Delionor 8/11/2022

L’image perdue de Dédé

Auteur : Delionor CTF FlagMalo 2022

Nous recevons pour ce défi une image png étrange, qui semble composé uniquement de pixels transparents (affichés en gris sur Linux).

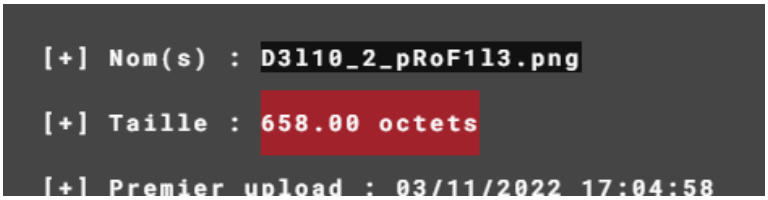
D’après l’énoncé, l’image contient des informations cachées que nous devons retrouver.

Pour commencer, je vous propose donc d’utiliser https://www.aperisolve.com/ , un site spécialisé dans la détection de données cachées dans les images.

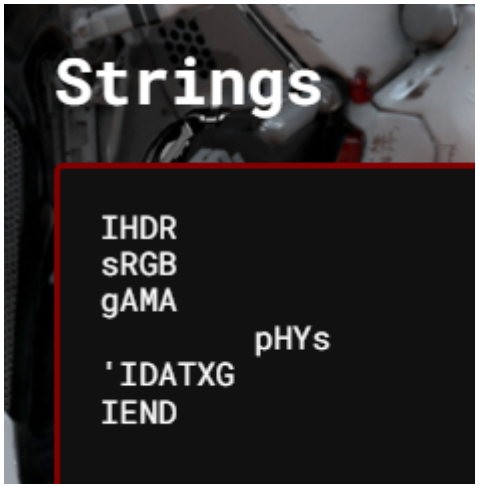
Après avoir uploadé notre png, le site effectue plusieurs tests. Il joue d’abord avec différent filtre pour essayer de faire ressortir une forme particulière (superposé, rouge, bleu, vert), puis va utiliser l’équivalent de commandes utiles en stéganographie (notons steghide, exiftool, binwalk, strings etc.)

Si vous avez déjà utilisé ces outils, vous vous rendrez vite compte que l’image semble particulièrement vide :

- Une taille de seulement 658 octets :

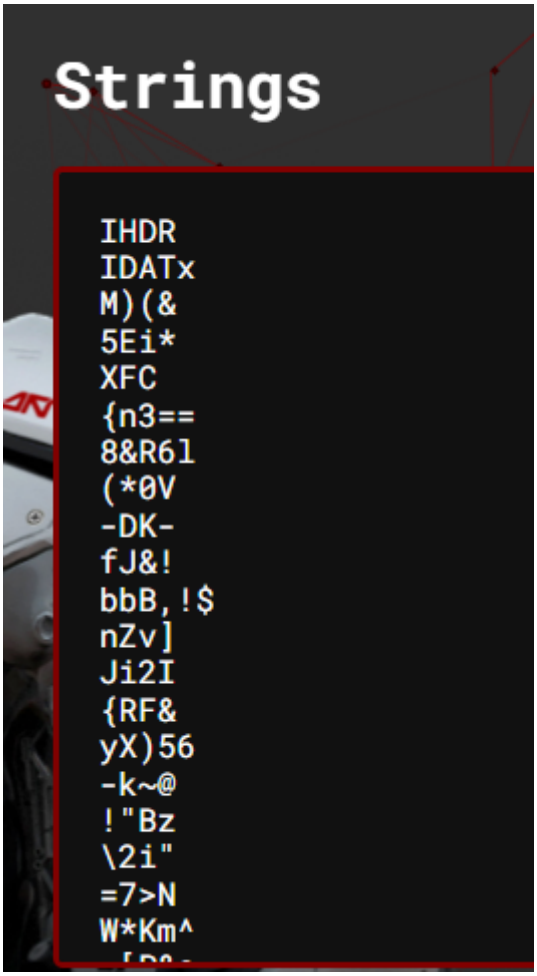


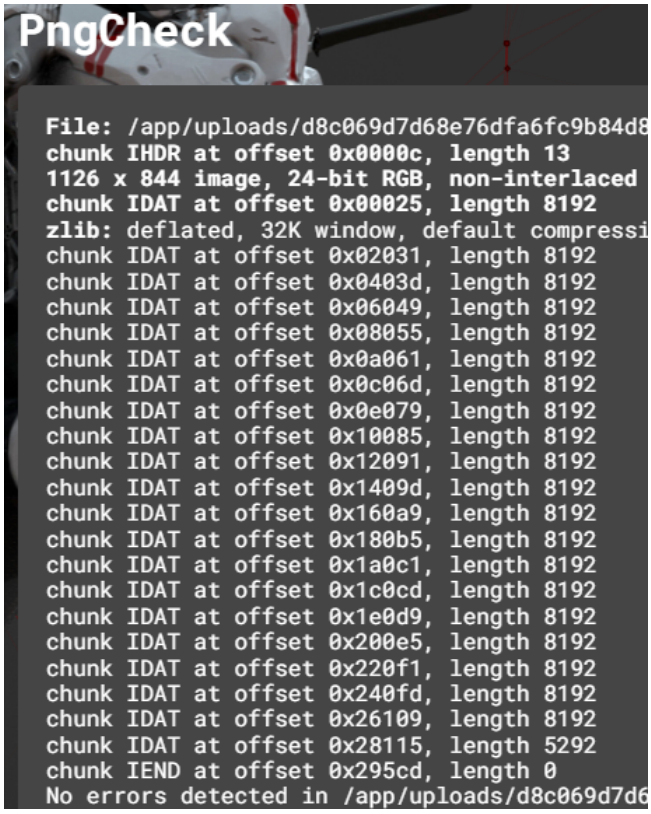
- Aucun strings présents à part les chunks PNG :



- Un seul chunk IDAT (qui grossièrement contient l’image affichée) d’une faible longueur :

En comparaison, voilà ce que nous pourrions trouver sur une image « normale » :





Il est clair que cette image ne contient quasiment rien (peut être rien du tout?). Essayons de l’ouvrir avec un éditeur hexadécimal pour voir ce qu’elle contient… Peut être que le flag est écrit en dur sur une ligne d’hexa ?

Utilisons HxD ou tout autre éditeur hexa et ouvrons ce png :

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Texte Décodé
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	‰PNG........IHDR
00000010	00	00	00	21	00	00	00	1E	08	06	00	00	00	A2	C8	77	...!.........¢Èw
00000020	17	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	.....sRGB.®Î.é..
00000030	00	04	67	41	4D	41	00	00	B1	8F	0B	FC	61	05	00	00	..gAMA..±..üa...
00000040	00	09	70	48	59	73	00	00	12	74	00	00	12	74	01	DE	..pHYs...t...t.Þ
00000050	66	1F	78	00	00	02	27	49	44	41	54	58	47	9D	97	61	f.x...'IDATXG.—a
00000060	72	DA	00	60	00	00	00	00	00	00	00	00	00	03	C0	00	rÚ.`..........À.
00000070	00	00	00	03	C0	00	00	00	00	0F	F0	00	00	00	00	0F	....À.....ð.....
00000080	F0	00	00	00	0F	F0	0F	F8	00	00	0F	F0	0F	F8	00	00	ð....ð.ø...ð.ø..
00000090	3C	00	00	1E	00	00	3C	00	00	1E	00	00	00	00	00	00	<.....<.........
000000A0	00	00	00	00	00	00	00	00	3F	FF	FF	FE	00	00	3F	FF	........?ÿÿþ..?ÿ
000000B0	FF	FE	00	00	3F	FF	FF	FE	00	00	3F	FF	FF	FE	00	00	ÿþ..?ÿÿþ..?ÿÿþ..
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	3F	00	00	00	............?...
000000D0	00	00	3F	00	00	00	00	00	3F	00	00	00	00	00	3F	00	..?.....?.....?.
000000E0	00	00	00	00	3F	00	00	00	00	00	3F	00	00	00	00	00	....?.....?.....
000000F0	3F	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	?...............
00000100	00	00	3F	FF	FF	FE	00	00	3F	FF	FF	FE	00	00	3F	FF	..?ÿÿþ..?ÿÿþ..?ÿ
00000110	FF	FE	00	00	3F	FF	FF	FE	00	00	3F	00	00	00	00	00	ÿþ..?ÿÿþ..?.....
00000120	3F	00	00	00	00	00	3F	00	00	00	00	00	3F	00	00	00	?.....?.....?...
00000130	00	00	3F	00	00	00	00	00	3F	00	00	00	00	00	00	00	..?.....?.......
00000140	00	00	00	00	00	00	00	00	00	00	0C	30	00	00	00	00	...........0....
00000150	0C	30	00	00	00	00	30	0C	00	00	00	00	30	0C	00	00	.0....0.....0...
00000160	00	00	0C	30	00	00	00	00	0C	30	00	00	00	00	03	C0	...0.....0.....À
00000170	00	00	00	00	00	00	00	FC	00	00	00	00	00	FC	00	00	.......ü.....ü..
00000180	00	00	3F	00	00	00	00	00	3F	00	00	00	00	FF	C0	00	..?.....?....ÿÀ.
00000190	00	00	00	FF	C0	00	00	00	0F	00	00	00	00	00	0F	00	...ÿÀ...........
000001A0	00	00	00	00	00	FF	C0	00	00	00	00	FF	C0	00	00	00	.....ÿÀ....ÿÀ...
000001B0	00	00	3F	00	00	00	00	00	3F	00	00	00	00	00	00	FC	..?.....?......ü
000001C0	00	00	00	00	00	FC	00	00	3F	00	00	00	00	00	3F	00	.....ü..?.....?.
000001D0	00	00	00	00	3F	00	00	00	00	00	3F	00	00	00	00	00	....?.....?.....
000001E0	3F	00	00	00	00	00	3F	00	00	00	00	00	3F	00	00	00	?.....?.....?...
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	3F	FF	..............?ÿ
00000200	FF	FE	00	00	3F	FF	FF	FE	00	00	3F	FF	FF	FE	00	00	ÿþ..?ÿÿþ..?ÿÿþ..
00000210	3F	FF	FF	FE	00	00	00	00	00	00	00	00	00	00	00	00	?ÿÿþ............
00000220	00	00	3F	FF	FF	E0	00	00	3F	FF	FF	FE	00	00	3C	00	..?ÿÿà..?ÿÿþ..<.
00000230	F0	00	00	00	3C	00	F0	00	00	00	3C	00	00	00	00	00	ð...<.ð...<.....
00000240	00	00	00	00	00	00	00	00	00	00	00	00	3C	00	00	1E	............<...
00000250	00	00	3C	00	00	1E	00	00	0F	F0	0F	F8	00	00	0F	F0	..<.......ð.ø...ð
00000260	0F	F8	00	00	00	0F	F0	00	00	00	00	0F	F0	00	00	00	.ø....ð.....ð...
00000270	00	03	C0	00	00	00	00	03	C0	00	00	00	00	00	00	00	..À.....À.......
00000280	00	00	07	56	17	8E	00	00	00	00	49	45	4E	44	AE	42	...V.Ž....IEND®B
00000290	60	82															`‚

On retrouve bien nos chunks PNG (IHDR, sRGB, gAMA, pHYs, IDAT, IEND). Vous pouvez tous les consultez sur http://www.libpng.org/pub/png/spec/1.2/PNG-Chunks.html

Avant de s'intéresser aux techniques habituelles (IHDR modifié, Chunk corrompu cf https://elsicarius.fr/les-images-png-comment-ca-marche-comment-corriger-manuellement-les-erreurs), nous pouvons remarquer que le chunk IDAT est plutôt particulier. Il n'est composé que de 00, FF, 3F etc.

Et le 00 est particulièrement redondant.

Nous pouvons essayer plusieurs manières de résoudre ceci : ne convertir que les symboles différents de 0, faire un joli mandala ou découvrir un code révolutionnaire à base de ‘.’, de ‘?’ et de ‘ÿ’

Vous vous doutez bien qu’aucune de ces solutions n’est la bonne. En y réfléchissant un peu, s’il y a autant de 00, cela veut dire qu’il y aura des grandes suites de ‘0000000000000000’ si nous convertissons l’hexa en binaire. Idem d’ailleurs pour ‘FF’ qui donnerait ‘1111111111111111’. Admettons que c’est plutôt rare de trouver de telles suites dans nos fichier…

Je vous propose donc d’analyser ce fichier à nouveau, mais cette fois-ci avec une vue binaire et non en hexa.

Utilisons xxd -b sous linux :

```
└─$ xxd -b D3l10_2_pRoF1l3.png
00000000: 10001001 01010000 01001110 01000111 00001101 00001010  .PNG..
00000006: 00011010 00001010 00000000 00000000 00000000 00001101  ......
0000000c: 01001001 01001000 01000100 01010010 00000000 00000000  IHDR..
00000012: 00000000 00100001 00000000 00000000 00000000 00011110  .!....
00000018: 00001000 00000110 00000000 00000000 00000000 10100010  ......
0000001e: 11001000 01110111 00010111 00000000 00000000 00000000  .w....
00000024: 00000001 01110011 01010010 01000111 01000010 00000000  .sRGB.
0000002a: 10101110 11001110 00011100 11101001 00000000 00000000  ......
00000030: 00000000 00000100 01100111 01000001 01001101 01000001  ..gAMA
00000036: 00000000 00000000 10110001 10001111 00001011 11111100  ......
0000003c: 01100001 00000101 00000000 00000000 00000000 00001001  a.....
00000042: 01110000 01001000 01011001 01110011 00000000 00000000  pHYs..
00000048: 00010010 01110100 00000000 00000000 00010010 01110100  .t...t
0000004e: 00000001 11011110 01100110 00011111 01111000 00000000  ..f.x.
00000054: 00000000 00000010 00100111 01001001 01000100 01000001  ..'IDA
0000005a: 01010100 01011000 01000111 10011101 10010111 01100001  TXG..a
00000060: 01110010 11011010 00000000 01100000 00000000 00000000  r..`..
00000066: 00000000 00000000 00000000 00000000 00000000 00000000  ......
0000006c: 00000000 00000011 11000000 00000000 00000000 00000000  ......
00000072: 00000000 00000011 11000000 00000000 00000000 00000000  ......
00000078: 00000000 00001111 11110000 00000000 00000000 00000000  ......
0000007e: 00000000 00001111 11110000 00000000 00000000 00000000  ......
00000084: 00001111 11110000 00001111 11111000 00000000 00000000  ......
0000008a: 00001111 11110000 00001111 11111000 00000000 00000000  ......
00000090: 00111100 00000000 00000000 00011110 00000000 00000000  <.....
00000096: 00111100 00000000 00000000 00011110 00000000 00000000  <.....
0000009c: 00000000 00000000 00000000 00000000 00000000 00000000  ......
000000a2: 00000000 00000000 00000000 00000000 00000000 00000000  ......
000000a8: 00111111 11111111 11111111 11111110 00000000 00000000  ?.....
000000ae: 00111111 11111111 11111111 11111110 00000000 00000000  ?.....
000000b4: 00111111 11111111 11111111 11111110 00000000 00000000  ?.....
000000ba: 00111111 11111111 11111111 11111110 00000000 00000000  ?.....
000000c0: 00000000 00000000 00000000 00000000 00000000 00000000  ......
000000c6: 00000000 00000000 00000000 00000000 00000000 00000000  ......
000000cc: 00111111 00000000 00000000 00000000 00000000 00000000  ?.....
000000d2: 00111111 00000000 00000000 00000000 00000000 00000000  ?.....
000000d8: 00111111 00000000 00000000 00000000 00000000 00000000  ?.....
000000de: 00111111 00000000 00000000 00000000 00000000 00000000  ?.....
000000e4: 00111111 00000000 00000000 00000000 00000000 00000000  ?.....
000000ea: 00111111 00000000 00000000 00000000 00000000 00000000  ?.....
000000f0: 00111111 00000000 00000000 00000000 00000000 00000000  ?.....
000000f6: 00000000 00000000 00000000 00000000 00000000 00000000  ......
000000fc: 00000000 00000000 00000000 00000000 00000000 00000000  ......
00000102: 00111111 11111111 11111111 11111110 00000000 00000000  ?.....
00000108: 00111111 11111111 11111111 11111110 00000000 00000000  ?.....
0000010e: 00111111 11111111 11111111 11111110 00000000 00000000  ?.....
00000114: 00111111 11111111 11111111 11111110 00000000 00000000  ?.....
0000011a: 00111111 00000000 00000000 00000000 00000000 00000000  ?.....
00000120: 00111111 00000000 00000000 00000000 00000000 00000000  ?.....
00000126: 00111111 00000000 00000000 00000000 00000000 00000000  ?.....
0000012c: 00111111 00000000 00000000 00000000 00000000 00000000  ?.....
00000132: 00111111 00000000 00000000 00000000 00000000 00000000  ?.....
00000138: 00111111 00000000 00000000 00000000 00000000 00000000  ?.....
0000013e: 00000000 00000000 00000000 00000000 00000000 00000000  ......
```

Ceci ressemble au début d’un flag non ? :D

Je vous épargne le screen entier, mais voici notre flag !

FMCTF{I_LoV_It}