

main ctf-writeup / 2023-ARA / Forensic-Thinker /



fhinnn feat:Thinker ...

6 minutes ago History

..



assets

6 minutes ago



README.md

6 minutes ago

README.md



## Forensic - Thinker

Kita diberikan gambar berformat PNG. lalu saya cek di meta data nya dengan membukanya melalui notepad dan menemukan beberapa keanehan.

```

Pz:®MÒYD;æµx@,±3Ê?^xß:ûÔçî%ëOëëânDÐD"Ûµ¥'n"Ä□□□□#“iZúuã@Z<-{D-o9MÊŽ®ë
×|ww
6x□□□',fý□p3□sb□FyüÖØ□'δükœzâÿÇ}û□ÖDUâ;□}ª)□Ðt5
□×ªÛ%ý?PK□□□□
4^GV
□ □ iA suspicious/UT□ □$âcux
□□è□ □è□ PK□□□□ □ 'GVBS?ô# { ' □ □ □E suspicious/y.pngUT□ □~âcux
□□è□ □è□ PK□□ □ □ § f$ PK□□□□
Ž^GV
□ □ iA something/UT□ □İâcux
□□è□ □è□ PK□□□□ □ 'HFVÖüí}) Z □ □ □ □D something/s.txtUT□ □2 âcux
□□è□ □è□ PK□□□□
p^GVÓ††, @% @% □ □ □ □ something/suspicious.zipUT□ □“âcux
□□è□ □è□ PK□□ □ □ □ □ H& PK□□□□
ê^GV □ □ □ iA find/UT□ □w,âcux
□□è□ □è□ PK□□□□
HFV/Cðw□ □
□ □ □? find/a.txtUT□ □à âcux
□□è□ □è□ PK□□□□
²^GV»ü×,a' a' □ □ □ □ find/something.zipUT□ □□,âcux
□□è□ □è□ PK□□ □ □ □ ?( PK□□□□
_GV □ □ □ iA didyou/UT□ □²,âcux
□□è□ □è□ PK□□□□
=GFV• V~

□ □ □A didyou/e.txtUT□ □f âcux
□□è□ □è□ PK□□□□
÷^GV□D,H) H) □ □ □ □ didyou/find.zipUT□ □',âcux
□□è□ □è□ PK□□ □ □ ô %*
```

ditemukan ada beberapa file didalam. jadi untuk lebih ditailnya saya cek menggunakan `binwalk` untuk melihat isi dari PNG tersebut.

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 720 x 881, 8-bit/color RGB, non-interlaced
6170	0x181A	Zlib compressed data, best compression
321663	0x4E87F	TIFF image data, big-endian, offset of first image directory: 8
321693	0x4E89D	Zip archive data, at least v1.0 to extract, name: didyou/
321758	0x4E8DE	Zip archive data, at least v1.0 to extract, compressed size: 13, uncompressed size: 13, name: didyou/e.txt
321841	0x4E931	Zip archive data, at least v1.0 to extract, compressed size: 10568, uncompressed size: 10568, name: didyou/find.zip
332460	0x512AC	End of Zip archive, footer length: 22
332726	0x513B6	End of Zip archive, footer length: 22

ternyata benar dan ditemukan beberapa file ada dialam PNG tersebut dan di kompres dengan ZIP, lalu selanjutnya saya lakukan extract agar bisa mengakses hidden file tersebut. Hasil dari extract dari file PNG tersebut sebagai berikut.





didyou	07/02/2023 23:56	File folder	
4E89D.zip	26/02/2023 20:13	Compressed (zipped)...	11 KB
181A	26/02/2023 20:13	File	0 KB
181A.zlib	26/02/2023 20:13	ZLIB File	319 KB

didalam direktori `didyou` ditemukan 2 file yaitu `e.txt` dan `find.zip`



e.txt	06/02/2023 20:57	Text Document	1 KB
find.zip	07/02/2023 23:55	Compressed (zipped)...	11 KB

didalam `e.txt` ditemukan kode yang sepertinya kode `base 64` dan coba saya translate. dan benar ternyata itu adalah potongan flag nya.

QVJBMjAyM3s=

Output			time: 59ms length: 17471 lines: 652				
Recipe (click to load)	Result snippet	Properties					
<code>From_Quoted_Printable()</code>	QVJBMjAyM3s	Valid UTF8 Entropy: 3.28					
<code>From_Base64('A-Za-z0-9+/',true,false)</code>	ARA2023{	Valid UTF8 Entropy: 2.50					
	QVJBMjAyM3s=.	Matching ops: From Base64, From Quoted					

lalu selanjutnya saya coba membuka file `find.zip` nya dan ditemukan file `a.txt` dan `something.zip`.






 a.txt	Text Document	1 KB	No
 something.zip	Compressed (zipped) Folder	10 KB	No

didalam `a.txt` ditemukan kode juga dan saya mencoba translate. Dan ternyata itu adalah potongan flag yang menggunakan kode hex.

35216D706C335F



Output

time: 31ms  
length: 11629  
lines: 436



Recipe (click to load)	Result snippet	Properties
<code>From_Hex('None')</code>	5!mpl3_	Valid UTF8 Entropy: 2.81
	35216D706C335F	Matching ops: From Hex, From Hexdump Valid UTF8 Entropy: 3.18

lalu selanjutnya saya mencoba buka file `something.zip` dan menemukan `s.txt` dan `suspicious.zip`.






 s.txt	Text Document	1 KB
 suspicious.zip	Compressed (zipped) Folder	10 KB

didalam `s.txt` ditemukan kode biner dan saya translate ternyata itu potongan dari flag juga.

01000011 00110000 01110010 01110010 01110101 01110000 01110100 00110011 01100100  
01011111

Output

time: 2ms  
length: 10  
lines: 1



C0rrupt3d\_

lalu selanjutnya saya buka file `suspicious.zip` nya dan menemukan PNG. namun PNG tersebut tidak dapat dibuka, lalu coba saya lihat menggunakan hex editor dan membandingkannya dengan PNG yang normal ada sebuah keanehan yaitu header file nya berbeda.

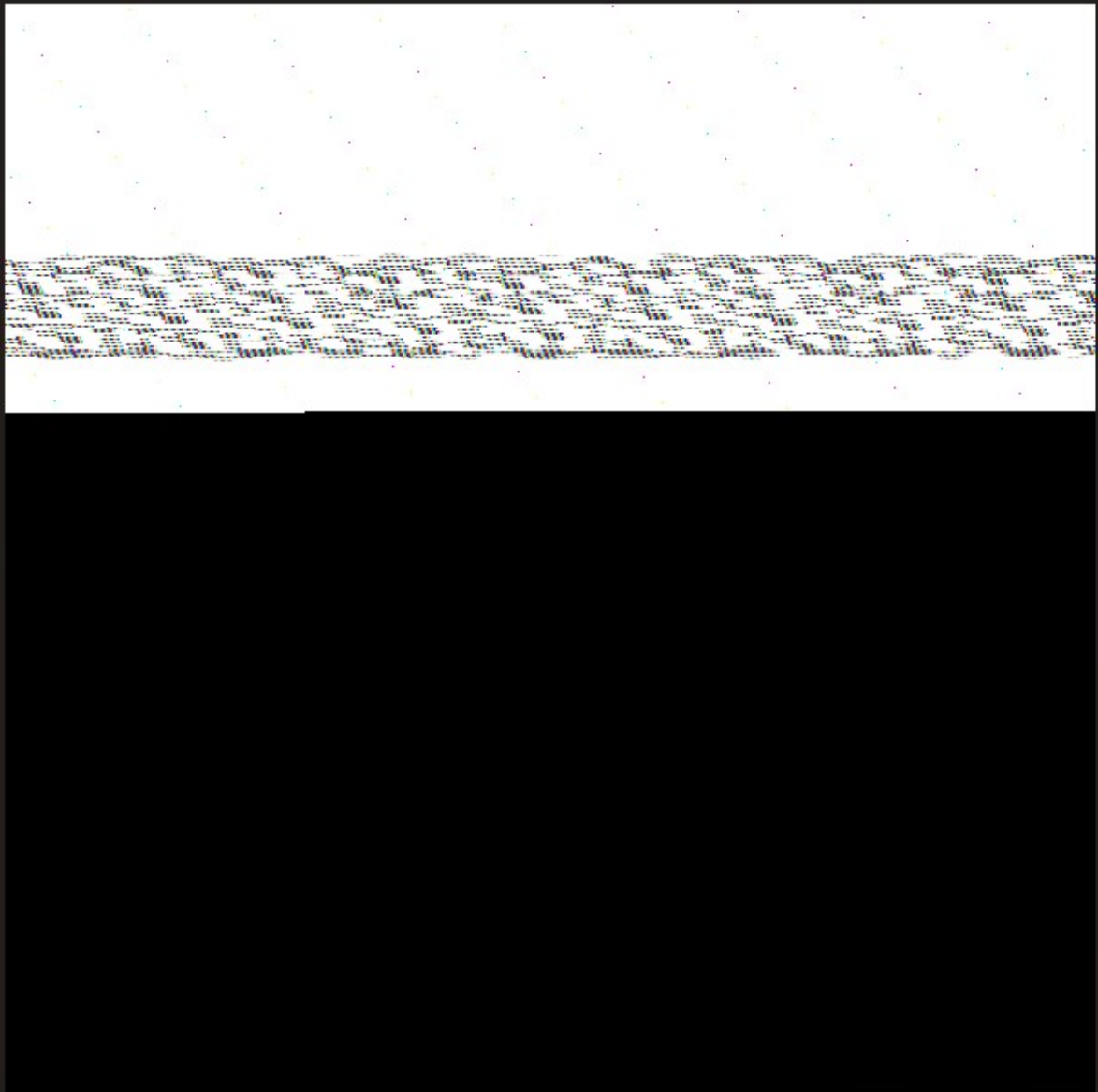
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG.....IHDR
0010h:	00	00	1F	40	00	00	11	94	08	02	00	00	00	50	03	1F	...@...".....P..
0020h:	C7	00	00	00	09	70	48	59	73	00	00	2E	23	00	00	2E	Ç....pHYs...#...
0030h:	23	01	78	A5	3F	76	00	00	20	00	49	44	41	54	78	9C	#.xÿ?v...IDATxœ
0040h:	EC	DC	41	01	C0	20	10	C0	B0	63	FE	7D	20	08	03	48	iÛA.À.À°cb}..H
0050h:	D9	83	CA	48	24	54	40	D7	3D	7B	00	00	00	00	00	00	ÛfÊH\$T@×={.....
0060h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0070h:	00	98	F9	34	00	00	00	00	00	00	00	00	00	00	00	00	.~ù4.....
0080h:	00	00	00	00	00	00	00	00	00	00	00	78	0C	DC	01	00	.....x.Û..
0090h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00A0h:	00	00	00	00	00	62	E0	0E	00	00	00	00	00	00	00	00	.....bà.....
00B0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	10	03	.....
00C0h:	77	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	w.....
00D0h:	00	00	00	00	00	00	00	80	18	B8	03	00	00	00	00	00	€

y.png

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	21	5A	78	52	0D	0A	1A	0A	00	00	00	0D	52	52	48	5C	!ZxR.....RRH\
0010h:	00	00	02	BD	00	00	00	90	08	06	00	00	00	05	89	D3	...½.....%Ó
0020h:	19	00	00	20	00	49	44	41	54	78	9C	ED	DD	79	98	13	...IDATxœíÿ~.
0030h:	F5	FD	07	F0	3E	4F	90	0A	5E	D5	5A	B5	B5	F5	68	00	õý.ð>O..^ÕZµµõh.
0040h:	59	B9	14	41	51	A1	08	5A	C5	7A	50	0F	44	94	96	D6	Y¹.AQj.ZÅzP.D''-Ö
0050h:	E3	27	87	A0	78	5B	2B	8A	A8	80	22	88	DC	87	C8	0D	ã'† x[+Š''€"^Ü†È.
0060h:	72	5F	2A	2C	16	15	AA	68	B2	F7	09	BB	2C	2C	CB	1E	r_*,...ªh²÷.»,,È.
0070h:	EC	91	5D	F6	3E	93	F7	EF	8F	6D	30	9B	CD	CC	F7	3B	ì_]ö>"÷ì.m0>Íì÷;
0080h:	D9	99	64	32	BC	5F	CF	33	7F	C1	66	92	99	64	E6	3D	Ùṡd2¼_î3.Áf'ṡdæ=
0090h:	DF	E3	F3	FD	05	88	88	88	88	88	2C	EE	17	E1	7E	03	ßãóý.^^^^^,î.á~.
00A0h:	44	44	44	44	44	46	63	E8	25	22	22	22	22	CB	63	E8	DDDDDFcè%""""Ècè
00B0h:	25	22	22	22	22	CB	63	E8	25	22	22	22	22	CB	63	E8	%""""Ècè%""""Ècè
00C0h:	25	22	22	22	22	CB	63	E8	25	22	22	22	22	CB	63	E8	%""""Ècè%""""Ècè
00D0h:	25	22	22	22	22	CB	63	E8	25	22	22	22	22	CB	63	E8	%""""Ècè%""""Ècè

Tetapi IDAT nya ada dan IEND nya pun ada sepertinya hanya ada kesalahan di header nya aja jadi saya ganti headernya dengan punya header PNG lain agar gambar bisa dibuka. Ternyata berhasil tetapi gambar masih tidak memberikan clue.





Selanjutnya saya manipulasi untuk width nya karena sepertinya kurang lebar sehingga tak bisa terbaca. jadi saya tambah widhtnya. Tetapi ternyata masih buram dan sulit terbaca maka saya ganti colornya dari truecolor menjadi alphatruecolor



dari gambar tersebut didapatkan deretan angka desimal lalu saya translate. dan akhirnya mendapatkan potongan akhir dari flag nya.

49 109 52 103 101 53 125

## Output

time: 0ms  
length: 7  
lines: 1



```
1m4ge5}
```

Akhirnya kita telah dapatkan semua flagnya dan tinggal di gabung saja menjadi flag yang utuh

```
ARA2023{5!mp13_C0rrupt3d_1m4ge5}
```

[Give feedback](#)