




# moctf misc writeup

原创

烟敛寒林o  于 2019-04-28 19:06:01 发布  613  收藏

分类专栏: [★CTF # ——【Misc】](#)

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/dyw\\_666666/article/details/89599664](https://blog.csdn.net/dyw_666666/article/details/89599664)

版权

## CTF

[★CTF 同时被 2 个专栏收录](#)

55 篇文章 2 订阅

订阅专栏



[——【Misc】](#)

1 篇文章 0 订阅

订阅专栏

1.我可是黑客

2.假装安全

3.扫扫出奇迹

4.光阴似箭

5.杰斯的魔法

6.流量分析

7.女神的告白

8.捉迷藏

9.是兄弟就来干我

10.百变flag

11.蒙娜丽莎的微笑

12.李华的双十一

---

### 1.我可是黑客

打开题目是一张图片, 保存到本地, 即:



一般第一题都是签到题，所以直接用nodepad++打开，在文档的最后面发现flag。

```

[!NUL]祢貽櫛NULNULACK€埒k?FSV这娼锋藩 ?
龍NUL齋[炴诋壘 SI ETXku榭p??n誥;嫖%"SI I) STX" ""ST
·教Z ??=NAKRS们飼DC1j禾峇赌?肠* 潔?~滌螳鷓翩w滹?=\1
ULNULNULNULmactf{e4sy_1ma9e_m1sc}
  
```

mactf{e4sy\_1ma9e\_m1sc}

## 2. 假装安全

同上题，先将图片保存到本地，再用nodepad++打开，即：

可以看到，在文档的最后面有flag.txt，这说明，这个图片不是一张简单的图片，他里面包含了文件，需要分离出来。。。

修改图片后缀名为zip，解压发现有伪加密，所以我们用 winhex 打开zip包查看一下。。。

Offset	U	L	Z	S	O	F	O	A	D	C	V	E	F	Hex	ASCII		
00004920	41	D0	02	F5	65	6F	AD	30	1E	77	89	9C	9A	02	8F	71	AD 0ec-0 wħαš q
00004930	F5	99	30	02	A4	88	33	3F	F5	EF	C6	A3	BB	C1	BE	28	õ"0 ɦ^3?điĤē»Á%( 4Z»Ūs1E)I^@4łot
00004940	34	8E	BB	DA	73	31	45	29	4C	AA	40	40	BC	C0	6F	86	-ŀ JVLiBÈtùB ;)É
00004950	AC	30	1F	4A	56	4C	ED	DF	C8	89	F9	42	1A	A1	29	C9	N!á ä "o" ó4- İÒ
00004960	4E	21	E2	11	E4	8D	99	6F	22	0C	F3	34	97	0B	CC	D2	=4ø{AóEŁtJ= ôiz@
00004970	3D	34	F8	7B	41	F4	45	A3	86	4A	3D	0E	F5	EE	5A	40	ŽR )Đ^ »FS U+†Ě
00004980	8E	52	10	29	D0	88	1B	BB	50	A7	13	55	86	D7	86	CB	ME fòĤ-c'™±<4
00004990	0F	4D	C6	0B	66	F2	C5	97	A2	27	99	B1	3C	34	14	0A	Sňä;ÿýiē÷ÿ PK ?
000049A0	A7	F1	E4	A1	FF	FD	ED	EB	F7	FF	00	50	4B	01	02	3F	: K š^'...
000049B0	00	14	00	09	08	08	00	3A	A0	05	4B	02	F0	08	B3	85	Ī ůđ \$
000049C0	49	00	00	D1	64	00	00	08	00	24	00	00	00	00	00	00	Flag.jp
000049D0	00	20	00	00	00	00	00	00	00	66	6C	61	67	2E	6A	70	í
000049E0	67	0A	00	20	00	00	00	00	00	01	00	00	00	00	00	00	g
000049F0	9F	E2	0D	D3	01	CE	10	05	9F	E2	0D	D3	01	EA	56	59	Ÿá ó í Ÿá ó évy
00004A00	88	E2	0D	D3	01	50	4B	05	06	00	00	00	00	01	00	01	^á ó PK
00004A10	00	5A	00	00	00	AB	49	00	00	00	00	00	00	00	00	00	Z «I

Annotations in the image:  
 - Red arrow pointing to '09 08' in offset 000049B0: 压缩原文件目录区  
 - Red arrow pointing to '50 4B' in offset 000049A0: 全局方式位标记，将09改成00，伪加密就没了  
 - Red arrow pointing to '00 00' in offset 000049D0: 压缩原文件目录结束标志

mcfCrflyS1eot{@eul\_id}

很明显不是正常flag。。。需要用到栅栏密码解密一下。。。

```
mcfCrflySleot{@eul_ld}
```

每组字数 2

加密

解密

```
moctf{C@refully_Sl1de}
```

[https://blog.csdn.net/dyw\\_666666](https://blog.csdn.net/dyw_666666)

```
moctf{C@refully_Sl1de}
```

另一种方法：

我们可以使用 kali 中的 **binwalk** 工具进行分离

在图片所在目录下，命令框执行语句：

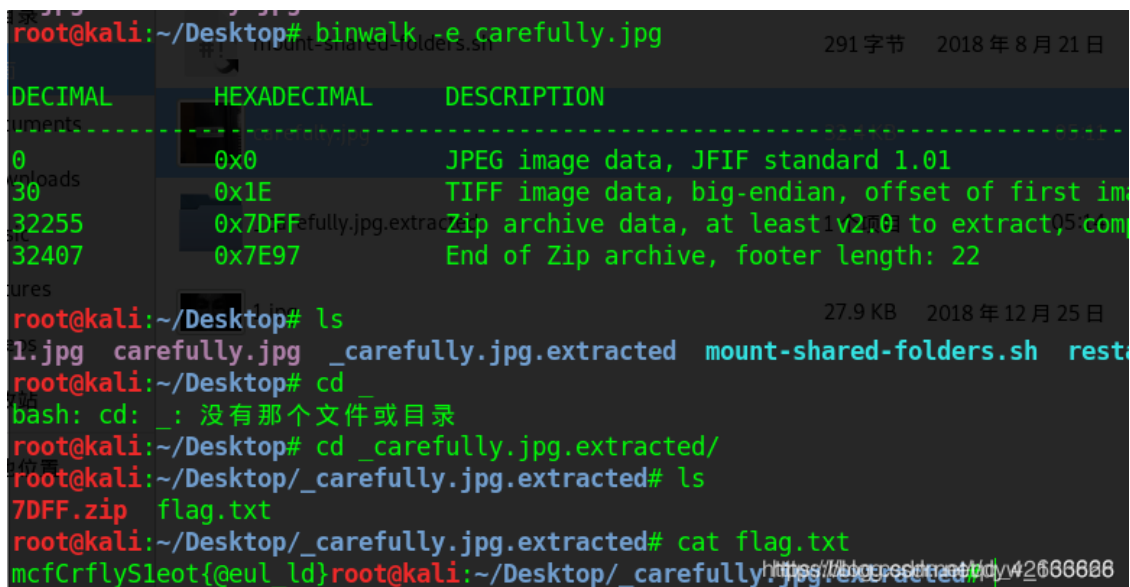
```
binwalk -e carefully.jpg //分离出carefully.jpg里的文件

ls

cd _carefully.jpg.extracted/ //进入分离出来的文件

ls

cat flag.txt //查看flag
```



```
root@kali:~/Desktop# binwalk -e carefully.jpg
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          JPEG image data, JFIF standard 1.01
30          0x1E         TIFF image data, big-endian, offset of first image
32255       0x7DFF       Zip archive data, at least v2.0 to extract, compressed
32407       0x7E97       End of Zip archive, footer length: 22

root@kali:~/Desktop# ls
1.jpg  carefully.jpg  _carefully.jpg.extracted  mount-shared-folders.sh  rest

root@kali:~/Desktop# cd _
bash: cd: _: 没有那个文件或目录
root@kali:~/Desktop# cd _carefully.jpg.extracted/
root@kali:~/Desktop/_carefully.jpg.extracted# ls
7DFF.zip  flag.txt
root@kali:~/Desktop/_carefully.jpg.extracted# cat flag.txt
mcfCrflySleot{@eul_ld}
```

```
moctf{C@refully_Sl1de}
```

### 3. 扫描出奇迹

同上题，先将图片保存到本地。可以看到，这是一张二维码，首先的反应一般都是先扫一扫



但是，不论怎么扫都扫不出来。。。

这时就应该检查一下二维码了，

从二维码可以很明显的看出“黑白分明”，那会不会他是反着来的？

上工具StegSolve。



这回，在扫一扫，flag就出来了。。。。。

moc{qr\_code\_1s\_1n\_1t}

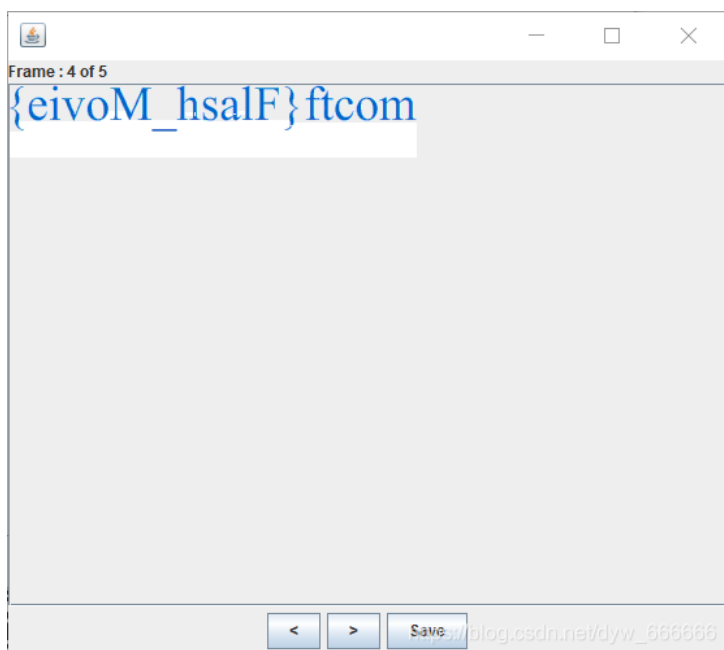
---

#### 4.光阴似箭

同上题，先将图片保存到本地。打开图片，可以看到，有flag闪过。。。。

## Where is the flag ?

直接上工具，StegSolve，利用 Analyse 的 Frame Brower，即：



moctf{Flash\_Movie}

---

## 5.杰斯的魔法

打开题目，这道题看来并不是一道图片题，并且页面给出了一串代码，瞅着像JS代码。。。

尝试在console里运行，即：

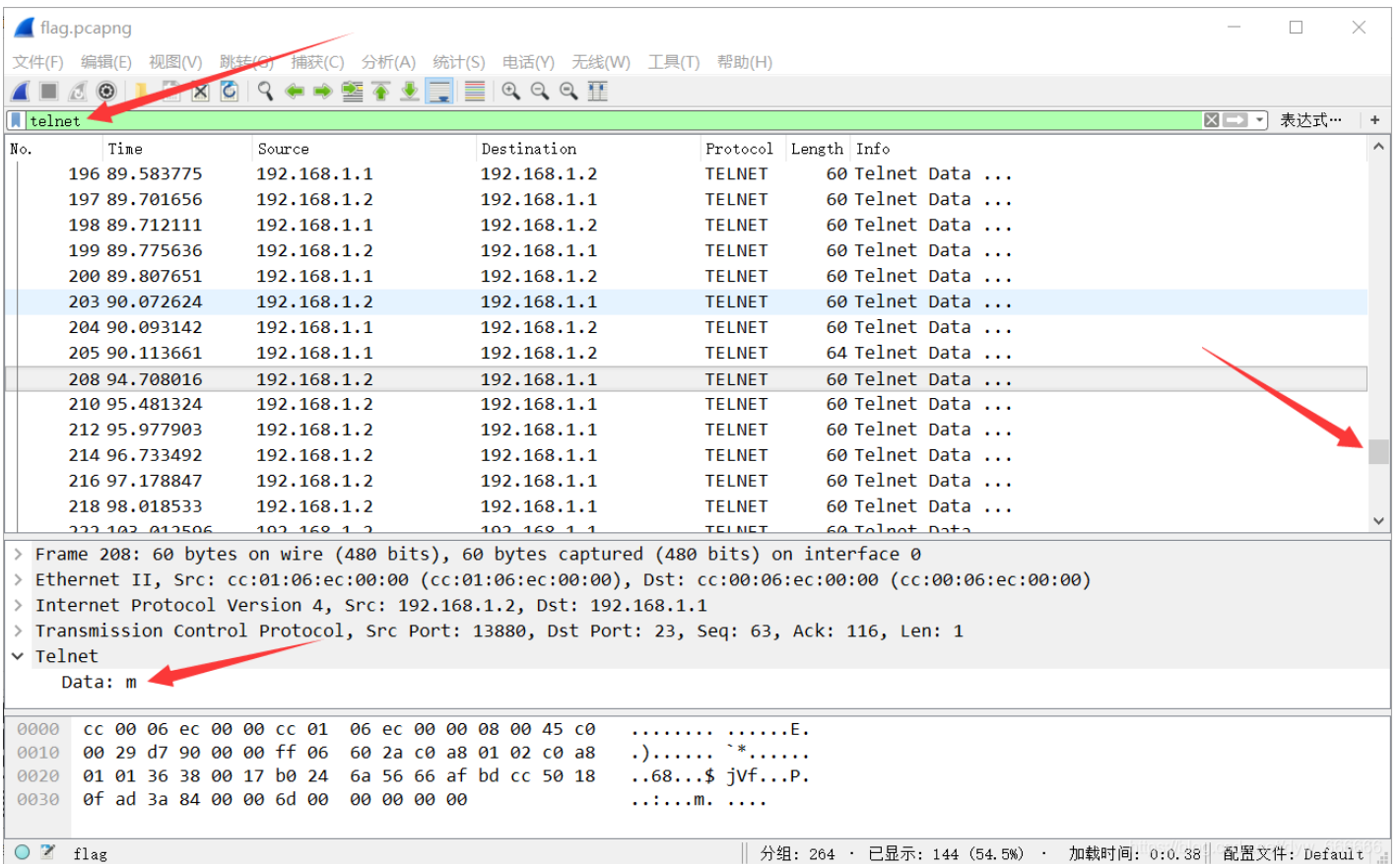


moctf{scr1pt\_1s\_magical}

---

## 6.流量分析

下载好题目给的文件，是一个以.pcapng结尾的文件，可以知道是一道流量分析题，用wireshark打开。。。



一个个包一直点就看到了。。 然后把flag拼接起来。。。

moctf{c@N\_y0U\_4lnd\_m8}

## 7.女神的告白

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？

所以我们可以知道压缩包的解压密码开头几个是meimei。

解压压缩包发现有密码。

所以我们需要用一个字典生成器生成的一个密码字典，再用另一个工具爆破密码。





爆破出来密码，meimei5435。

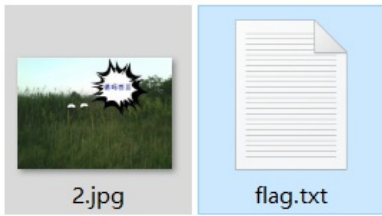


输入密码，解压文件得到flag:

moctf{Y0u\_@re\_A\_g00d\_man}

## 8.捉迷藏

下载，并解压题目给的安装包，可以看到两个文件：



打开flag.txt，里面有一串字符串，base64解码后得到一个flag，但是不是真的flag。。。。

当前位置： [站长工具](#) > [Base64加密解密](#)

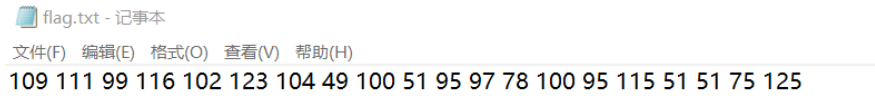
文字加密解密    MD5加密/解密    URL加密    JS加/解密    JS混淆加密压缩    ESCAPE加/解密    **BASE64**    散列

---

<code>moc{Bu_yA0_t1_j1a0}</code>	<code>bW9jdGZ7QnVfeUEwX3QxX2oxYTB9</code>
----------------------------------	---

[https://blog.csdn.net/dyw\\_666666](https://blog.csdn.net/dyw_666666)

所以目标转为图片，先把图片后缀名改为zip，解压出来得到一个新的flag.txt。。。。



打开发现一串ASCII码值。。。

<http://www.ab126.com/goju/1711.html>



## ASCII在线转换器-十六进制, 十进制, 二进制

ASCII转换到 ASCII (例: a b c)

```
m o c t f { h 1 d 3 _ a N d _ s 3 3 K }
```

添加空格

删除空格

将空白字符转换

十六进制转换到16进制(例:0x61或61或61/62)  删除 0x

```
0x6d 0x6f 0x63 0x74 0x66 0x7b 0x68 0x31 0x64 0x33  
0x5f 0x61 0x4e 0x64 0x5f 0x73 0x33 0x33 0x4b 0x7d
```

十进制转换到 10进制 (例: 97 98 99)

```
109 111 99 116 102 123 104 49 100 51 95 97 78 100 95  
115 51 51 75 125
```

[https://blog.csdn.net/lyw\\_666](https://blog.csdn.net/lyw_666)

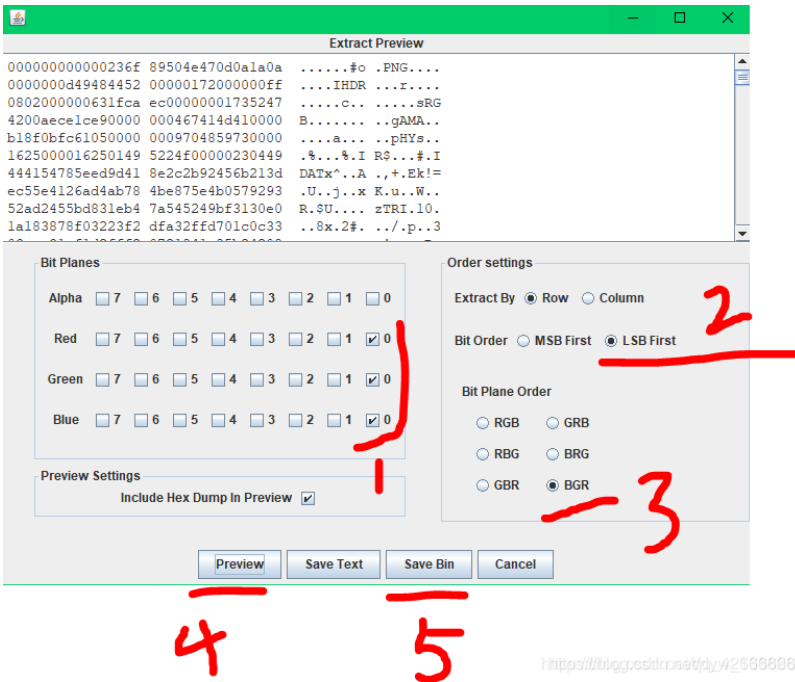
mocftf{h1d3\_aNd\_s33K}

## 9.是兄弟就来干我

下载，并解压题目给的安装包，可以看到：



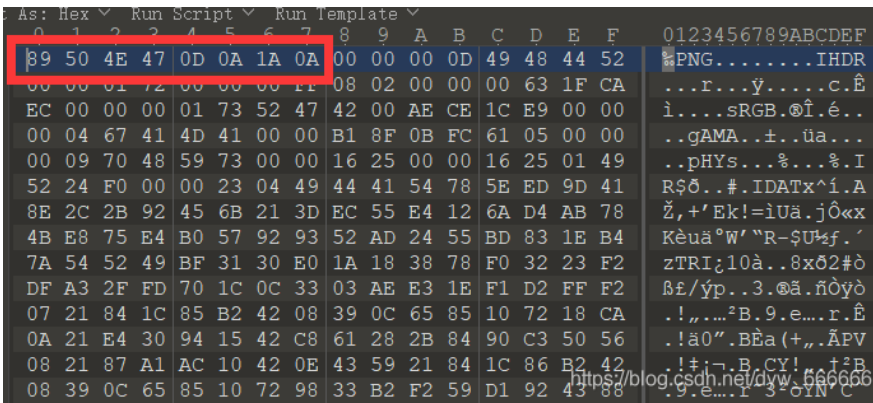
由于打开flag.zip里面的文件需要密码，所以先对图片分析一波，使用StegSolve里的Analyse里的Data Extract:



将文件使用二进制保存，因为png的头文件为八个字节

**89 50 4E 47 0D 0A 1A 0A**

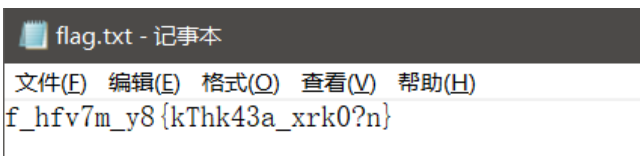
所以使用010Editor打开并将000000000000236f删除保存为新的图片。。。



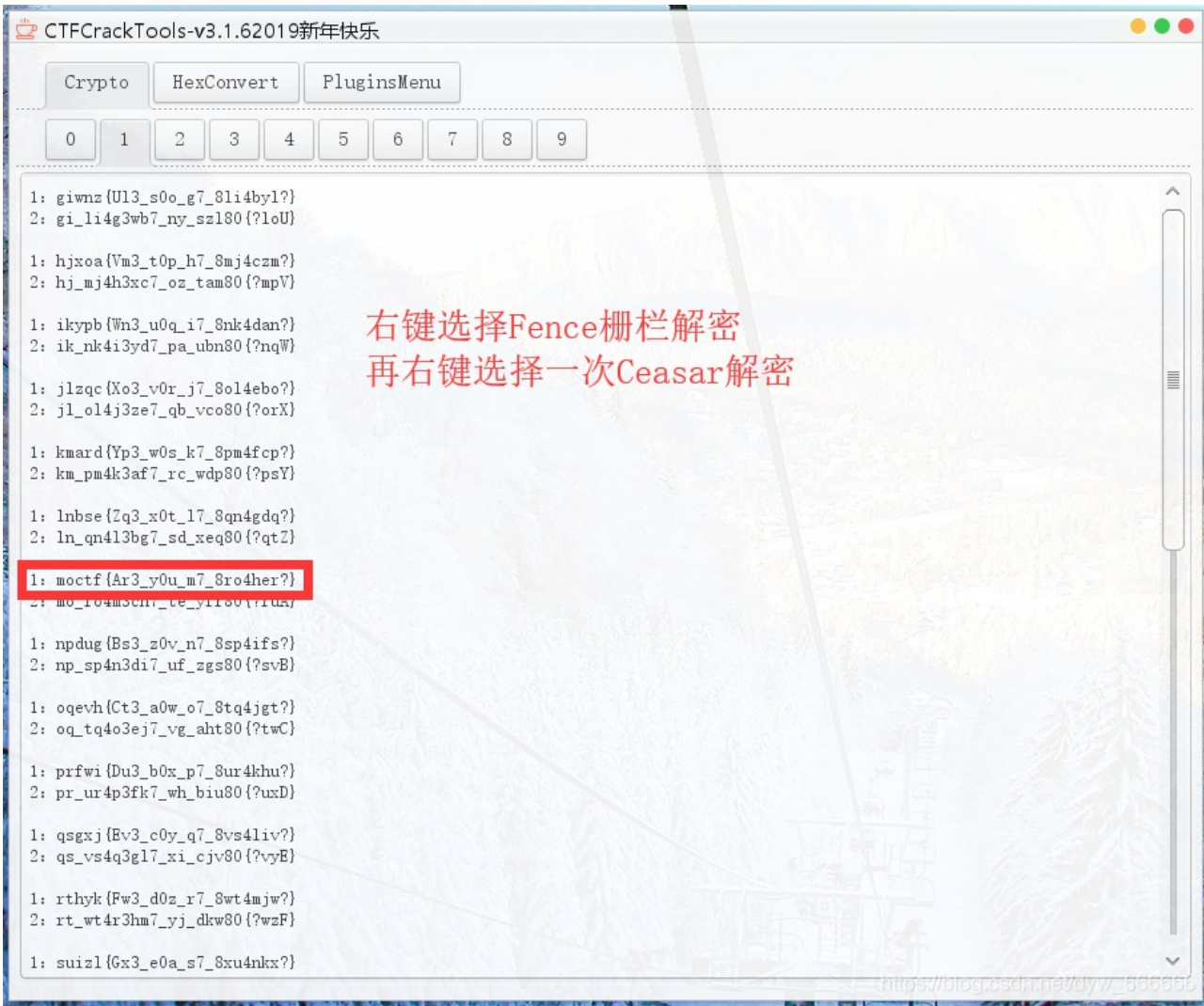
大家好，我是....  
 古天乐骗了我，《贪玩蓝  
 月》里的麻痹戒指根本不值  
 钱!!!

[https://blog.csdn.net/dyw\\_666666](https://blog.csdn.net/dyw_666666)

根据图片提示在猜测名字为zhazhahui的时候解开flag.zip得到flag.txt。。。



栅栏密码解密+凯撒密码解密:



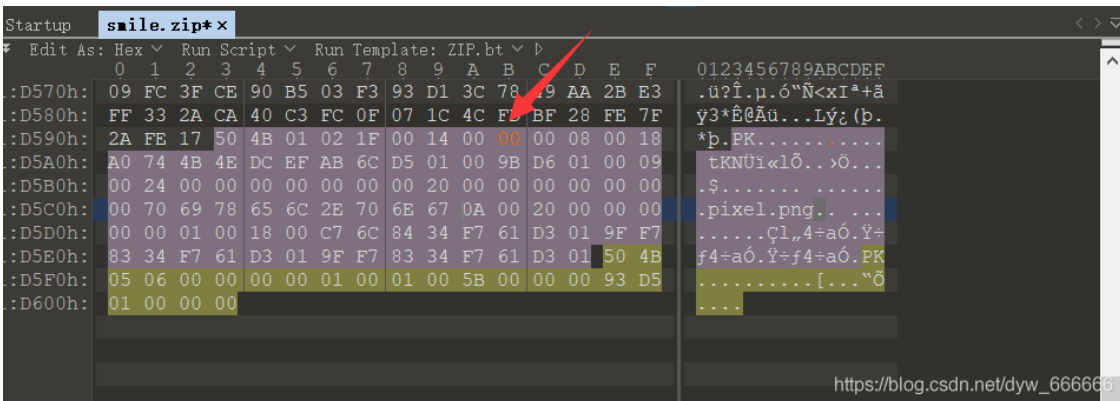
moctf{Ar3\_y0u\_m7\_8ro4her?}

## 10. 百变flag

疑似题已崩。

## 11. 蒙娜丽莎的微笑

首先破伪加密，把09改为00



看到蒙娜丽莎是个秃头猜测可能高度不正确，继续修改高度，把01改为02。

```

Startup pixel.png x
Edit As: Hex Run Script Run Template: PNG.bt
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 01 F4 00 00 02 74 08 03 00 00 00 F8 72 28 ...ø...t....ør(
0020h: 15 00 00 00 19 74 45 58 74 53 6F 66 74 77 61 72 .....tEXtSoftwar
0030h: 65 00 41 64 6F 62 65 20 49 6D 61 67 65 52 65 61 e.Adobe ImageRea
0040h: 64 79 71 C9 65 3C 00 00 03 10 69 54 58 74 58 4D dygEe<...iTXtXM
0050h: 4C 3A 63 6F 6D 2E 61 64 6F 62 65 2E 78 6D 70 00 L:com.adobe.xmp.
0060h: 00 00 00 00 3C 3F 78 70 61 63 6B 65 74 20 62 65 ....<?xpacket be
0070h: 67 69 6E 3D 22 EF BB BF 22 20 69 64 3D 22 57 35 gin="i»;" id="w5
0080h: 4D 30 4D 70 43 65 68 69 48 7A 72 65 53 7A 4E 54 M0MpCehiHzreSzNT
0090h: 63 7A 6B 63 39 64 22 3F 3E 20 3C 78 3A 78 6D 70 czkC9d ?> <x:xmp
https://blog.csdn.net/dyw_666666

```

得到一串字符串:



c2ltbGVpc2ludGVyaW5n



使用base64解密。

明文:

simleisintering

BASE64编码

BASE64解码

BASE64:

c2ltbGVpc2ludGVyaW5n

意思是微笑被埋葬，猜测图片里面大概藏有玄机。发现存有504B0304zip压缩包头标识，504B压缩包结束标识，其中有flag文件。

```

Startup pixel.zip x
Edit As: Hex Run Script Run Template: ZIP.bt
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0000h: 50 4B 03 04 0A 00 01 08 00 00 B2 9E 74 4B 2A 14 PK.....ztk*.
0010h: D5 2A 24 00 00 00 18 00 00 00 04 00 00 00 66 6C Ô*$.....fl
0020h: 61 67 B2 32 4A 6E A9 8E 31 2B 7D 65 DE 47 D1 C3 ag²2Jn©ž1+}ePĜÑ
0030h: 2F 3F 89 F5 E1 6C 35 2D 9F 50 4A D8 93 75 03 7D /?%ôá15-ŸPJØ"u.)
0040h: 01 99 37 A5 54 E1 50 4B 01 02 3F 00 0A 00 01 08 .m7¥TáPK..?....
0050h: 00 00 B2 9E 74 4B 2A 14 D5 2A 24 00 00 00 18 00 ..²žtk*.Ô*$.....
0060h: 00 00 04 00 24 00 00 00 00 00 00 00 20 00 00 00 ....$.....
0070h: 00 00 00 00 66 6C 61 67 0A 00 20 00 0A 00 00 00 ....flag.....
0080h: 01 00 18 00 C5 6B 70 31 F6 61 D3 01 A6 96 75 2E ...Ākp1øaó.|-u.
0090h: F6 61 D3 01 A6 96 75 2E F6 61 D3 01 50 4B 05 06 öaÓ.|-u.öaÓ.PK..
00A0h: 00 00 00 00 01 00 01 00 56 00 00 00 46 00 00 00 .....V...F...
00B0h: 00 00
https://blog.csdn.net/dyw_666666

```

将以504B0304开头部分保存为新文件得到一个压缩包。发现压缩包中有个flag的文件，打开提示需要输入密码，密码就是之前我们得到的smileisintering，输入后使用记事本打开得到flag。

mocf{Int3resting\_piXe1}

## 12.李华的双十一

解压发现有伪加密、修改09为00。。。

```
93 B3 EB 3C 9A 9A 9A 76 80 FF 50 4B 01 02 1F  "e<sssvey PK
00 14 00 00 00 08 00 88 5B 7E 4B 3E E4 CD 19 E9  ^[~K>áí é
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  money.z
69 70 0A 00 20 00 00 00 00 00 01 00 18 00 AC 88  ip
10 43 8B 69 D3 01 0D 5B D1 41 5D B1 D3 01 0D 5B  C< ió [ŃA]±ó [
D1 41 5D B1 D3 50 4B 01 02 1F 00 14 00 00 00  ŃA]±ó PK
08 00 1B A9 61 4C 6C 62 F4 9C 30 74 31 00 0C 2C  @aLlbœœOt1 ,
32 00 0D 00 24 00 00 00 00 00 00 00 20 00 00 00  2 $
10 01 00 00 73 69 6E 67 6C 65 64 6F 67 2E 6D 70  singledog.mp
33 0A 00 20 00 00 00 00 00 01 00 18 00 BA E3 D8  3 °ãø
73 5E B1 D3 01 91 A5 3A 98 5E B1 D3 01 8A A7 D2  s^±ó `¥:^^±ó ššó
41 5D B1 D3 01 50 4B 05 06 00 00 00 00 02 00 02  A]±ó PK
00 BA 00 00 00 6B 75 31 00 00 00  https://blog.csdn.net/dnyw_666666
```

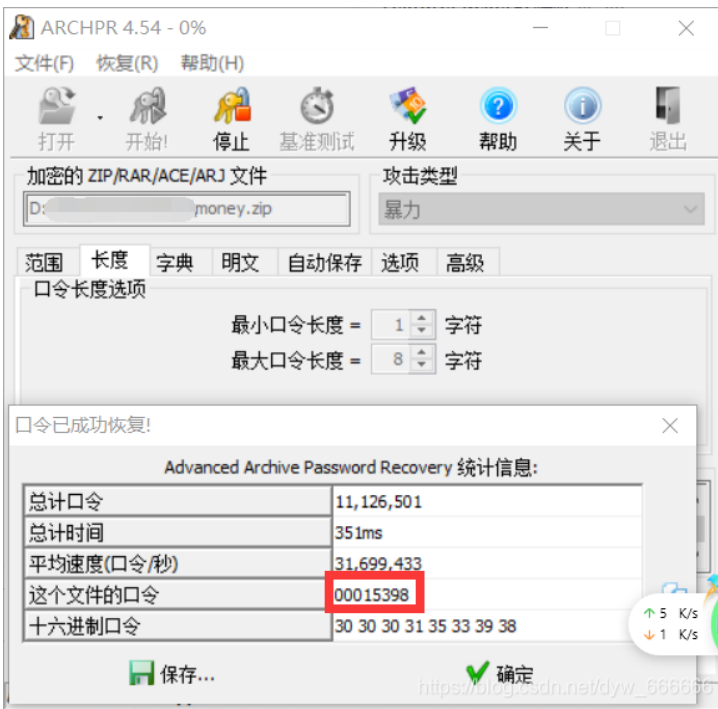
但kali对伪加密其实可以直接提取。。。



得到一个money.zip的压缩包和一个singledog.mp3，都需要密码解密。

那么就只能粗暴一点，直接爆破出他的密码，即：

用ARCHPR暴力破解得到密码00015398。。。



解密money.zip，并打开里面得文件，在文件的最底部，即：



摩斯密码解密得：



这里附上一个CTF编码密码在线工具：

<http://ctf.ssleye.com/>

BOY1111是我们另一个mp3文件的密码，我们可以使用工具MP3Stego，即：

```

D:\MP3Stego_1_1_18\MP3Stego>Decode.exe -X -P BOY1111 singledog.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = 'singledog.mp3' output file = 'singledog.mp3.pcm'
Will attempt to extract hidden information. Output: singledog.mp3.txt
the bit stream file singledog.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=stereo, sblim=32, jsbd=32, ch=2
[Frame 7866]Avg slots/frame = 417.906; b/smp = 2.90; br = 127.984 kbps
Decoding of "singledog.mp3" is finished

```

音乐	singledog.mp3	2019/4/26 16:00	MP3 文件	3,212 KB
桌面	singledog.mp3.pcm	2019/4/26 19:31	PCM 文件	35,400 KB
系统 (C:)	singledog.mp3.txt	2019/4/26 19:31	文本文件	1 KB

### MP3Stego下载链接:

<https://www.petitcolas.net/fabien/software/>

### MP3Stego用法:

解密: 通常做CTF题目用这条命令最多:

```
Decode -X -P 123456 test.mp3
```

其中 123456 是密码

```
加密: encode -E hidden.txt -P 123456 test.mp3
```

打开后得到base64密文字符串。解密得flag。

```
moc tf{#S1ngl3_D0g#}
```