8A 01 09 00 00 00 E1 08        Š.....á.
```

Doing this we recovered the imgae!



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! :)

flag{d1g1tak_f0r3ns1cs_101}

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.

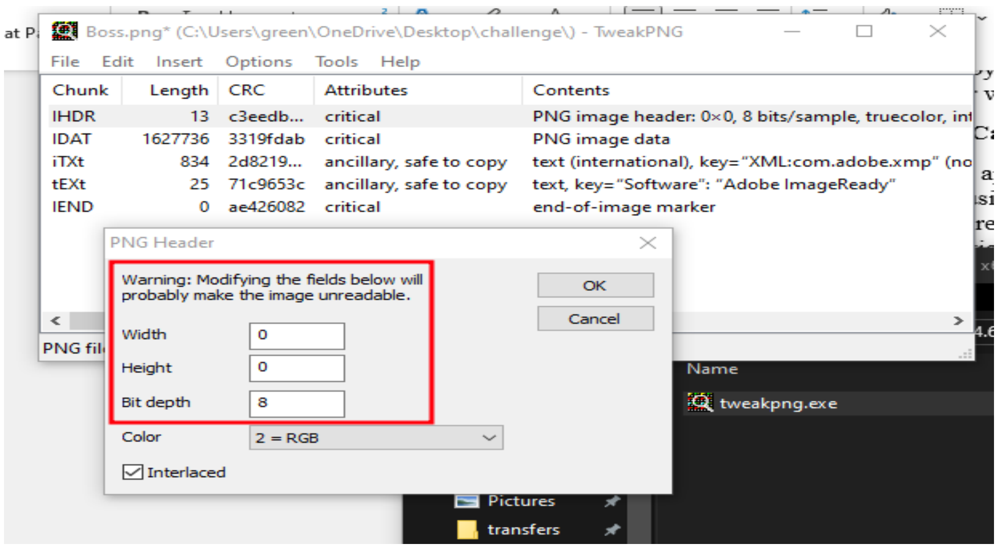
Inside me, stories are often shown.”

__Ans__: When magic bytes are out of place, it is better to use the a chunk editor which will show you the chunks out of order which we can then edit and correct as per our requirements.

Task 06 [Bonus]: Can you recover Boss.png?

__Ans:__ In this task, it appears that the chunks such as the header, data and end are out of place and we have to recover the file using a chunk editor such as *tweakpng*. We moved the chunks to their original place which should have recovered the image but it seems like there is one more problem with the file.
Upon further investigation, I found out that in the image data header, the resolution bits are NULL so naturally I had to brute-force the resolution

Flag{N0T_0nLy_D1m3ns1oNs_bu7_ChunK5_T0O}


Boss.png* (C:\Users\green\OneDrive\Desktop\challenge\) - TweakPNG

Chunk	Length	CRC	Attributes	Contents
IHDR	13	c3eedb...	critical	PNG image header: 0×0, 8 bits/sample, truecolor, int
IDAT	1627736	3319fdab	critical	PNG image data
iTXt	834	2d8219...	ancillary, safe to copy	text (international), key="XML:com.adobe.xmp" (no
tEXt	25	71c9653c	ancillary, safe to copy	text, key="Software": "Adobe ImageReady"
IEND	0	ae426082	critical	end-of-image marker

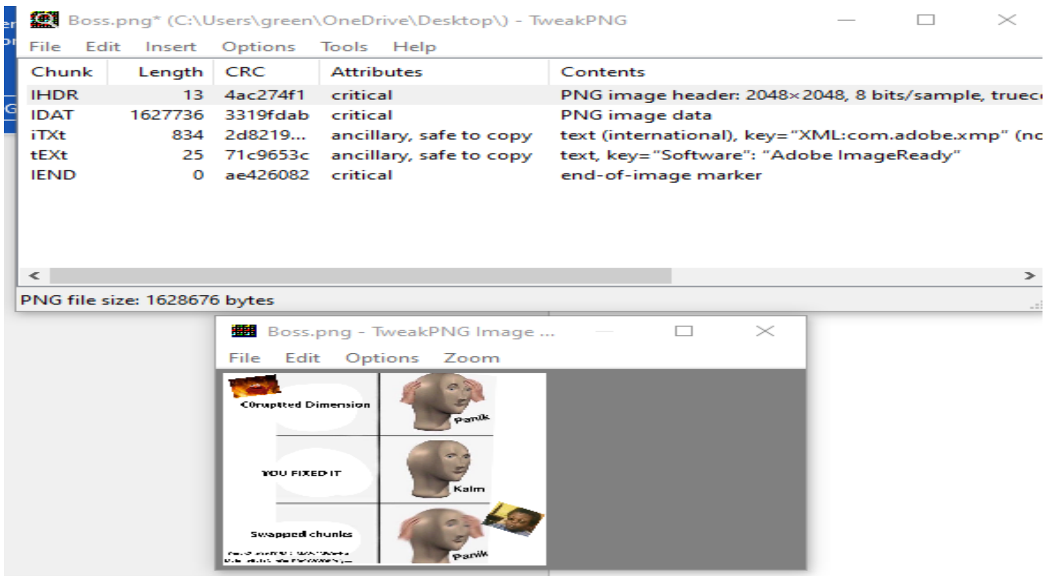
PNG Header

Warning: Modifying the fields below will probably make the image unreadable.

Width	0
Height	0
Bit depth	8
Color	2 = RGB

☑ Interlaced

For this, I used a Python script to brute-force image resolutions one by one and found that the image resolution was 2048x2048.


Boss.png* (C:\Users\green\OneDrive\Desktop\) - TweakPNG
File Edit Insert Options Tools Help
Boss.png - TweakPNG Image ...
File Edit Options Zoom
C0rupted Dimension
Panik
YOU FIXED IT
Kalm
Swapped chunks
Panik

Chunk	Length	CRC	Attributes	Contents
IHDR	13	4ac274f1	critical	PNG image header: 2048×2048, 8 bits/sample, truec
IDAT	1627736	3319fdab	critical	PNG image data
iTXt	834	2d8219...	ancillary, safe to copy	text (international), key="XML:com.adobe.xmp" (nc
tEXt	25	71c9653c	ancillary, safe to copy	text, key="Software": "Adobe ImageReady"
IEND	0	ae426082	critical	end-of-image marker

PNG file size: 1628676 bytes