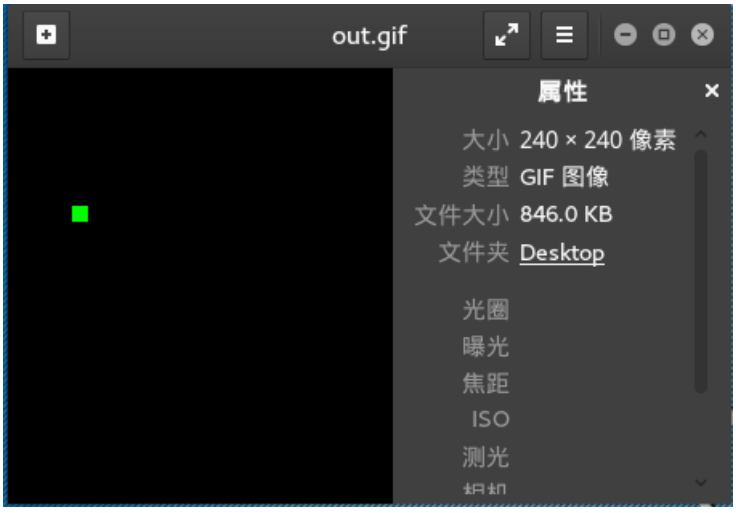
CTF-i春秋网鼎杯第四场部分writeup题目分析

原创

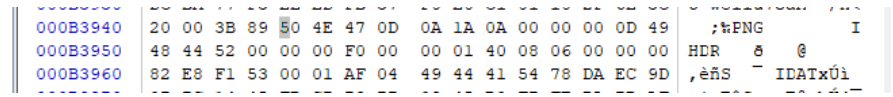
季海晨 于 2018-08-31 17:34:08 发布
分类专栏： CTF 信息安全 文章标签： 春秋网鼎杯

双色块

下载题目发现只有一个文件且为gif文件，可以正常打开，且只存在绿色和紫色两个颜色，分布不均匀。



先丢到winhexv看一下有没有插入其他文件，确实找到了png头文件。

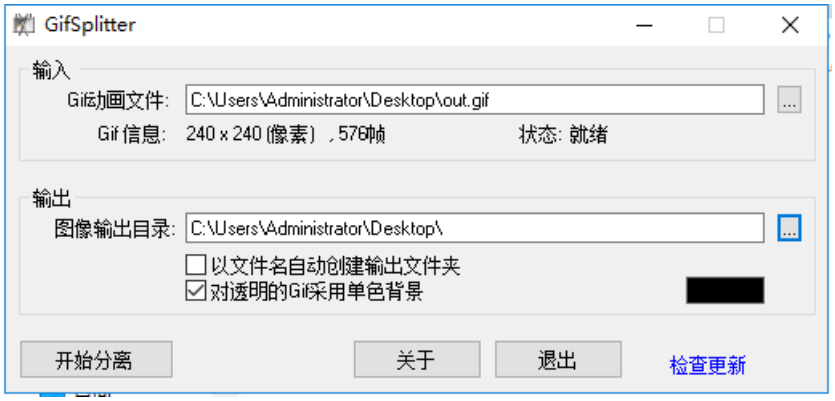


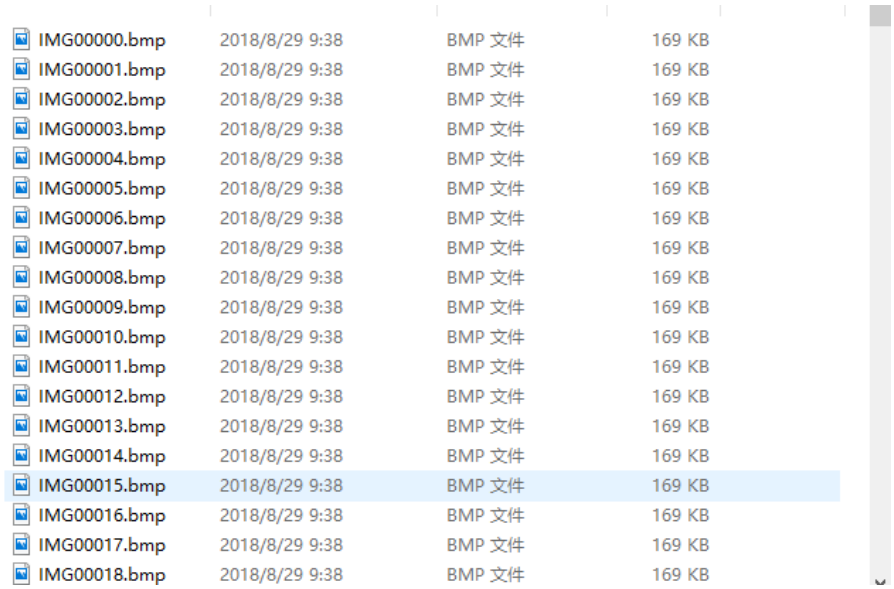
到binwalk分析一下，分离出图片

```
root@kali:~/Desktop# binwalk out.gif

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             GIF image data, version "89a", 240 x 240
735555        0xB3943         PNG image, 240 x 320, 8-bit/color RGBA, non-interl
aced
735596        0xB396C         Zlib compressed data, best compression

root@kali:~/Desktop# dd if=out.gif of=1.png skip=735555 bs=1
记录了110397+0 的读入
记录了110397+0 的写出
110397字节(110 kB)已复制，0.259133 秒，426 kB/秒
root@kali:~/Desktop#
```

上面写着key，可能下面用得到，继续分析这张图片无异常

接着分离一下gif，分离出576张图片，是24²





这两个变量应该是代表0，1了

按照紫色1，绿色0的规则排列出了以下数据：

01101111001110000100010001101100011110000100101100101011010010000011100001110111011001

按照紫色0，绿色1的规则排列出以下数据：

10010000110001111011101110010011100001111011010011010100101101111100011110001000100011

与ASCII码表(表见下)比对发现紫色1，绿色0的数据可翻译为编码格式：

o8DlxK+H8wsiXe/ERFpAMaBPilcj1sHyGOMmQDkK+uXsVZgre5DSXw==hhhhhhhhhhhhhhhh

ASCII可显示字符

二进制	十进制	十六进制	图形
0010 0000	32	20	（空格）(␣)
0010 0001	33	21	!
0010 0010	34	22	"
0010 0011	35	23	#
0010 0100	36	24	$
0010 0101	37	25	%

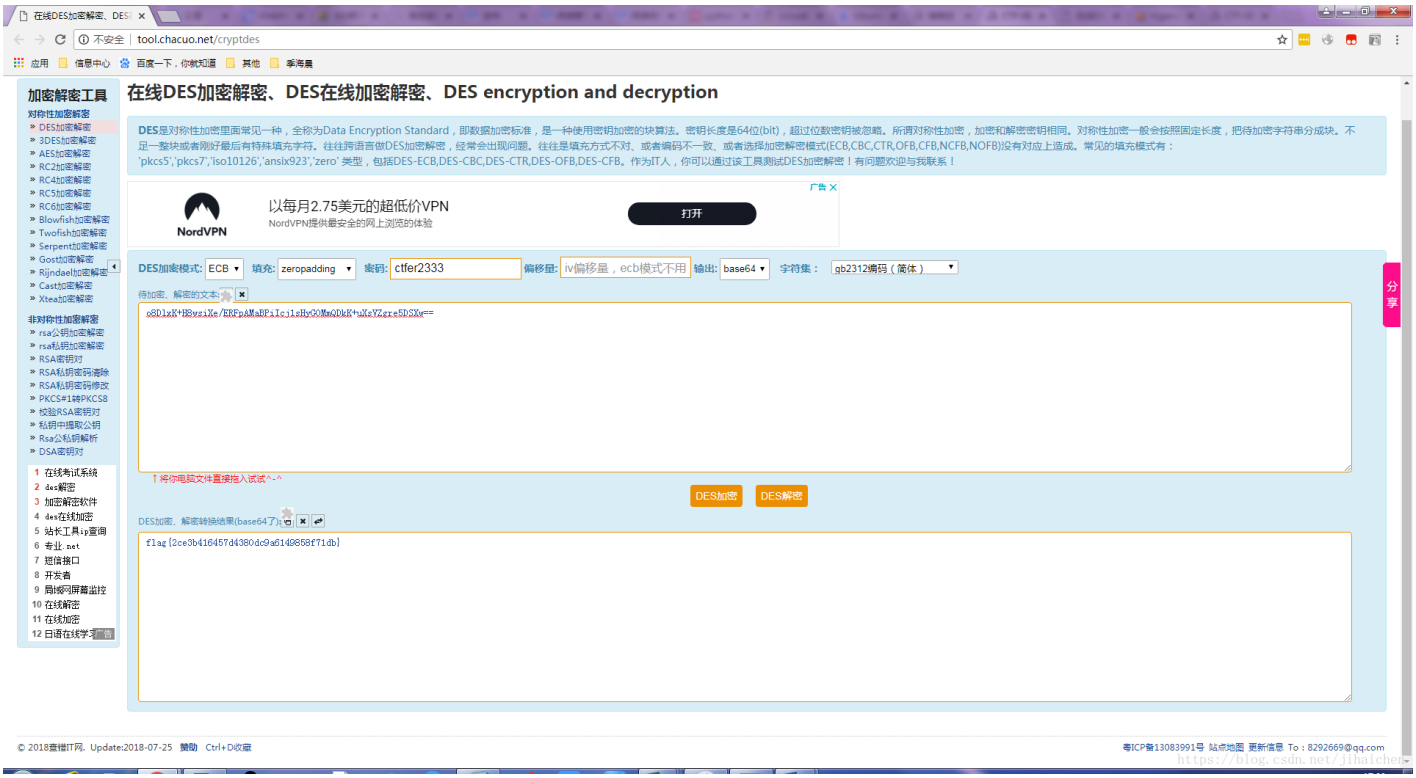
0010 0110	38	26	&
0010 0111	39	27	'
0010 1000	40	28	(
0010 1001	41	29	)
0010 1010	42	2A	*
0010 1011	43	2B	+
0010 1100	44	2C	,
0010 1101	45	2D	-
0010 1110	46	2E	.
0010 1111	47	2F	/
0011 0000	48	30	0
0011 0001	49	31	1
0011 0010	50	32	2
0011 0011	51	33	3
0011 0100	52	34	4
0011 0101	53	35	5
0011 0110	54	36	6
0011 0111	55	37	7
0011 1000	56	38	8
0011 1001	57	39	9
0011 1010	58	3A	:
0011 1011	59	3B	;
0011 1100	60	3C	<
0011 1101	61	3D	=
0011 1110	62	3E	>
0011 1111	63	3F	?
0100 0000	64	40	@
0100 0001	65	41	A
0100 0010	66	42	B
0100 0011	67	43	C

0100 0100	68	44	D
0100 0101	69	45	E
0100 0110	70	46	F
0100 0111	71	47	G
0100 1000	72	48	H
0100 1001	73	49	I
0100 1010	74	4A	J
0100 1011	75	4B	K
0100 1100	76	4C	L
0100 1101	77	4D	M
0100 1110	78	4E	N
0100 1111	79	4F	O
0101 0000	80	50	P
0101 0001	81	51	Q
0101 0010	82	52	R
0101 0011	83	53	S
0101 0100	84	54	T
0101 0101	85	55	U
0101 0110	86	56	V
0101 0111	87	57	W
0101 1000	88	58	X
0101 1001	89	59	Y
0101 1010	90	5A	Z
0101 1011	91	5B	[
0101 1100	92	5C	\
0101 1101	93	5D	]
0101 1110	94	5E	^
0101 1111	95	5F	_
0110 0000	96	60	`
0110 0001	97	61	a

0110 0010	98	62	b
0110 0011	99	63	c
0110 0100	100	64	d
0110 0101	101	65	e
0110 0110	102	66	f
0110 0111	103	67	g
0110 1000	104	68	h
0110 1001	105	69	i
0110 1010	106	6A	j
0110 1011	107	6B	k
0110 1100	108	6C	l
0110 1101	109	6D	m
0110 1110	110	6E	n
0110 1111	111	6F	o
0111 0000	112	70	p
0111 0001	113	71	q
0111 0010	114	72	r
0111 0011	115	73	s
0111 0100	116	74	t
0111 0101	117	75	u
0111 0110	118	76	v
0111 0111	119	77	w
0111 1000	120	78	x
0111 1001	121	79	y
0111 1010	122	7A	z
0111 1011	123	7B	{
0111 1100	124	7C	|
0111 1101	125	7D	}
0111 1110	126	7E	~

这应该是des加密或者base64，但是有提示key，所以应该是des加密，key是上面的图片内容，正常来说des结尾是=，这一堆h去掉就好了。

然后到http://tool.chacuo.net/cryptdes解密



得到flag为：flag{2ce3b416457d4380dc9a6149858f71db}