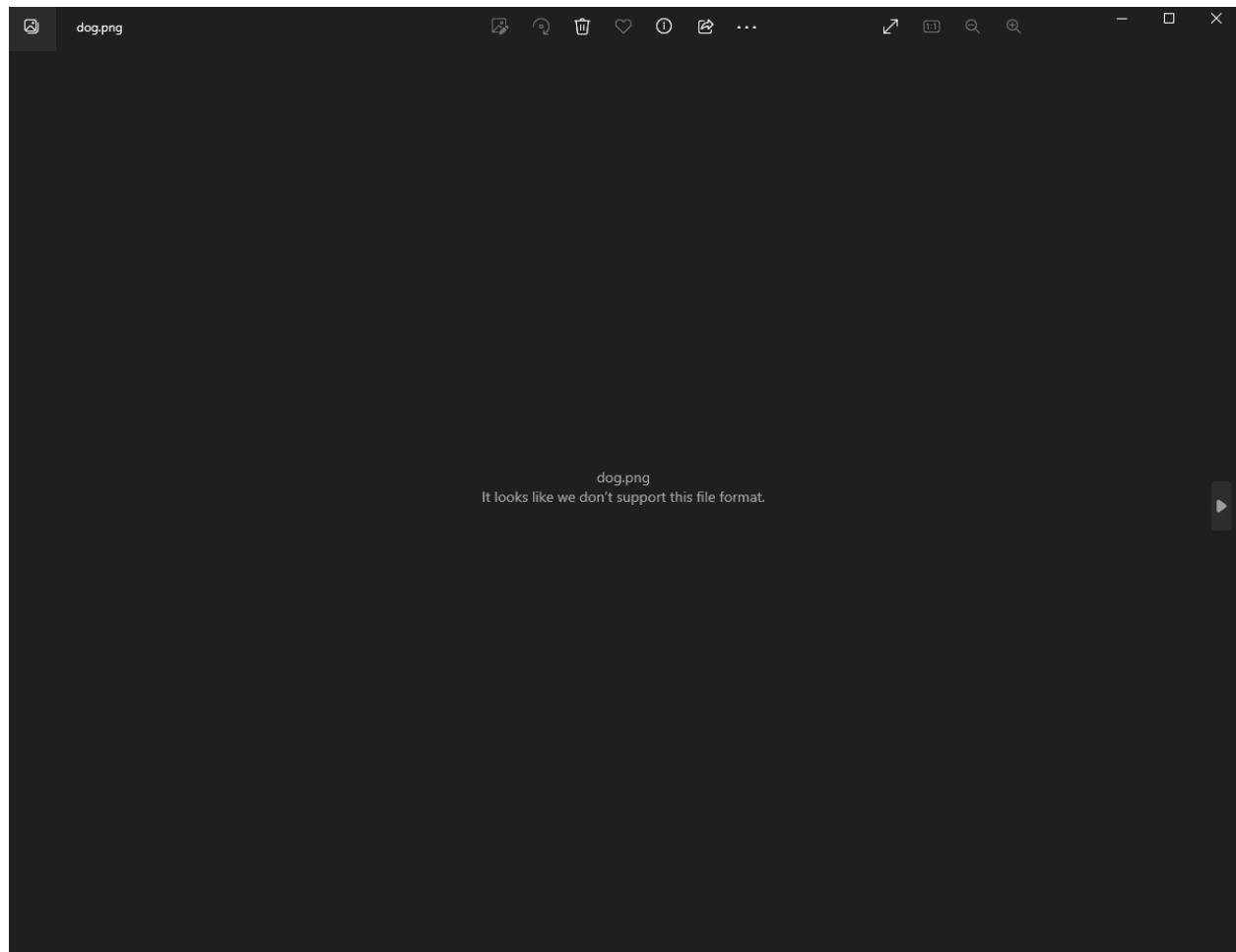


Umer Farooq   i220518   CY-A

Answer 1:

Upon trying to open dog.png the following error occurs




Checking the magic bytes of this png don't match the headers of png format.

-Untitled- x	Boss.png x	challenge.png x	Image.jpg x	dog.png x	
00000000	50 4B 03 04 0A 00 00 00	00 00 57 4C 13 59 00 00	PK.....WL.Y..		
00000010	00 00 00 00 00 00 00 00	00 00 0A 00 00 00 63 68	.....ch		
00000020	61 6C 6C 65 6E 67 65 2F	50 4B 03 04 14 00 00 00	allenge/PK.....		
00000030	08 00 E8 88 8B 57 C8 FB	65 EB 59 B6 18 00 04 DA	..ëêîWℓveδY ...r		
00000040	18 00 12 00 00 00 63 68	61 6C 6C 65 6E 67 65 2F	.....challenge/		
00000050	42 6F 73 73 2E 70 6E 67	7C FD 73 90 65 4D F0 2E	Boss.png ²sÊeM≡.		
00000060	0A EF B6 6D DB B6 6D DB	B6 6D BB A7 6D 7B DA 3D	.n m  m  m  °mf =		
00000070	ED EE 69 DB B6 6D DB EE	BE F3 9E 7B 7E F7 7E F1	φεï{ m ε}≤P{~≈±		
00000080	45 9C 5B B1 FE A8 55 2B	33 57 55 D6 93 19 4F EE	E£[    ·¿U+3WUπ.ôε		
00000090	A8 58 3B 52 51 5E 02 0E	1A 1B 1A 00 00 11 B6 52	¿X;RQ^..... R		
000000A0	D5 74 D5 94 93 E5 36 71	B0 A3 37 32 75 30 36 A3	fτ pōδσ6q\\ú72u06ú		
000000B0	F7 B4 73 04 FC D7 78 05	3C 1D 8D 4C 6C CC 5C 09	≈ s. n x.<.iLl f .		
000000C0	8D CD 2C AC EC F9 88 6F	3A 7A 88 09 AD 4C F9 88	i=,∫∞·êo:zê;jL·ê		
000000D0	35 D8 E4 18 E5 1C 45 CC	2C AD 24 BD 9D CD 54 BC	5τΣ.σ.E j,i\$∥Y=τΔ		
000000E0	E5 55 4D BC 6D 4C B8 4C	89 05 F8 09 79 3D B9 FF	σUM∥mLq LË.° .y=		

These magic bytes match the signature of zip files.

50 4B 03 04



 HIMG ADEA Corp. ChromaGraph Graphics Card Bitmap Graphic file

PK...

ZIP PKZIP archive file ([Ref 1](#) | [Ref 2](#))

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

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

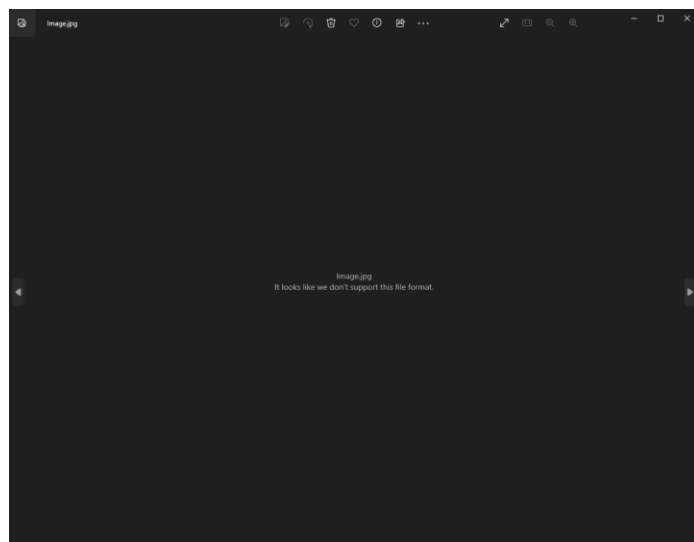
**Note:** PK are the initials of Phil Katz, co-creator of the ZIP file format and author of PKZIP.

ZIP Apple Mac OS X Dashboard Widget, Aston Shell theme, Oolite eXpansion Pack, Opera Widget, Pivot Style Template, Rockbox Theme package, Simple Machines Forums theme, SubEthaEdit Mode, Trillian zipped skin, Virtual Skipper skin

It is actually a .zip file.

Answer 2:

Image.jpg doesn't open at first.



Checking the hex bytes we see its jfif format but some magic bytes are not correct.

```
000000 EF 56 21 56 00 10 4A 46 49 46 00 01 01 00 00 01 nV!V..JFIF.....
000010 00 01 00 00 FF DB 00 84 00 09 06 07 08 07 06 09 .... ä.....
```

Correct bytes:

```
FF D8 FF E0 xx xx 4A 46      ÿøÿà..JF
49 46 00                      IF.
                                JFIF, JPE, JPEG, JPG JPEG/JFIF graphics file
                                Trailer: FF D9 (ÿù)
```

We can simply edit the hex and save the new file.



FLAG{stronk}.

Answer 3:

Original jpg file:

```
FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01 + α..JFIF.....
00 01 00 00 FF DB 00 84 00 09 06 07 08 07 06 09 .... ä.....
08 07 08 0A 0A 09 0B 0D 16 0F 0D 0C 0C 0D 1B 14 .....
15 1A 16 2A 1D 22 22 2A 1D 1E 1E 24 28 24 2C 24 "" 67A 6
```

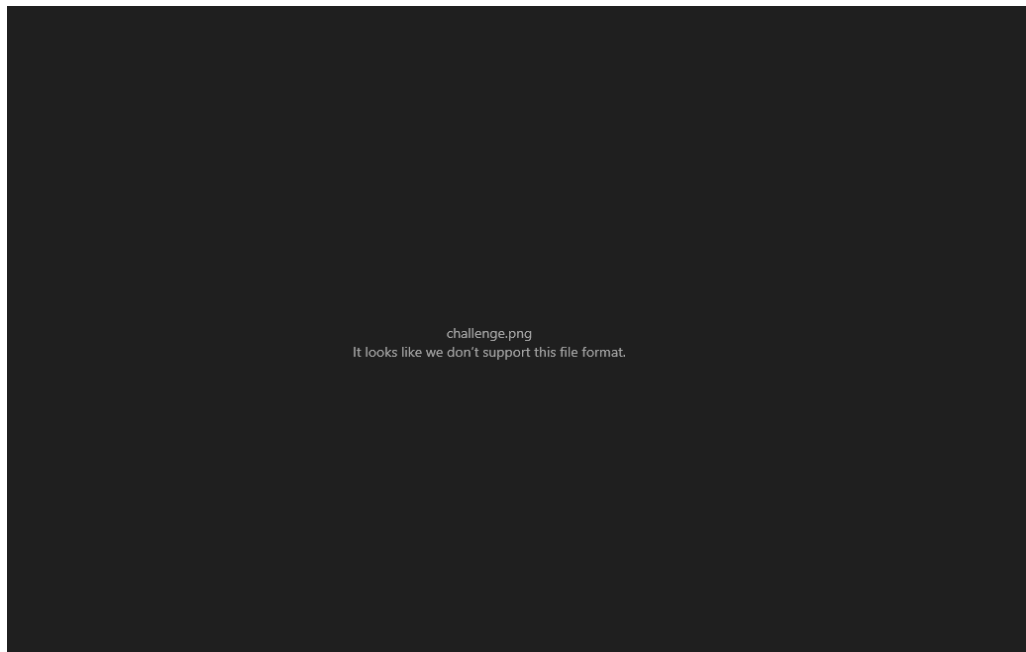
Modified to png format:

-Untitled- x	Boss.png x	challenge.png x	checking.jpg x	checking.png x			
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	1A	16	2A 1D 22 22 2A	1D 1F 1F 24 28 34 2C 24	...	"...\$(4 \$

The magic bytes do not change if extension is changed.

Answer 4:

Its doesn't open.



Checking hexvalues:

-Untitled- x	Boss.png x	challenge.png x		
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.«+..
00000030	00 04	07 41 4D 41 00 00	B1 0F 0B 5C 01 0F 00 00	-AMA 00 00

I see that the NG could be PNG and try to match with the png header:

all IPv6 packet. See [THIS ABOUT LOOKING FOR NETWORK PACKET IDS](#)

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`,...)

..

The first 2 bytes are changed so changing them leads to recover of the image.



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 {d1g1tal\_f0r3ns1cs\_101}.

Answer 5:

Trailer bytes at the end of the file.