

实验吧/隐写术/so beautiful so white

原创

SIAT_啊哦 于 2016-07-17 21:48:46 发布 3531 收藏

分类专栏: [CTF](#) 文章标签: [密码](#) [隐写术](#) [头文件标志](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/ETF6996/article/details/51934848>

版权



[CTF 专栏收录该内容](#)

17 篇文章 0 订阅

[订阅专栏](#)

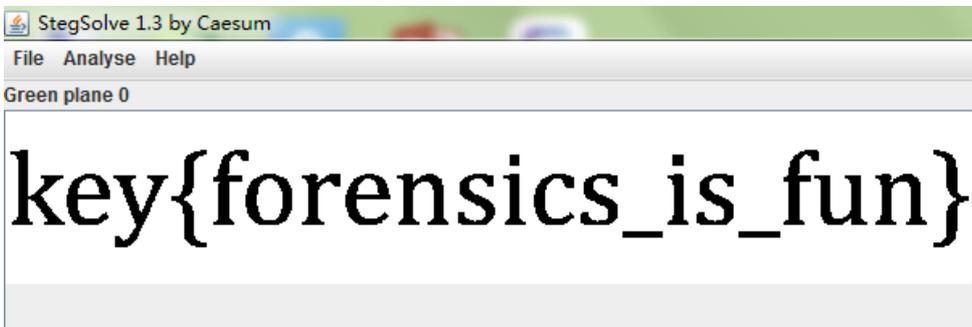
[题目链接](#)

下载得到一个zip文件, 解压后发现里面一个password.png是另一个zip文件的密码, 毫无疑问先把png文件binwalk一遍:

```
root@kali: ~/Desktop
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali: ~/Desktop# binwalk password.png
extracted
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          PNG image, 600 x 108, 8-bit/color RGB, non-interlaced
62          0x3E          Zlib compressed data, default compression, uncompressed size >= 194508
root@kali: ~/Desktop#
```

果然里面还有东东。

再用神器StegSolve把password.png过一遍:



得到另一个zip文件的密码。

解压后发现里面只有一个a.gif文件, 打开后什么都看不到, 自然而然想到另一个神器Winhex:

a.gif	Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
	00000000	B9	61	E3	00	14	01	F7	FF	00	F6	99	29	ED	E9	E7	F7	9aã ÷ÿ ö™) iéç÷
	00000010	DC	D5	F6	F6	F5	FB	C7	DB	F9	CC	6D	FD	EA	B0	FE	E9	üôäöðöüüü ïmúê°hé

```

00000020 F5 E8 B2 B1 94 8F 8E F5 EB E5 F2 4C 6A B2 88 73 8è±" ŽšššLj±^s
00000030 D8 B7 AA FC F3 ED D9 D8 D8 E5 CE C4 DA CB C5 FD 0·*úóìÛøøáíÄÜÉÁý
00000040 FB F6 DC C5 B9 ED E4 DD F7 DF 13 E5 C8 BC F3 30 úóÜÄ±iaÝ÷ß áÉ4ó0
00000050 57 F7 6C 91 F5 E5 DD F8 B1 4B C9 A5 99 ED DD D5 W÷l'ðáÝø±KÉÝ±iÝÖ
00000060 9C 5F 20 8D 75 6E F5 EE EB C7 9B 8C F5 D8 CC F7 æ_ unóieç>GóøI÷
00000070 F3 EE DB BD B4 73 6E 6D F5 B7 69 F8 CE 4E B7 A4 óiÜ±'snmø·ieİN·x

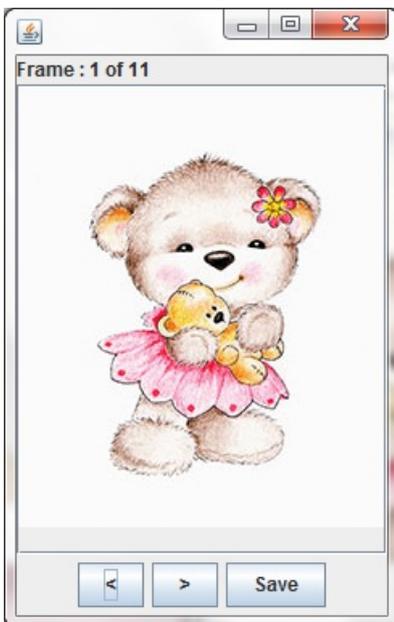
```

先分析头文件，这里是39 61开头，很明显不是gif头文件标志，但是39 61 刚好是gif头文件标志的后两个数，自然想到补齐前四个字节，即：47 49 46 38:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	47	49	46	38	39	61	E3	00	14	01	F7	FF	00	F6	99	29	GIF89aã ±ÿ çP)
00000010	ED	E9	E7	F7	DC	D5	F6	F6	F5	FB	C7	DB	F9	CC	6D	FD	íéç÷ÛÖøøóçÛùImý
00000020	EA	B0	FE	E9	F5	E8	B2	B1	94	8F	8E	F5	EB	E5	F2	4C	è°péðè±" ŽšššL
00000030	6A	B2	88	73	D8	B7	AA	FC	F3	ED	D9	D8	D8	E5	CE	C4	j±^sø·*úóìÛøøáíÄ
00000040	DA	CB	C5	FD	FB	F6	DC	C5	B9	ED	E4	DD	F7	DF	13	E5	ÜÉÁýúóÜÄ±iaÝ÷ß á

save后再打开a.gif，会看到一闪而过的动图。

最后用终极神器StegSolve一帧一帧地看，得到最终flag！啦啦啦~:



下面列出各类文件的头文件标志:

[here!!!](#)