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】

本文链接：https://blog.csdn.net/dyw_666666/article/details/89599664

CTF

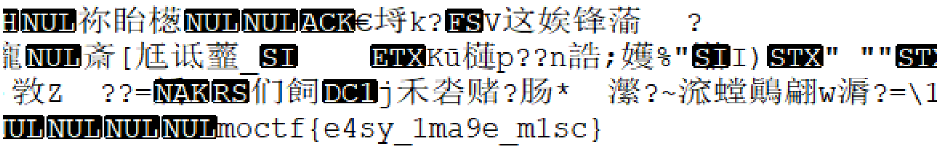
★ CTF 同时被 2 个专栏收录
55 篇文章 2 订阅
订阅专栏


——【 Misc】
1 篇文章 0 订阅
订阅专栏

1.我可是黑客

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。



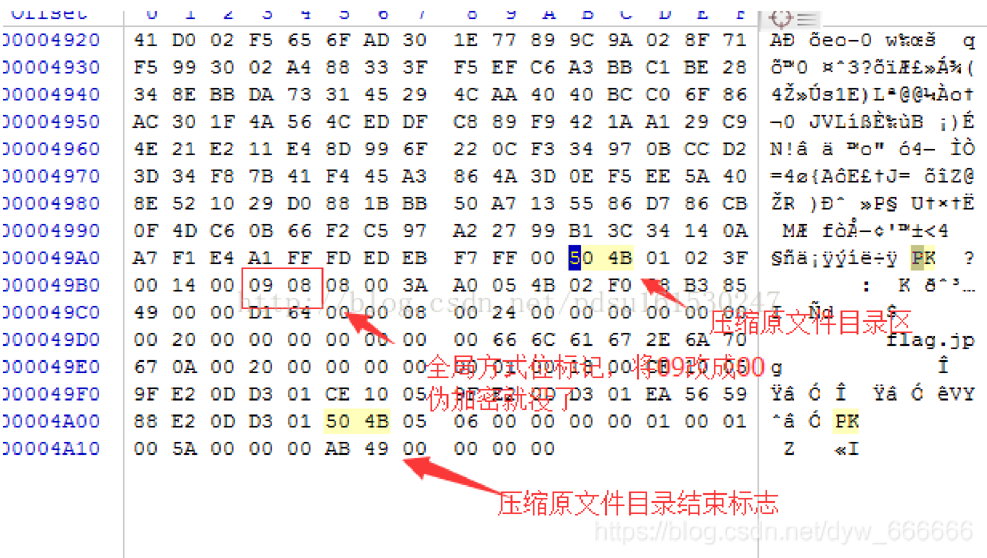
moctf{e4sy_1ma9e_m1sc}

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。。。



mcfCrflyS1eot{@eul_ld}

很明显不是正常flag。。。需要用到栅栏密码解密一下。。。

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：

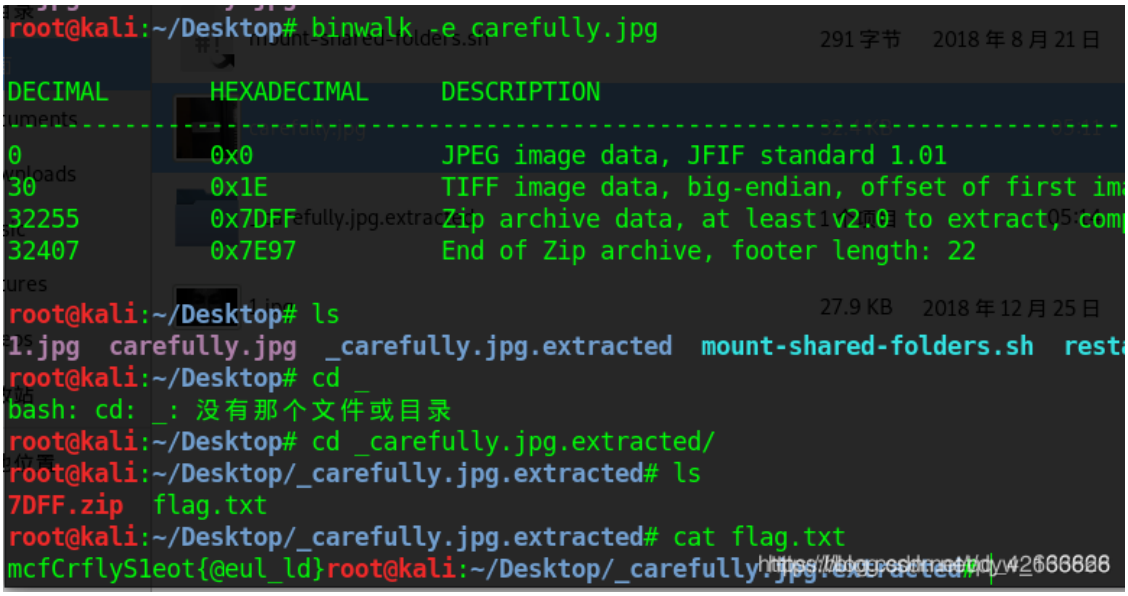
```
binwalk -e carefully.jpg  //分离出carefully.jpg里的文件

ls

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

ls

cat flag.txt    //查看flag
```



moctf{C@refully_Sl1de}

3.扫扫出奇迹

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。。。。。

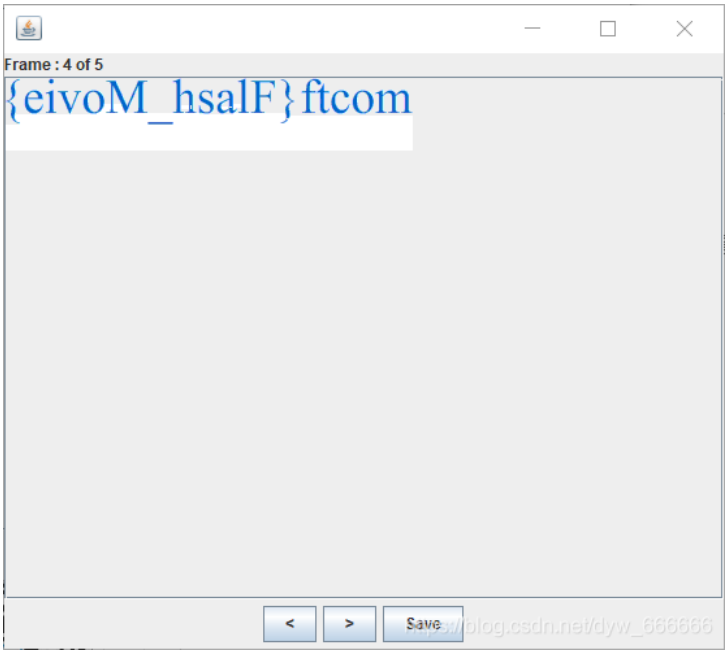
moctf{qr_code_1s_1n_1t}

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

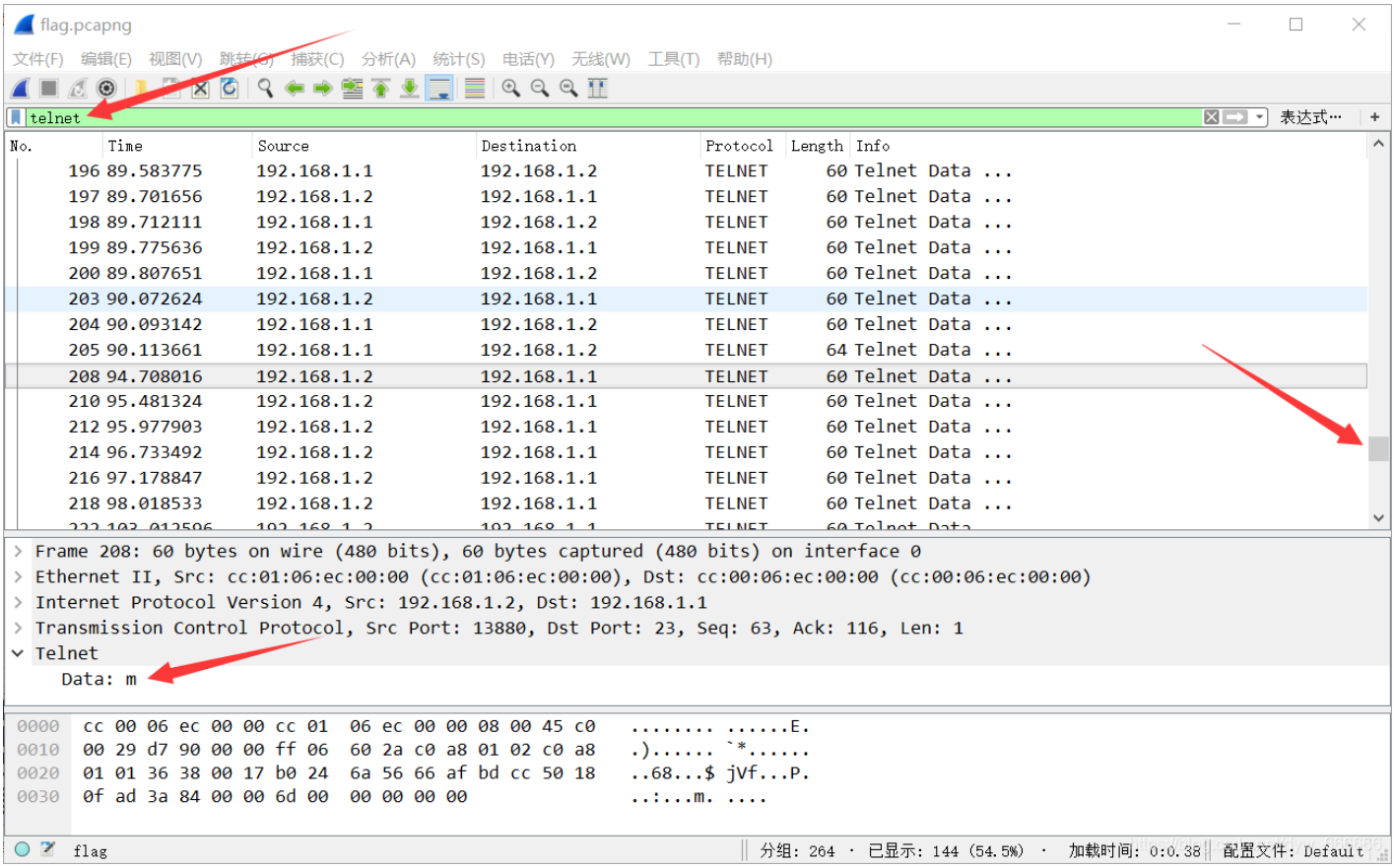
打开题目，这道题看来并不是一道图片题，并且页面给出了一串代码，瞅着像JS代码。。。

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_4Ind_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。

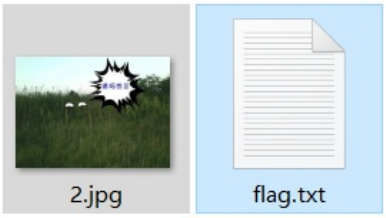
爆破出来密码，meimei5435。

输入密码，解压文件得到flag：

moctf{Y0u_@re_A_g00d_man}

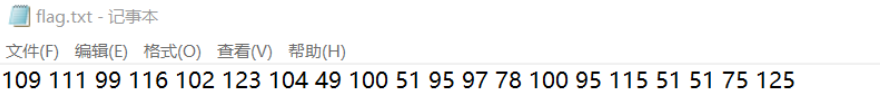
8.捉迷藏

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。。。。

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)

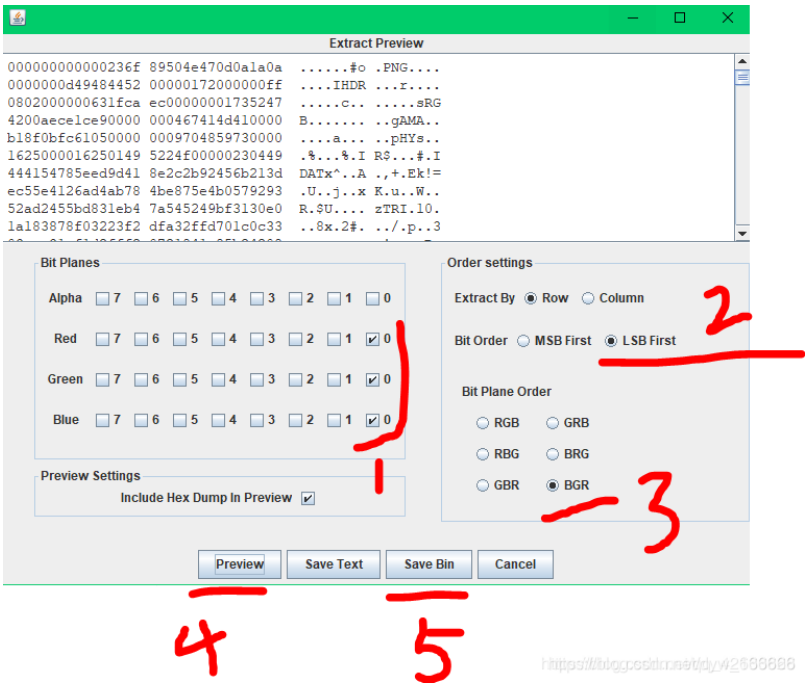
```
109 111 99 116 102 123 104 49 100 51 95 97 78 100 95
115 51 51 75 125
```


moctf{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：

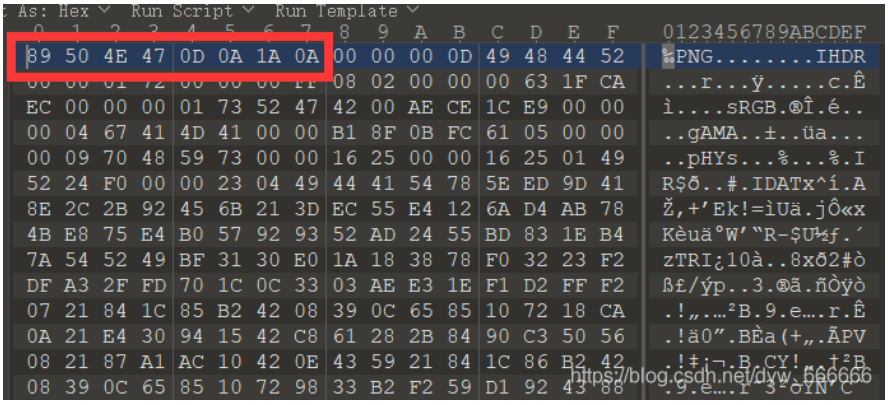
由于打开flag.zip里面的文件需要密码，所以先对图片分析一波，使用StegSolve里的Analyse里的Data Extract：

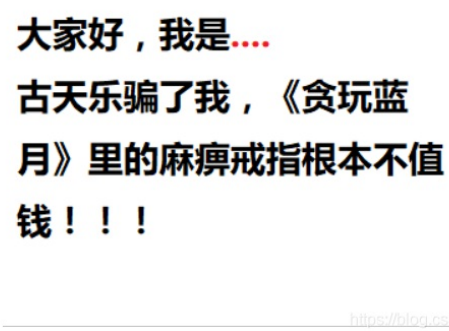


将文件使用二进制保存，因为png的头文件为八个字节

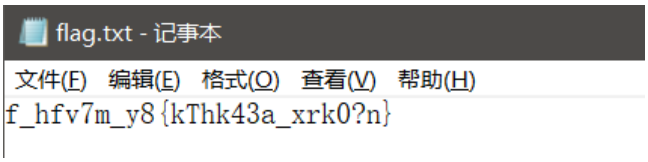
89 50 4E 47 0D 0A 1A 0A

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

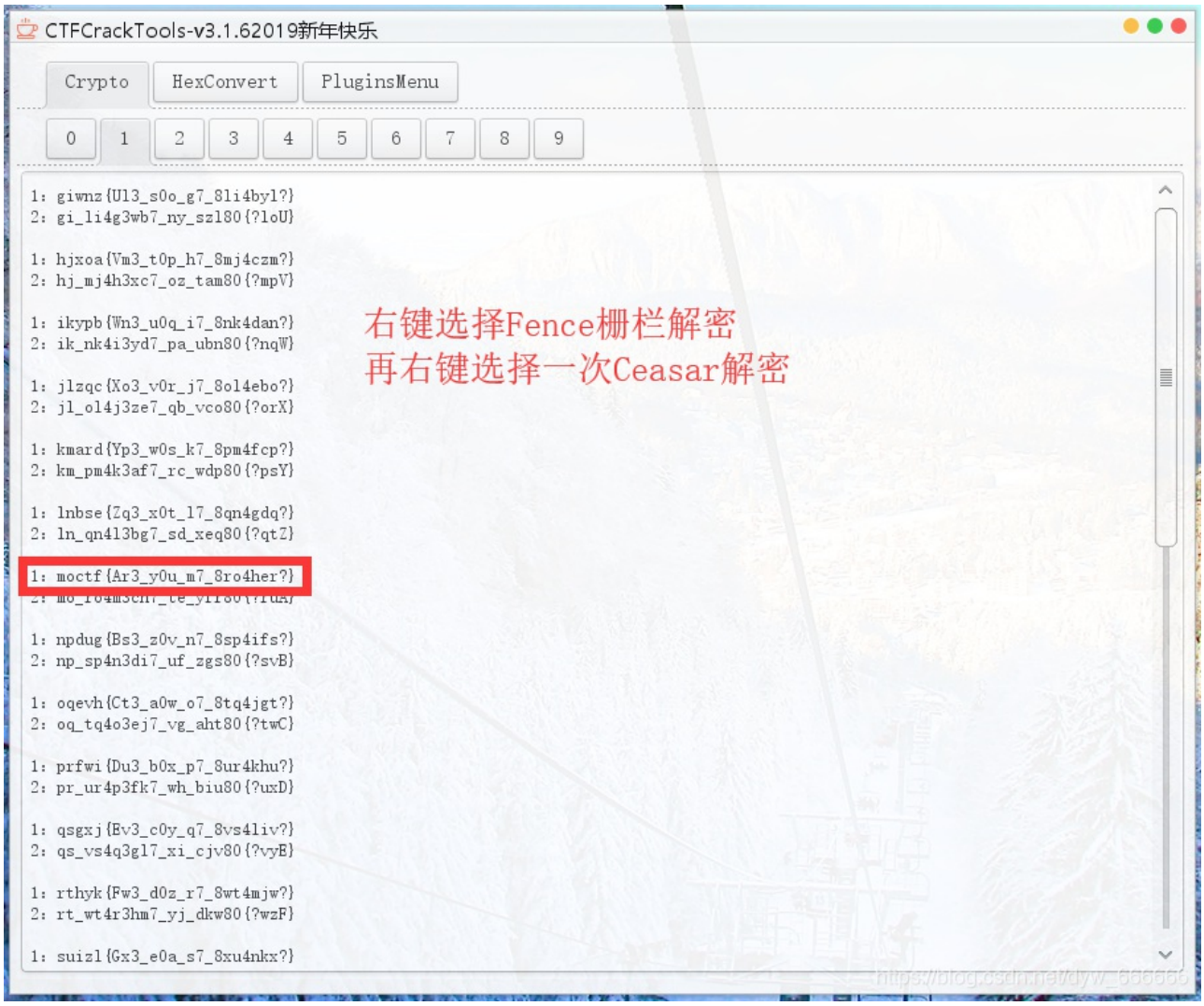




根据图片提示在猜测名字为zhazhahui的时候解开flag.zip得到flag.txt。。。



栅栏密码解密+凯撒密码解密：



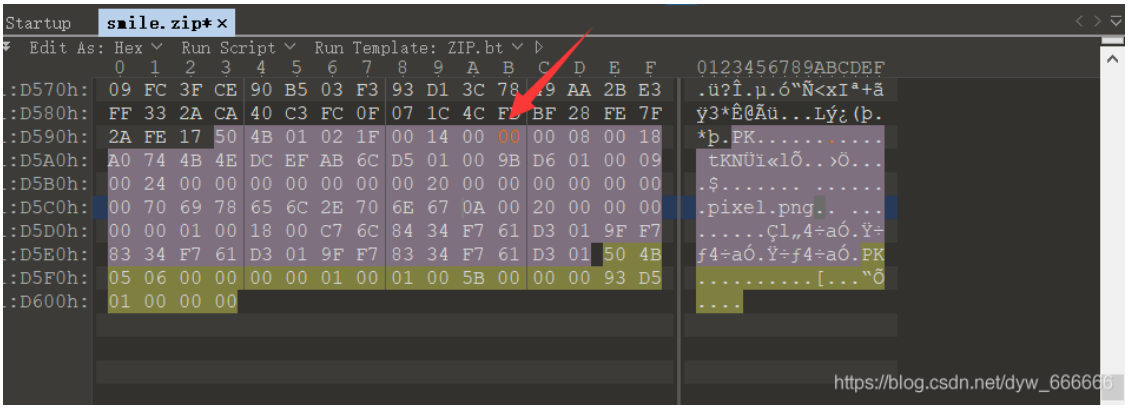
moctf{Ar3_y0u_m7_8ro4her?}

10.百变flag

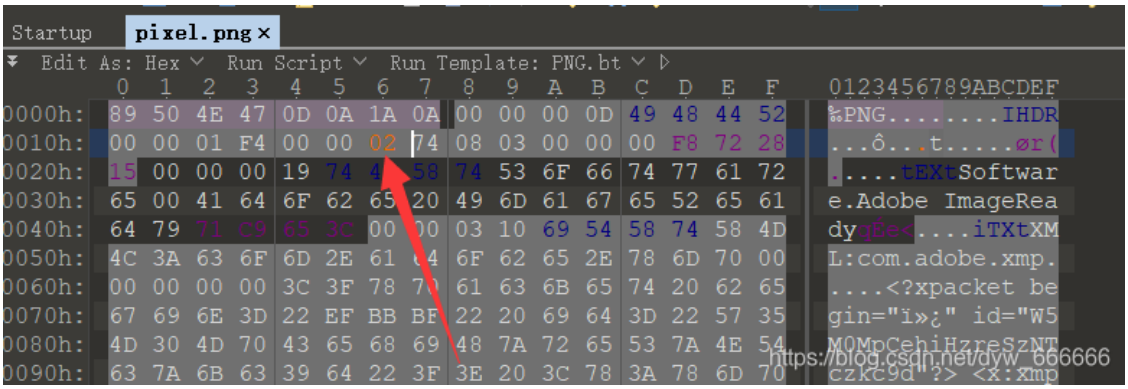
疑似题已崩。

11.蒙娜丽萨的微笑

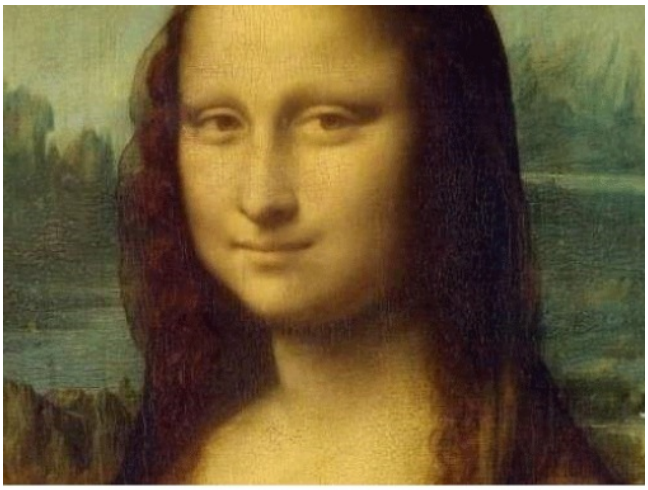
首先破伪加密，把09改为00



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。

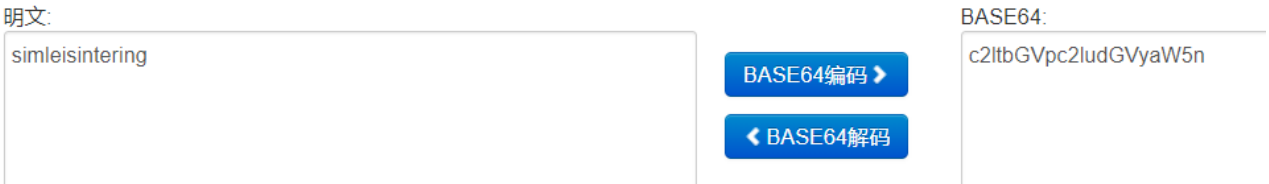


得到一串字符串：

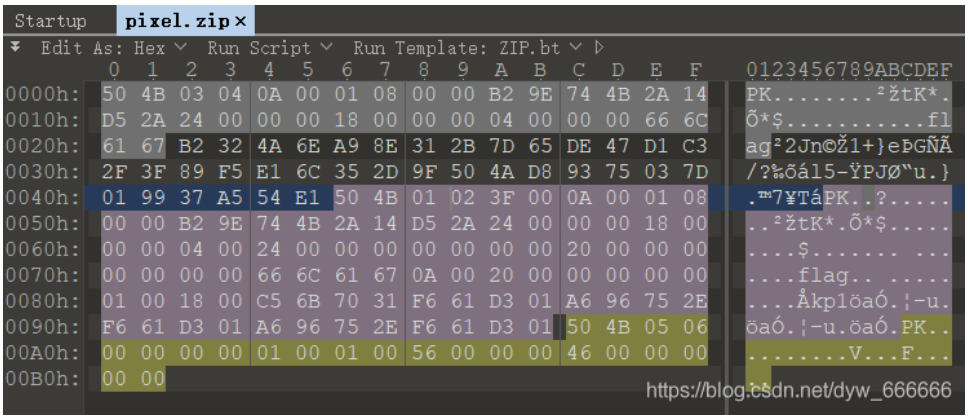


c2ltbGVpc2ludGVyaW5n

使用base64解密。



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。

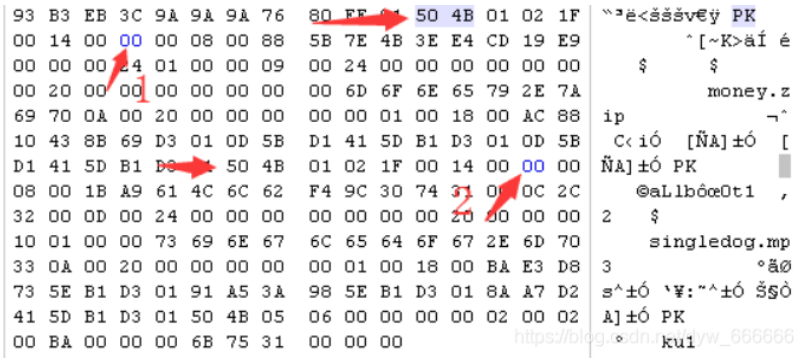


将以504B0304开头部分保存为新文件得到一个新压缩包。发现压缩包中有个flag的文件，打开提示需要输入密码，密码就是之前我们得到的smileisintering，输入后使用记事本打开得到flag。

moctf{lnt3resting_piXe1}

12.李华的双十一

解压发现有伪加密、修改09为00。。。

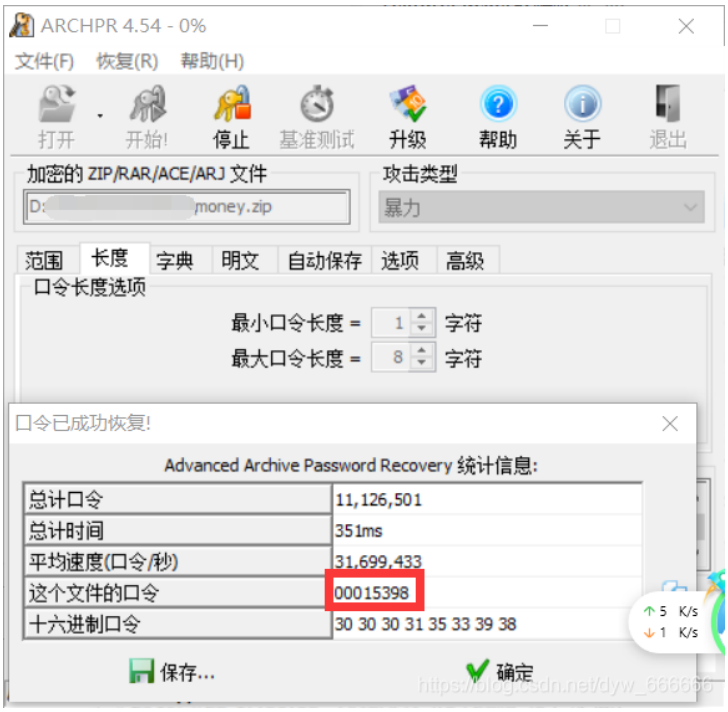


但kali对伪加密其实可以直接提取。。。

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。。。



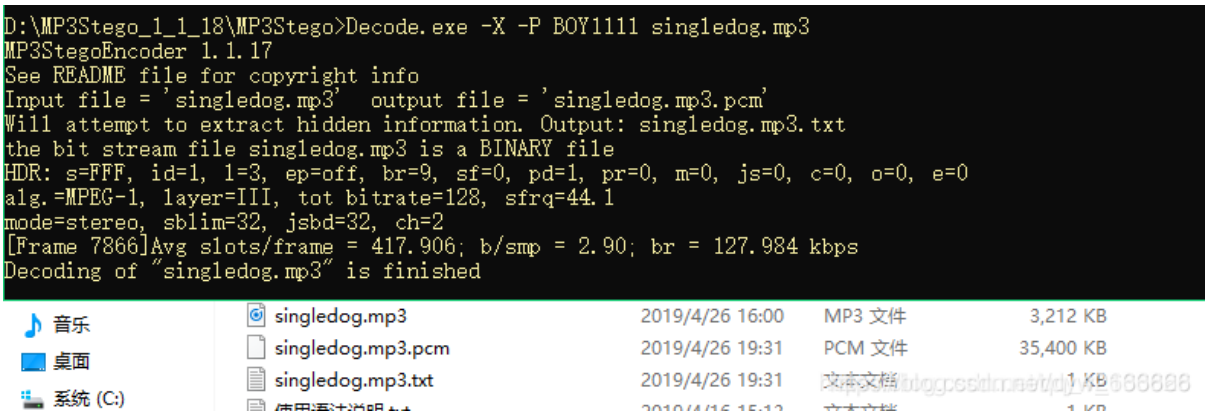
解密money.zip，并打开里面得文件，在文件的最底部，即：

```
-... --- -.-- .---- .---- .---- .----
```

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：



> **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。

moctf{#S1ngl3_D0g#}