

MOCTF-MISC-writeup

转载

[baochigu0818](#) 于 2019-07-31 02:14:00 发布 212 收藏

文章标签: [php](#) [网络](#) [python](#)

原文链接: <http://www.cnblogs.com/mortals-tx/p/11273745.html>

版权

小菜鸡终于想要开通博客, 要开始写东西了。第一次, 献给了MOCTF MISC writeup, 各种借鉴大哥们的writeup, 写的不好的话, 算了, 后果自负(嘤嘤嘤)。

MOCTF平台地址: www.moctf.com

MISC writeup

0x01.我可是黑客

题目链接: <http://119.23.73.3:6001/misc1/hacker.jpg>

得到的是这样一个图片, 直接放到winhex里面去看。



在最后面可以看到flag, get flag: moctf{e4sy_1ma9e_m1sc}, 可以很适合我这种小白。

0x02.假装安全

题目链接: <http://119.23.73.3:6001/misc9/carefully.jpg>

丢wenhex, 头部没什么问题, 往下看, 到最后的时候可以看到pk, flag.txt等有用信息,

说明里面隐藏的有文件, 而且加密了。直接改后缀名, 改为zip, 或者是用kali linux里面的binwalk/foremost分离里面的隐藏文件。

将zip文件再次丢到winhex里里面, 发现是一个伪加密, 直接改09为00即可解密。

```

4B 03 04 14 00 00 08 08 00 14 09 0F 4B 03 42 E0  A          i n Be
C6 18 00 00 00 16 00 00 00 08 00 00 00 66 6C 61  E          fla
67 2E 74 78 74 CB 4D 4E 这里改为40 CB A9 0C 36 4C  g.txtEMNs.JE@ 6L
CD 2F A9 76 48 2D 40 89 CF 49 A9 05 00 50 4B 01  í/çvH-í%II@ PK
02 3F 00 14 00 09 08 08 00 14 69 0F 4B 05 42 E8  ?          i K Bè
C6 18 00 00 00 16 00 00 00 08 00 24 00 00 00 00  E          $
00 00 00 20 00 00 00 00 00 00 00 66 6C 61 67 2E  flag.
74 78 74 0A 00 20 00 00 00 00 00 01 00 18 00 9F  txt          Ÿ
4A 58 8E 84 15 D3 01 DC E1 95 32 8E 0F D3 01 DC  JXž,, ó ůá•2ž ó ů
E1 95 32 8E 0F D3 01 50 4B 05 06 00 00 00 00 01  á•2ž ó PK
00 01 00 5A 00 00 00 3E 00 00 00 00 00          z >

```

解压之后可以得到一个flag.txt, 直接get flag: mcfCrflyS1eot{@eul_ld}

0x03.扫扫出奇迹

题目链接: <http://119.23.73.3:6001/misc4/qr.png>

hint: 扫二维码姿势要正确

得到一个二维码, 直接百度二维码在线识别, 可惜, 什么也扫不到。

刚开始不知道是取反色的二维码, 后来知道之后, 直接Stegsove上线

打开之后, 直接点下一个, 就会看下如下的xor图片, 这时候就可以随便扫了。



最后get flag: moctf{qr_code_1s_1n_1t}

0x04.光阴似箭

题目链接: <http://119.23.73.3:6001/misc2/flag.png>

hint: 眼睛一睁一闭, 我好像错过了啥?

你闪任你闪, 我有Stegsove(滑稽),

打开之后, 选择Analyse-Frame Browser,就可以看到每一帧了。

最后 get flag: moctf{F1ash_Movie}

0x05.杰斯的魔法

题目链接: http://119.23.73.3:6001/misc5/f1ag_print.txt

hint: 杰斯鼠标一挥, flag就跳出来了 $O(\cap\cap)O$

一个txt文本, 里面的字符编码, 第一个想到的是URL编码, 然后直接进行URL解码就可以发现flag了

```
cument.write(unescape('%3Cscript%20language%20%3D%20%22javascript%22%3Ealert%28%22moctf%7Bscr1pt_1s_magical%7D%22%29%3B%3C/script%3E'));
```

get flag: moctf{scr1pt_1s_magical}

0x06.流量分析

题目链接: <https://pan.baidu.com/s/1s-YU7ptXnlRmswuRcc7dlg> 提取码: y2s7

hint: 来吧尽情地分析我吧

流量分析, 直接丢Wireshark, 利用追踪流分析TCP流, 逐个看, 当eq=1的时候就会看到flag

Time	Source	Destination	Protocol
237	192.168.1.2	192.168.1.1	TELNET
238	192.168.1.1	192.168.1.2	TCP
239	192.168.1.2	192.168.1.1	TELNET
240	192.168.1.1	192.168.1.2	TCP
241	192.168.1.2	192.168.1.1	TELNET
242	192.168.1.1	192.168.1.2	TCP
243	192.168.1.2	192.168.1.1	TELNET
244	192.168.1.1	192.168.1.2	TCP
245	192.168.1.2	192.168.1.1	TELNET
246	192.168.1.1	192.168.1.2	TCP
247	192.168.1.2	192.168.1.1	TELNET

```
User Access Verification
Password: ..!..!.....P....
Password: co.....cisco
Password: cisco123
R1>eennaabbllee
Password: moctf{c@N_y0U_4lnd_m8}
R1#
```

get flag: moctf{c@N_y0U_4lnd_m8}

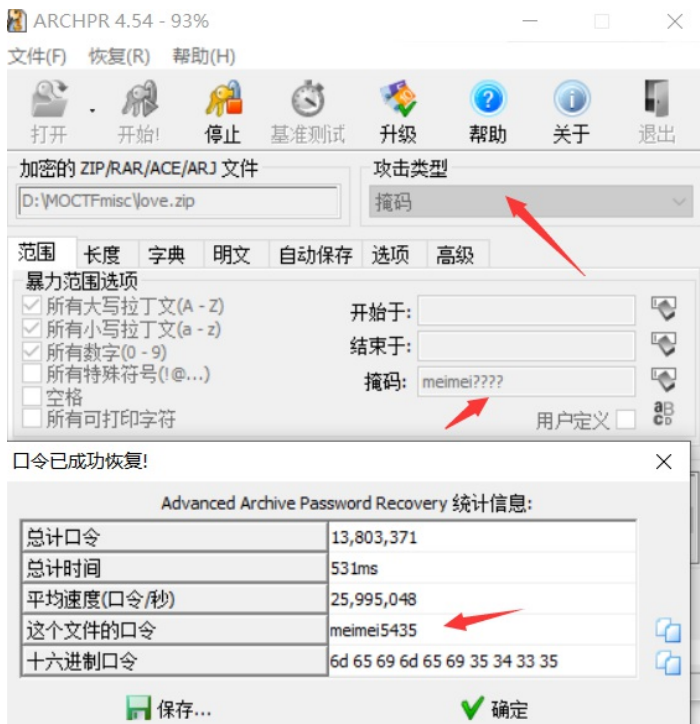
0x07.女生的告白

题目链接: <https://pan.baidu.com/s/1blBpTEcZ0hFgyEXTGUeQaw> 提取码: 40w4

hint: 李华的女神美美 (meimei)给李华发了一个压缩包, 却只告诉了李华压缩包密码是以她的名字开头, 你能帮李华获得真爱吗?

解压需要密码, 提示说压缩包密码是以meimei开头, 利用ARCHPR直接掩码攻击, 设置好掩码, 后面的位数可以一位一位的试。

将得到的密码解压文件, 获取flag。get flag: moctf{Y0u_@re_A_g00d_man}



0x08.捉迷藏

题目链接: <https://pan.baidu.com/s/1nghKOWj7QA8KEucEzIXm1g> 提取码: 9smz

hint: 草丛中突然钻出来一个光头

解压文件, 一张图片和一个flag.txt, 打开flag.txt, 一串字符, 直接base64解密, 可惜不对(大佬就是爱开玩笑)

那只能看图片了, 直接丢到winhex, 发现里面隐藏有一个flag.txt, 用binwalk/foremost分离出来, 或者直接改后缀为zip也行。

没有密码, 直接打开, 得到一串数字, ascii码转字符即可得到flag.

ascii在线解码: <https://www.mokuge.com/tool/asciito16/>, 不过好像就几个几个的解, 各位大佬可以直接写脚本跑也行。

get flag: moctf{h1d3_aNd_s33K}

0x09.是兄弟就来干我

题目链接: <https://pan.baidu.com/s/11PeWKvHp2HRZ-oTICujGkQ> 提取码: oib6

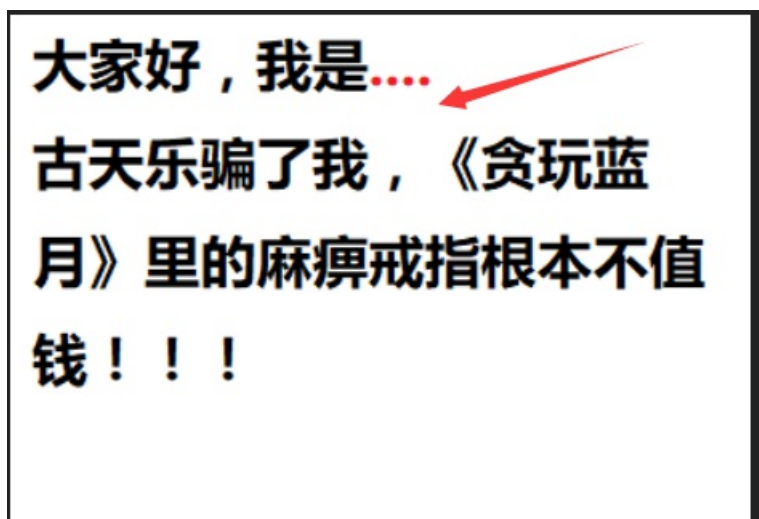
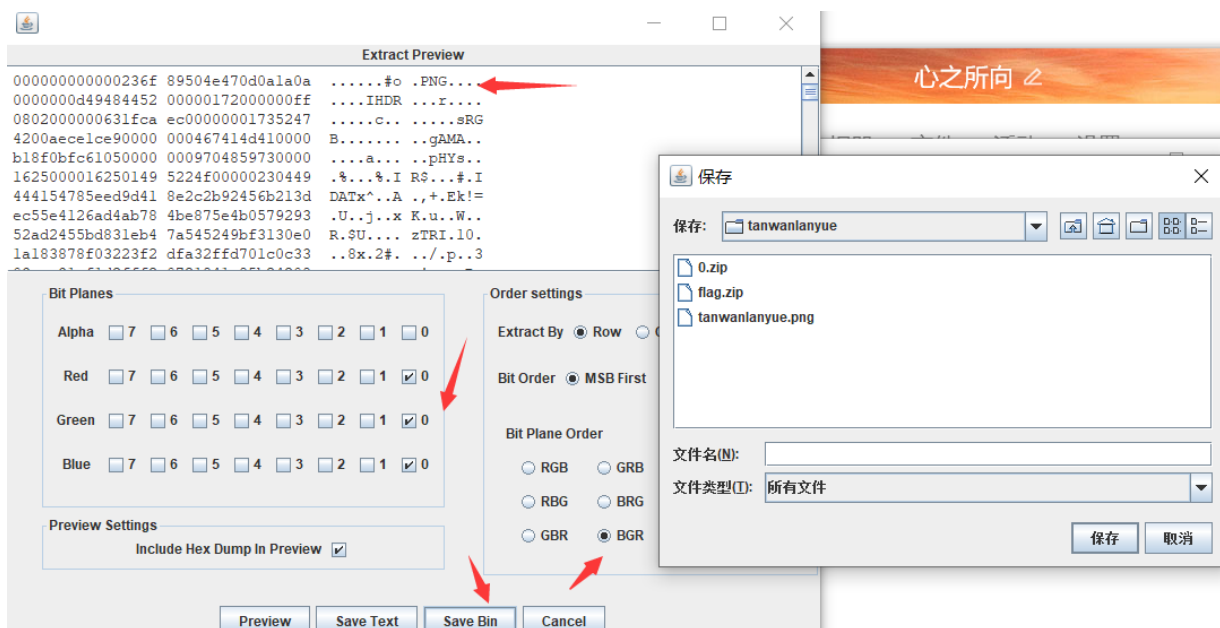
解压出来一个压缩包和一张图片, winhex没发现什么东西, binwalk/foremost也正常, 分离不出来东西

用stegsolvef中的LSB隐写分析, 选择Data Extract, 这里对图中左下角的RGB等一个个的试, 最后在选择BGR的时候有数据, 但是可以看到, 在PNG图片固定开头的前面多了些东西, 用winwex打开的时候删除掉就行了, 最后得到下面熟悉的台词, 省略的地方就是压缩文件的密码(zhazhahui)。居然还没完。。。

解压之后得到的字符: f_hfv7m_y8{kThk43a_xrk0?n}, 凯撒在线解密: <https://www.qqxiuzi.cn/bianma/kaisamima.php> (偏移设置19)

得到: m_omc7t_f8{rAor43h_eyr0?u}, 之后栅栏解密就行了, 在线解密: <https://www.qqxiuzi.cn/bianma/zhalanmima.php>.

get flag: moctf{Ar3_y0u_m7_8ro4her?}



```
m_omc7t_f8{rAor43h_eyr0?u}
```

每组字数

```
moctf{Ar3_y0u_m7_8ro4her?}
```

0x10.百变flag

题目链接: <http://119.23.73.3:6001/misc6/f1ag.png>

图片文件，winhex不解释，发现隐藏一个flag.exe，而且进行加密了。解压之后里面有一个flag.exe文件，再次winhex打开

20	17	F8	F9	FC	88	1C	2B	17	F8	39	BE	63	F8	B3	8B	80	øüü" + ø9%çø* <€
36	F9	65	5C	51	00	C5	F3	22	90	77	09	F3	A3	FC	51	0F	ùè\Q Áó" w ófúQ
52	27	E0	77	3D	AC	81	3F	EA	F1	53	B6	2B	28	58	C0	45	'àw=- ?éñsq+(XÀE
68	74	99	03	50	57	07	00	3B	47	7F	45	72	A2	05	E4	CC	t™ PW :G Erç äi
84	FD	3F	50	4B	01	02	1F	00	14	00	09	00	08	00	B2	55	y?PK █ ^U
00	01	4B	39	24	2F	08	DC	58	00	00	1E	8A	00	00	08	00	K9\$/ ÜX š
16	24	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	\$
32	66	31	61	67	2E	65	78	65	0A	00	20	00	00	00	00	00	flag.exe
48	01	00	18	00	B6	65	1D	41	70	0A	D3	01	DE	8A	AC	ED	ŕe Ap Ó ÞŠ-í
64	72	0A	D3	01	DE	8A	AC	ED	72	0A	D3	01	50	4B	05	06	r Ó ÞŠ-ír Ó PK
80	00	00	00	00	01	00	01	00	5A	00	00	00	02	59	00	00	Z Y
96	00	00															

伪加密，将其改为00即可

可以看到，ASCII那里都反过来了

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
09	FF	AF	62	57	B1	AB	D8	55	EC	2A	76	15	BB	8A	5D	Üÿ	bw±«ØUi*v »Š]Å
15	AE	62	57	B1	AB	D8	55	EC	2A	76	15	BB	8A	5D	C5	Å@bw±«ØUi*v »Š]Å	Å
1E	62	57	B1	AB	D8	55	EC	2A	76	15	BB	8A	5D	C5	AE	@bw±«ØUi*v »Š]Å@	
52	57	B1	AB	D8	55	EC	2A	76	15	BB	8A	5D	C5	AE	62	bw±«ØUi*v »Š]Å@b	
57	B1	AB	D8	55	EC	2A	76	15	BB	8A	5D	C5	AE	62	57	w±«ØUi*v »Š]Å@bw	
31	AB	D8	55	EC	2A	76	15	BB	8A	5D	C5	AE	62	57	B1	±«ØUi*v »Š]Å@bw±	
1B	D8	55	EC	2A	76	15	BB	8A	5D	C5	EE	75	BB	F9	EA	«ØUi*v »Š]Åíu»ùè	
01	FF	AF	62	57	B1	AB	D8	55	EC	2A	76	15	BB	8A	5D	Ńÿ	bw±«ØUi*v »Š]Å
15	AE	62	57	B1	AB	D8	55	EC	2A	76	15	BB	8A	5D	C5	Å@bw±«ØUi*v »Š]Å	Å
1E	62	57	B1	AB	D8	55	EC	2A	76	15	BB	8A	5D	C5	AE	@bw±«ØUi*v »Š]Å@	
52	57	B1	AB	D8	55	EC	2A	76	15	BB	8A	5D	C5	AE	62	bw±«ØUi*v »Š]Å@b	
57	B1	AB	D8	55	EC	2A	76	15	BB	8A	5D	C5	AE	62	57	w±«ØUi*v »Š]Å@bw	
31	AB	D8	55	EC	2A	76	15	BB	8A	5D	C5	AE	62	57	B1	±«ØUi*v »Š]Å@bw±	

全是反的

用的mo0rain这位大哥的python脚本。（这里用的python2运行的，flag.exe放到了python2的根目录下，生成的flag.jpg也是在根目录下）得到的图片上就有flag

```
get flag: moctf{1mage is funny}
```

```
f=open('flag.exe','rb')
b=open('flag.jpg','wb')
R=f.read()[::-1]
b.write(R)
```



0x11.蒙娜丽莎的微笑

题目链接: <https://pan.baidu.com/s/1h0UrrztPaske05G6bWoQ0Q> 提取码: prhm

和上面一样,压缩包使用的是伪加密,同样改09为00之后就可以解密,解压之后得到女朋友一个(有趣)可以看到图片的高宽有点不协调,下面应该还有东西,winhex打开,修改高度,将74改为F4,这样就可以高宽差不多了。

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	4
6	00	00	01	F4	00	00	01	74	08	03	00	00	00	F8	7
2	15	00	00	00	19	74	45	58	74	53	6F	66	74	77	6
8	65	00	41	64	6F	62	65	20	49	6D	61	67	65	52	6
4	64	79	71	C9	65	3C	00	00	03	10	69	54	58	74	5
0	4C	3A	63	6F	6D	2E	61	64	6F	62	65	2E	78	6D	7
6	00	00	00	00	3C	3F	78	70	61	63	6B	65	74	20	6
2	67	69	6E	3D	22	EF	BB	BF	22	20	69	64	3D	22	5
8	4D	30	4D	70	43	65	68	69	48	7A	72	65	53	7A	4
4	63	7A	6B	63	39	64	22	3F	3E	20	3C	78	3A	78	6
0	6D	65	74	61	20	78	6D	6C	6E	73	3A	78	3D	22	6

修改之后得到这样的图片,对图中的字符进行base64解码, c2ltbGVpc2ludGVyaW5n→simleisintering

不是flag,应该里面还隐藏得有文件,binwalk(或者直接改后缀为zip),打开需要密码,密码就是上面bsae64解码的字符, get flag: moctf{Int3resting_piXe1}



0x12.李华的双十一

题目链接: <https://pan.baidu.com/s/1enWLOxZQPr4rbKiG4Xq-uQ> 提取码: h450

hint: 程序员李华双十一帮女朋友清了购物车, 但是场面太过惨烈以至于他都不愿意回忆起那个数字, 你能帮他回忆一下吗?

又是压缩包, 又是伪加密, 不过这次有两处需要改。解压之后还有压缩包和MP3。money.zip, 不过不是伪加密了, 根据提示

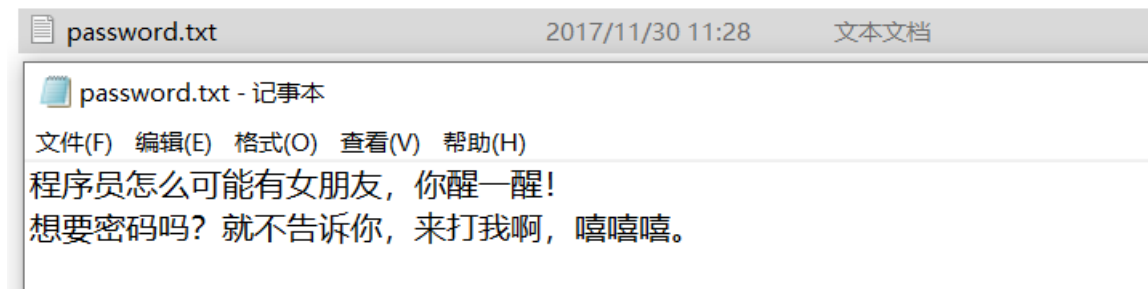
放ARCHPR里面纯数字暴力破解。

```
03 81 58 36 21 73 3E 3A 1D C0 21 10 33 DA F3 D0
93 B3 EB 3C 9A 9A 9A 76 80 FF 01 50 4B 01 02 1F
00 14 00 09 00 08 00 88 5B 7E 4B 3E E4 CD 19 E9
00 00 00 24 01 00 00 09 00 24 00 00 00 00 00 00
00 20 00 00 00 00 00 00 00 6D 6F 6E 65 79 2E 7A
69 70 0A 00 20 00 00 00 00 00 01 00 18 00 AC 88
10 43 8B 69 D3 01 0D 5B D1 41 5D B1 D3 01 0D 5B
D1 41 5D B1 D3 01 50 4B 01 02 1F 00 14 00 09 00
08 00 1B A9 61 4C 6C 62 F4 9C 30 74 31 00 0C 2C
32 00 0D 00 24 00 00 00 00 00 00 00 20 00 00 00
10 01 00 00 73 69 6E 67 6C 65 64 6F 67 2E 6D 70
33 0A 00 20 00 00 00 00 00 01 00 18 00 BA E3 D8
73 5E B1 D3 01 91 A5 3A 98 5E B1 D3 01 8A A7 D2
41 5D B1 D3 01 50 4B 05 06 00 00 00 00 02 00 02
00 BA 00 00 00 6B 75 31 00 00 00
```

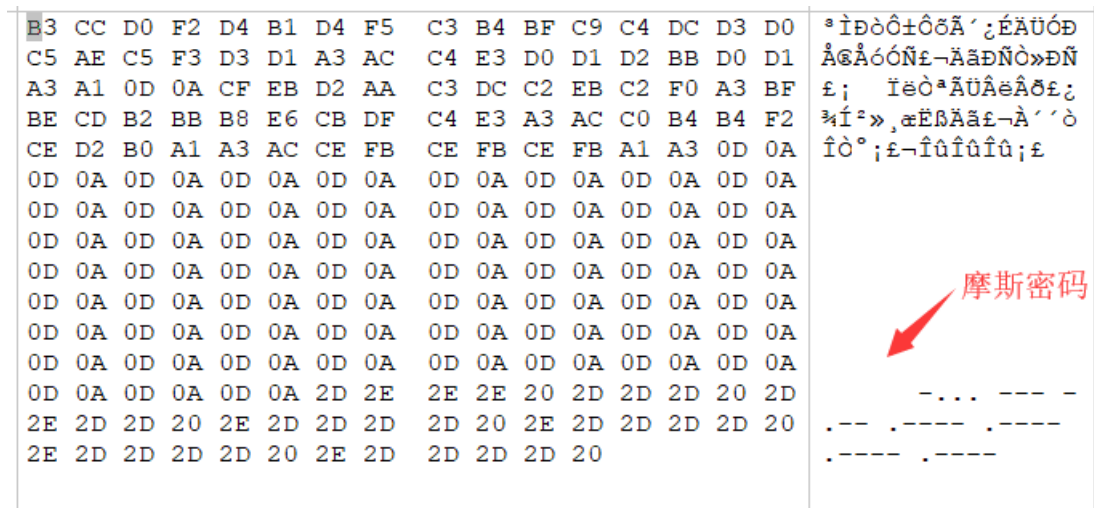
```
X6!s>: A! 3UoD
""e<šššveÿ PK
^ [~K>aí é
$ $
money.z
ip -^
C<ió [ŃA]±ó [
ŃA]±ó PK
@aLlbôœ0t1 ,
2 $
singledog.mp
3 °ãø
s^±ó `¥:~^±ó ššò
A]±ó PK
° kul
```



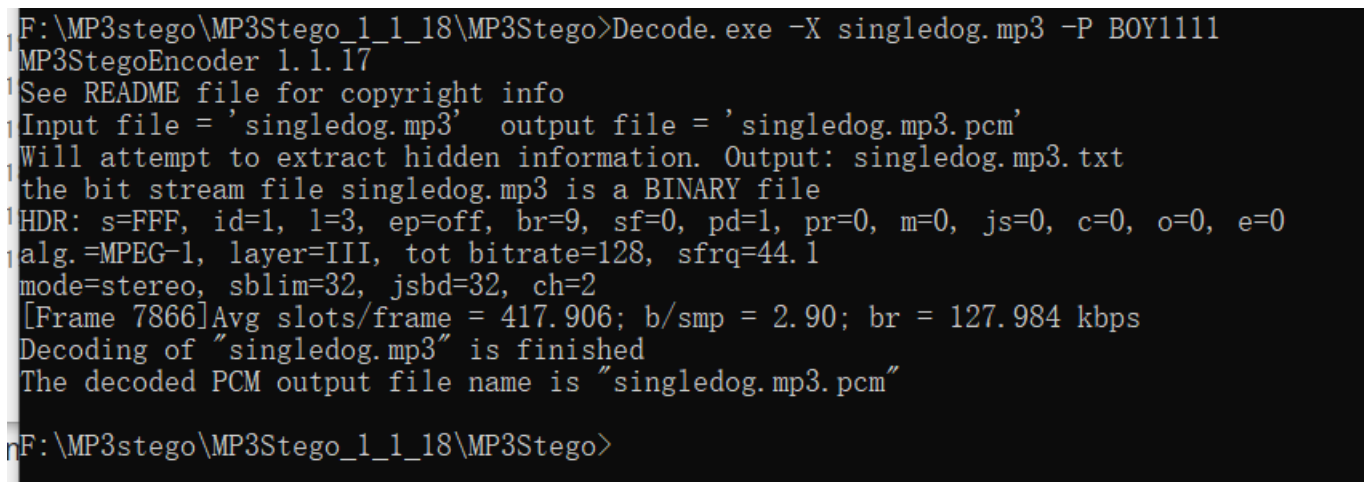
money.zip解压之后, 给单身狗致命一击。



winhex打开试试，摩斯密码



解码之后为BOY1111，应该是用来解上面得到的MP3，这里需要用到MP3Stego进行解密，这里需要将mp3放到MP3Stego下。



在MP3Stego下会得到一个txt文档，打开为bW9jdGZ7I1MxbmDsM19EMGcjfQ==，base64解码

get flag: moctf{#S1ngl3_D0g#}

0x13.李华的疑惑

题目链接: <https://pan.baidu.com/s/1Wcufz9zZkSAW532Ei0D4OQ> 提取码: w97c

压缩包解压之后，得到一个password.txt和一个压缩包(需要密码，不是伪加密了)，应该是前面的txt解除密码。

打开之后看到一大堆255，misc，web?用notepad++打开之后，发现有22500行，这里应该就是RGB转图片了

```
22491 255,255,255
22492 255,255,255
22493 255,255,255
22494 255,255,255
22495 255,255,255
22496 255,255,255
22497 255,255,255
22498 255,255,255
22499 255,255,255
22500 255,255,255
```

Normal text file length : 267,890

这里用了大佬们的脚本，现在还小，不会写脚本（呜呜），需要先安装PIL库，cmd→easy_install Pillow进行安装的：

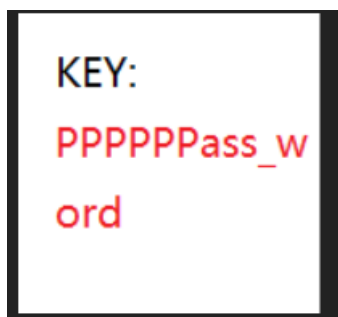
```
#-*- coding:utf-8 -*-
from PIL import Image
#这里可能需要通过pip install PIL命令安装Python的PIL库，强烈建议直接kali: 自带库，而且安装库也方便
import re

x = 150 #x坐标 通过对txt里的行数进行整数分解
y = 150 #y坐标 x*y = 行数
#猜测的行数要改好，不要漏了

im = Image.new("RGB", (x,y)) #创建图片
file = open('misc100.txt') #打开rbg值文件

#通过一个个rgb点生成图片
for i in range(0,x):
    for j in range(0,y):
        line = file.readline() #获取一行
        rgb = line.split(",") #分离rgb
        im.putpixel((i,j), (int(rgb[0]), int(rgb[1]), int(rgb[2]))) #rgb转化为像素
im.show()
```

python2运行之后得到一个图片，用PPPPPPass_word对flag.zip进行解密



得到一串字符

```
U2FsdGVkX18R9Ey1BVacP/j0XpCISh9nZth6TFwoh5GUv0edeVp3ZV9gXVqd/r1H660IZgSHn2Mock4hcdqFE==
```

复制粘贴，base64一顿操作，不对，base12也不对，最后试了AES，成功解出来，AES在线解密地址：<http://tool.oschina.net/encrypt/>。

```
get flag: moctf{D0_You_1ik3_tO_pAinH_wi4h_pi8e1}
```

明文:

mocff{D0_You_1ik3_tO_pAinH_wi4h_pi8e1}

加密算法:

- AES
- DES
- RC4
- Rabbit
- TripleDes

密码:

密文:

U2FsdGVkX18R9EyIBVacPj0XpClSh9nZth6TFwoh5GUv0edeVp3ZV9gXVqd/riH66OlZgSHn2Mock4hcdqFEg==

0x14.奇怪的01

题目链接: https://pan.baidu.com/s/1IPK9usOLDRK3K6a8QM_m0w 提取码: hjrr

解压得到一个flag的压缩包和一个manchester.txt, 看txt名字, 知道是曼切斯特编码,

这里用的是Cosmos大哥的脚本进行解码的, 小菜鸡还不会写脚本(好难受)

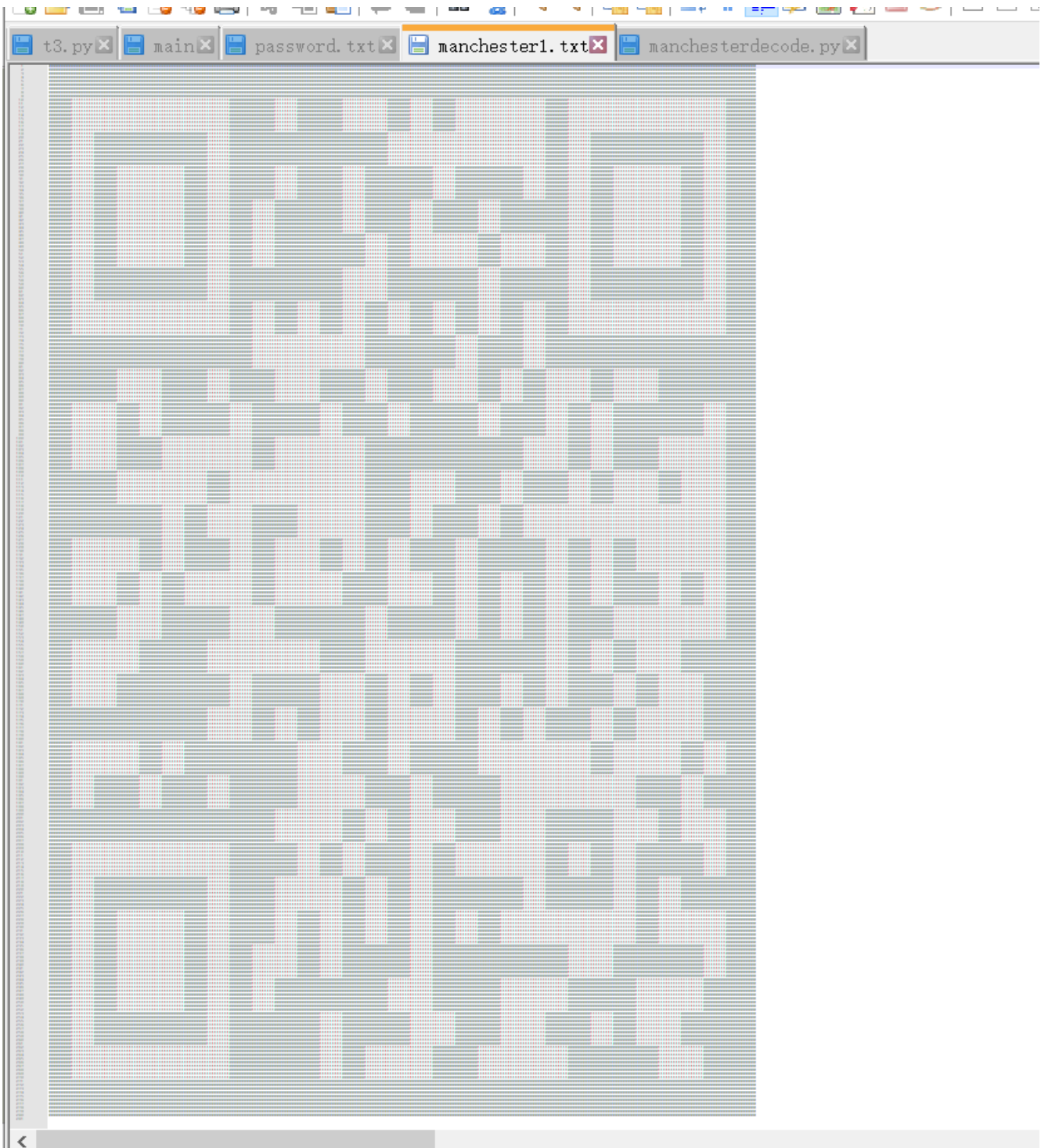
```
#!/usr/bin/env python
#-*- coding:utf-8 -*-

f=open('manchester.txt','r')
f1=open('manchester1.txt','w')

for line in f.readlines():
    content=''
    for i in range(0,len(line),2):
        if line[i:i+2]=='10':
            content+='1'
        else: #01
            content+='0'
    f1.write(content+'\n')

f.close()
f1.close()
```

解压之后的文本, Notepad++打开, 然后一直缩小就会发现一个二维码(出题大哥脑洞真大, 做出来的大哥也好厉害, 另外我的记事本和sublime_text打开缩小看不到完整的二维码)



死活没扫出来（不知道是不是我自己的原因），然后截图用Stegsolve打开进行，一个个找，找一个颜色比较深（黑一点的？）一点的来扫。扫描得到：`m0ctf{Wr0ng_Answ3r}`

< 返回

扫描结果

扫描到以下内容

```
moctf{Wr0ng_Answ3r}
```

用扫出来的字符对压缩包进行解压，得到摩斯密码，解码就行了

```
-----  
-----
```

get flag: moctf{wha7-a-fuck1ng-qr-c0de}

转载于:<https://www.cnblogs.com/mortals-tx/p/11273745.html>