Bugku_Misc部分wp(持续更新中)

原创

FFgege 于 2021-05-21 15:11:29 发布 1177 收藏 5

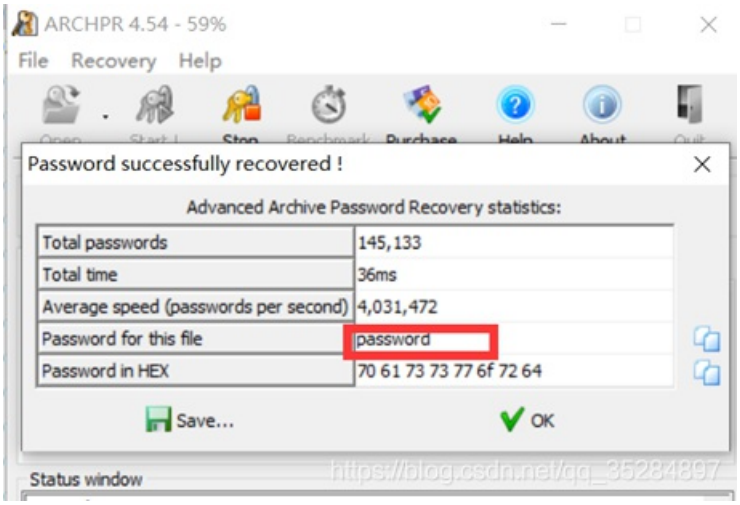
分类专栏： CTF Bugku 文章标签： 信息安全 加密解密

目录：

1.怀疑人生

下载附件得到

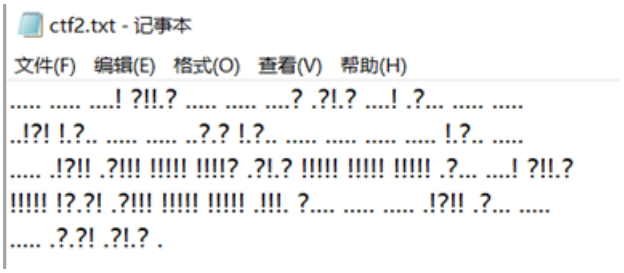
ctf1有密码，暴力破解得password



解压得

Base64解密得\u66\u6c\u61\u67\u7b\u68\u61\u63\u6b\u65\u72
Unicode解密得flag{hacker

ctf2用010Editor打开看到PK，直接修改后缀zip，解压得



ook编码，（ook解密网址https://www.splitbrain.org/services/ook）
解密得3oD54e （鬼知道是base58编码https://www.jisuan.mobi/pbHzbBHbzHB6uSJx.html）
解码得misc

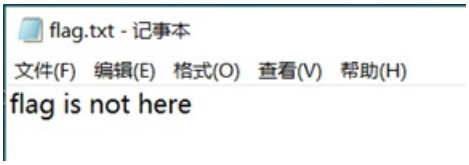
ctf3用二维码解码器解码得到12580}

在这里插入图片描述

得到flag

2. 一个普通的压缩包

下载得到flag.rar，解压得flag.txt



同时报png文件头损坏

在010Editor中修复，修改A8 3C后得7A为74

> HEAD_CRC 2 bytes CRC of total block or block part png为0xA8
> 0x3C
> 整个块或者块某个部分的CRC（根据块类型而有不同） HEAD_TYPE 1 byte Block type
> png为0x74
> 块类型【译者注：也可以理解为块头部类型，因为不同的块对应不同的块头部。后文也经常混淆这两种概念。】 HEAD_FLAGS 2 bytes Block flags
> 块标志 HEAD_SIZE 2 bytes Block size
> 块大小【译者注：本文中和块头部大小的概念一直混淆。后文中当遇到标志块、结尾块等只有头部的块时，也可理解为块头部大小】
> ADD_SIZE
> 4 bytes Optional field - added block size
> 添加块的大小（这是一个可选域）

解压得secret.png文件
打开之后空白，放在010Editor中发现是gif文件，修改后缀.gif，打开之后仍是空白，放在Stegsolve中试试，发现可以看到一半二维码

缺少一半怎么办，因为是gif文件，用动态图分解软件分解gif后得到两个bmp文件，放在Stegsolve后得到
在这里插入图片描述

将二维码拼接在一起后，发现少东西，仍然扫不出来

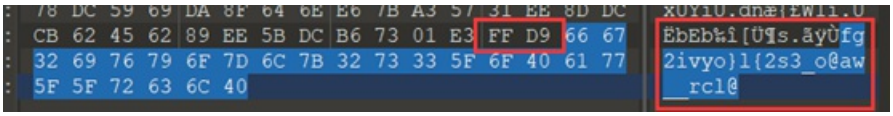
然后运用神奇得剪切拼贴技术，得到完整得二维码

扫码得到flag

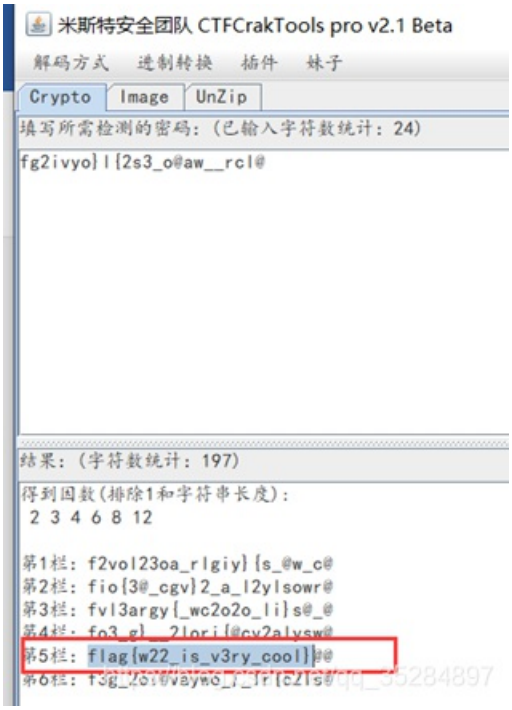
3. 白哥的鸽子

下载得到jpg文件，在010Editor打开

Jpg文件头FF D8 FF 文件尾FF D9

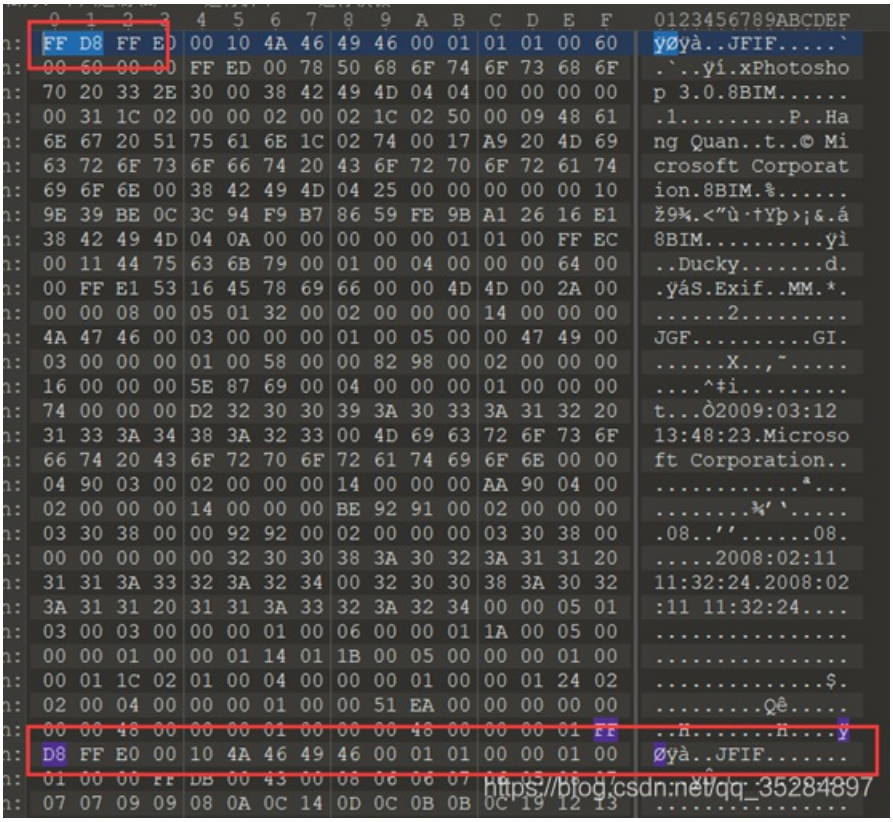


发现尾部多了一串字符串，
分析 fg2ivyo}l{2s3_o@aw__rcl@ 感觉flag、{}等信息都在此字符串中，因此段断定是栅栏密码，解密得flag

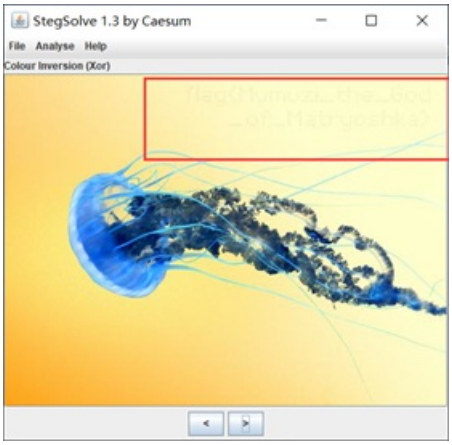


4.简单套娃

下载得到Jellyfish.jpg，扔到010Editor发现有两个jpg文件头



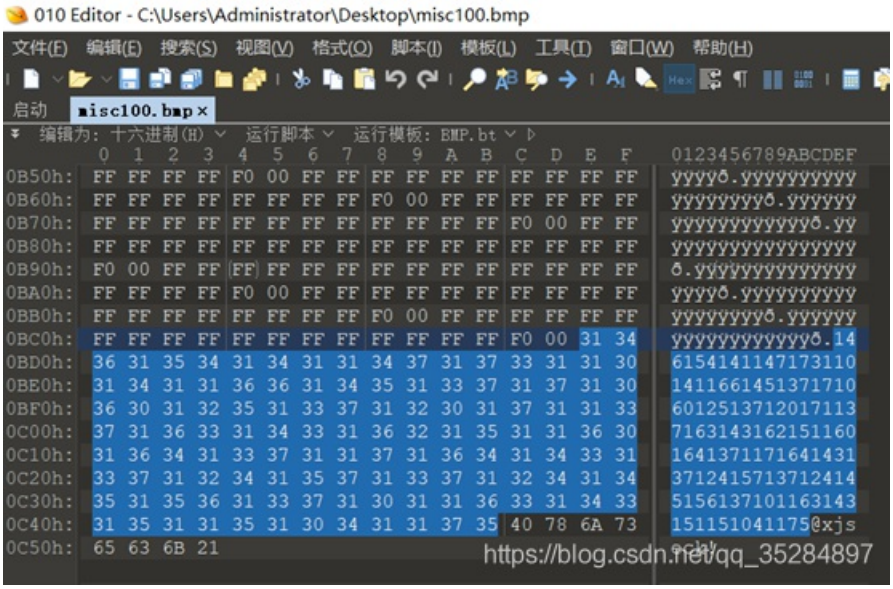
将第一个头删除之后，另存为新图片，放在StegSolve跑一下得到flag



5.普通的二维码

下载附件得到misc100.bmp图片数据

扫码发现没有什么有用信息
用010Editor打开分析，发现文件最后有一串数字



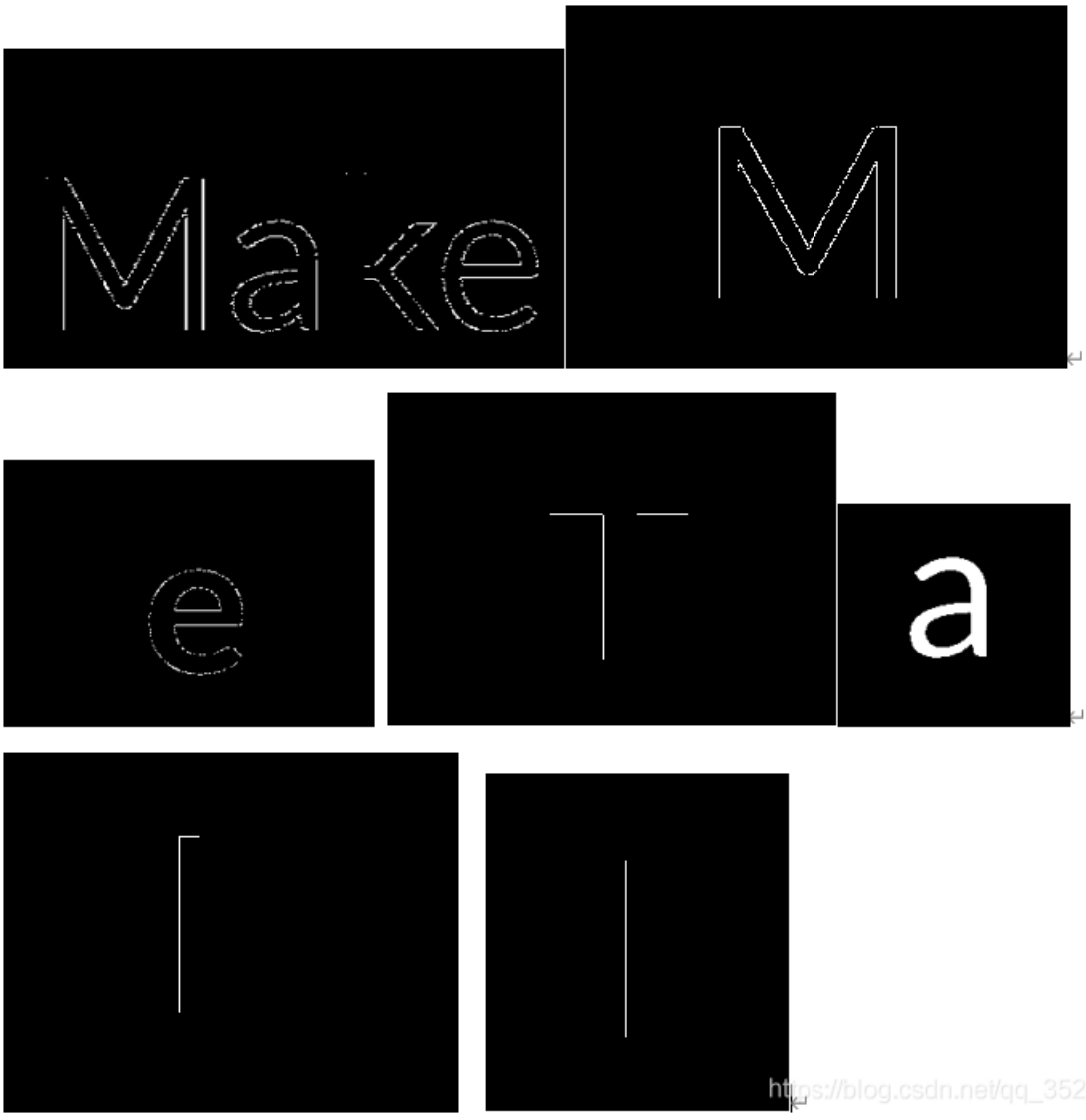
最大数字不超过8，猜测是8进制数据，可能就是flag所在。
写个脚本跑一下（8进制→10进制→字符串，注意3位一组，2位一组尝试后会乱码）得到flag

附上代码

```
f = open('./8进制数据.txt')
list = []
while True:           #将8进制数据3位一组，存储在列表list中
    k = f.read(3)
    if k:
        list.append(k)
    else:
        break
f.close()
for i in list:           #遍历列表
    num = '0o' + i        #取出8进制数据
    num = int(num, 8)     #8进制转为10进制
    num = chr(num)        #10进制转为字符串
    print(num, end='')
```

6.color

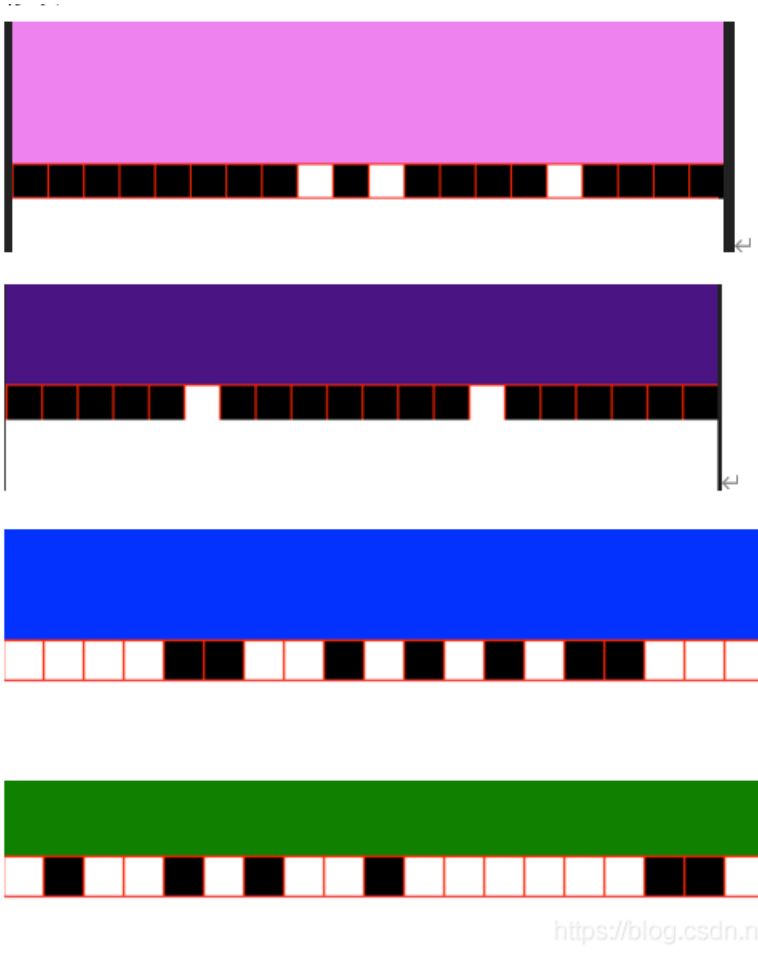
下载附件，得到color.zip，解压得到7张图片。颜色这么多，放在Stegsolve跑一下，得到如下：

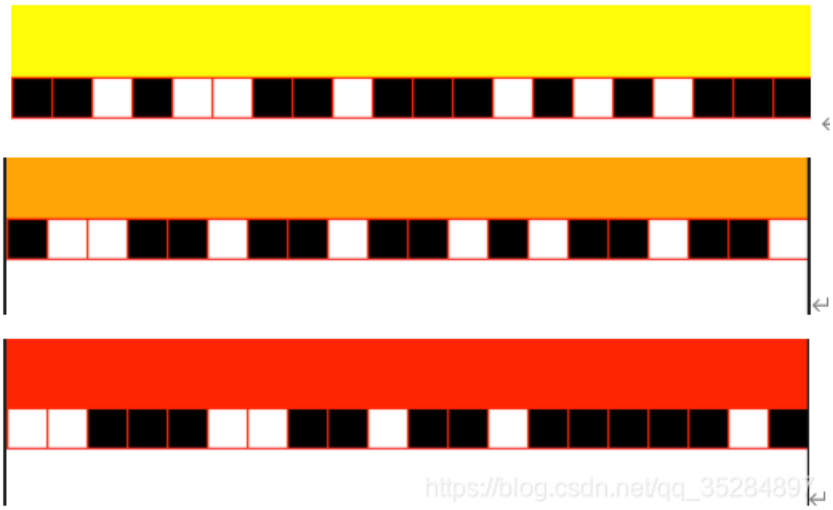


组合起来即为 Make Me Tall （让我变高）
那就放在010Editor，参考png图像文件中文件头数据块（IDER）的各字段含义，修改图片高度

十六进制值	描　述
00 00 00 0D	文件头的数据长度，00 00 00 0D =13
49 48 44 52	数据块类型标志，49 48 44 52的ASCII值等于IHDR
00 00 00 C8	图像的宽度，00 00 00 C8 = 200
00 00 00 96	图像的高度，00 00 00 96 = 150
08	色深，表示2的8次幂等于256色
03	03表示索引图像
00	00表示使用Deflate压缩编码压缩图像数据
00	00表示为将来使用更好的压缩方法预留
00	00表示非隔行扫描
AC 02 37 2B	AC 02 37 2B表示CRC

修改后如下：





猜测可能是二进制数据，令黑块为1，白块为0，得到如下二进制数据

```
11111111010111101111
11111011111110111111
00001100101010110001
01001010010000001101
11010011011101010111
10011011011010110110
00111001101101111101
```

根据观察，取每串数字第一位，组合起来“1100110”，根据Ascii表就是f.

写个脚本跑一下

```
p0 = '11111111010111101111'
p1 = '11111011111110111111'
p2 = '00001100101010110001'
p3 = '01001010010000001101'
p4 = '11010011011101010111'
p5 = '10011011011010110110'
p6 = '00111001101101111101'

flag = []
for i in range(20):
    temp = p0[i]+p1[i]+p2[i]+p3[i]+p4[i]+p5[i]+p6[i]
    temp = chr(int(temp,2))
    flag.append(temp)
print (flag)
print (''.join(flag))  #列表转为字符串
```

得到flag

7. 一切有为法如梦幻泡影

先吐槽一句，这个题的压缩包和图片是真的容易迷……但是整体来说不难，且听我慢慢道来。

写在前面：注意文件头和文件尾16进制表示，此题需要多次用到……

JPEG (jpg),	文件头：FFD8FF		文件尾：FF D9
PNG (png),	文件头：89504E47		文件尾：AE 42 60 82
GIF (gif),	文件头：47494638		文件尾：00 3B
	ZIP Archive (zip),	文件头：504B0304	
文件尾：50 4B			

下载附件“一切有为法如梦幻泡影.zip“

1. 解压得到“《察》.zip”（加密压缩包）和”Zero.png”，

将“Zero.png”丢在010Editor分析一下，发现不是文件尾不是AE 42 60 82，

搜索找到png文件尾，删除png文件部分，剩余部分开头为50 4B，另存为zip文件“第1个隐藏压缩包.zip”，解压得“问.png”

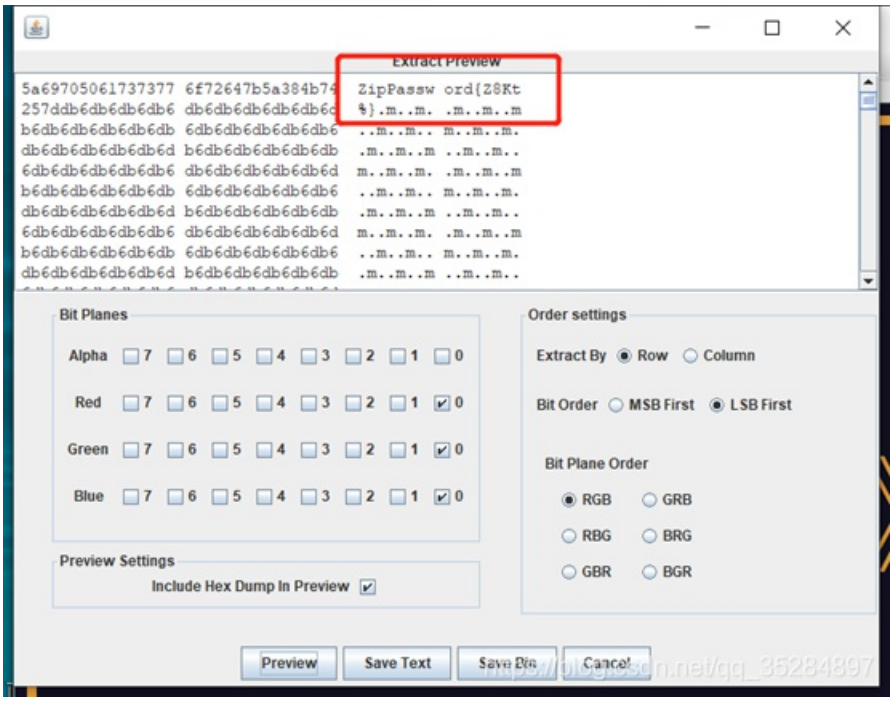
2. 将“问.png” 在010Editor分析一下，一切正常，考虑怎样解开“《察》.zip”（加密压缩包），既然没有提示，暴力破解试一下。

得到密码42，解压得“《探》.zip”（加密压缩包）和“one.png”,将“one.png” 丢在010Editor分析一下，同上可得“第2个隐藏压缩包.zip”，解压得“感.png”

3. 同样套路010分析“感.png”，一切正常，暴力破解“《探》.zip”（加密压缩包）和伪加密也无果。

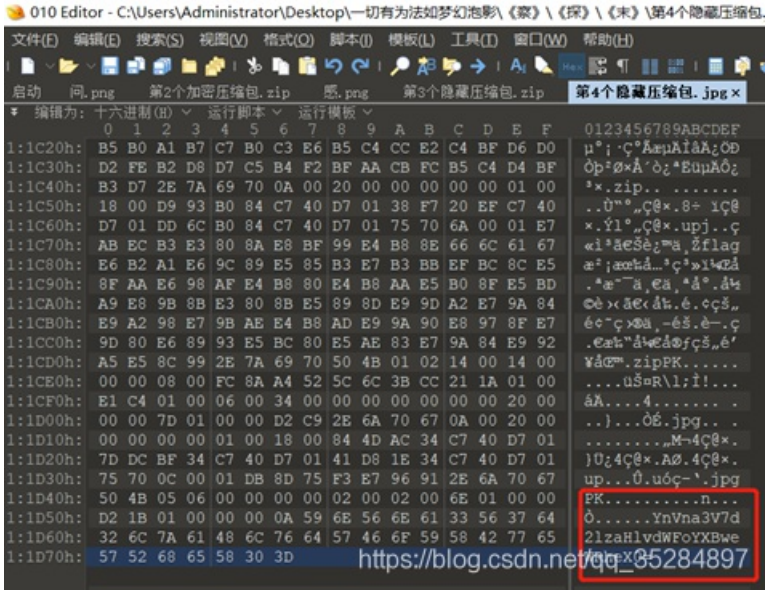
重新考虑“感.png”，应该是图像隐写。尝试Stegsolve分析，png图像尝试Data Extract提取，

仍然无果。猜测可能“感.png”无用，还有“one.png”没有用，继续尝试Stegsolve分析，png图像尝试Data Extract提取，这次得到zippassword{Z8Kt%}。解压“《探》.zip”（加密压缩包）得，“《末》.zip”，“Tow.jpg”，“Tow.mp3”



“Tow.jpg”010分析，同样套路得到“第3个隐藏压缩包.zip”，解压得到“思.jpg”。分析了一下好像没有什么用。
转过头处理“Tow.mp3”，听了一下，不太好听。用audacity打开，也没有发现摩斯密码。看一下频谱图，得到一串字符串“jBL7@”,就是“《末》.zip”的密码。

解压“《末》.zip”得到“Three.jpg”，用010分析一下，同样的套路得到“第4个隐藏压缩包.zip”。注意，010打开的“Three.jpg”最后，藏了一串看起来像base64加密的字符串“YnVna3V7d2lzaHlvdWFoYXBweWRheX0=”



解码base64得flag
6. 其实题目到这里就结束了，作者给各位师傅留了个彩蛋，解压“第4个隐藏压缩包.zip”，得到“《这与flag没有关系，只是一个小彩蛋》前面的题目中隐藏着打开它的钥匙.zip”和“疑.jpg”。
作者给师傅们留了一个彩蛋~~~，password就在前面。也许你已经看到了，祝好运。
hint：……
彩蛋密码就是前面图片中下面的点转换为数字。

8.这是一张单纯的图片

010分析得Unicode编码，解码得flag

9. 又一张图片，还单纯吗

Foremost提取得falg

falg{NSCTF_e6532a34928a3d1dadd0b049d5a3cc57}

10. 眼见非实

下载附件得“眼见非实.docx”，010分析发现是压缩包，更改后缀解压。在document.xml中发现flag

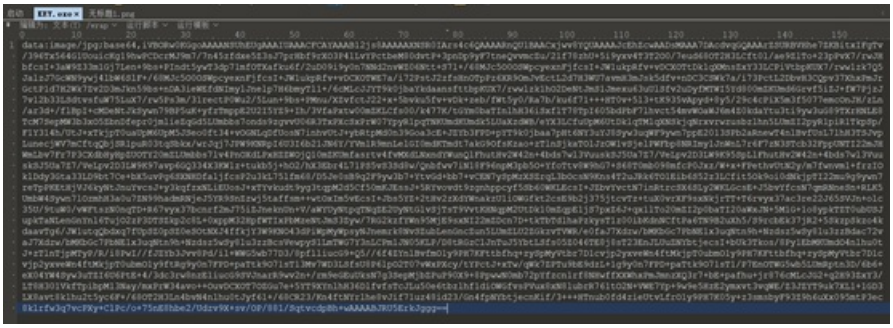
11. 啊哒

ada.jpg用010分析，发现后面又压缩包。分离出压缩包，解压需要密码。可以尝试一下爆破。解压密码在ada.jpg文件的属性里，照相机型号是16进制，转为字符串即为密码sdnisc_2018。

解压得flag

12. 多种方法解决

下载附件得KEY.exe，010分析发现有一串base64。



Base64转字符串发现乱码。根据题目提示，尝试base64转图片（https://tool.jisuapi.com/base642pic.html）

扫码得flag

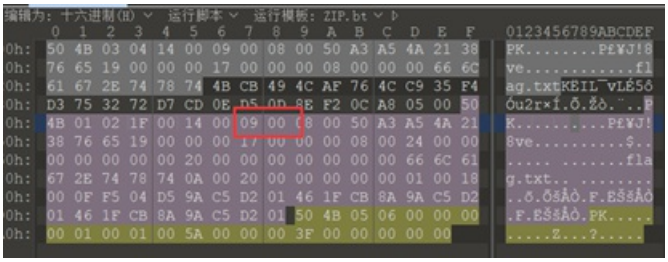
12. ok

下载附件解ook编码得flag
Ook解码地址https://www.splitbrain.org/services/ook

13.猜

百度搜图，

14. zip伪加密



09 00 改为 00 00

或者使用zip伪加密修复工具，ZipCenOp.jar

15.三色绘恋

下载附件得到“三色绘恋.jpg”，010分析发现后面藏有zip压缩包。分离出压缩包解压发现没有加密，尝试发现不是伪加密，爆破也无果。继续分析jpg文件寻找解压密码，010分析发现，“三色绘恋.jpg”16进制中存在两个文件头，FF D8 FF ，删掉一个，重新保存新的图片，得到解密密码key，解压得flag

16. 不简单的压缩包

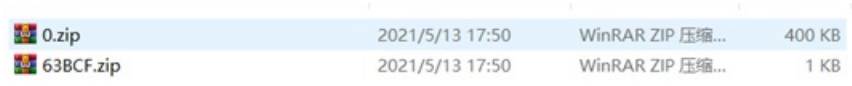
    下载得到加密压缩包，里面藏有txt文件

010分析，发现似乎还隐藏了另外一个压缩包。

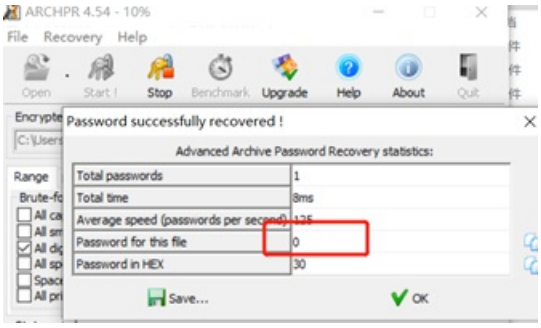

```
D:\python27\Scripts>python2 binwalk file.zip

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, encrypted at least v2.0 to extract, compressed size: 408361, uncompresse
d size: 408284, name: flag.swf
408505        0x63BB9         End of Zip archive, footer length: 22
408527        0x63BCF         Zip archive data, encrypted at least v2.0 to extract, compressed size: 43, uncompressed si
ze: 26, name: tingshuo.txt
408722        0x63C92         End of Zip archive, footer length: 22
```

用binwalk也可以发现两个压缩包，binwalk分离一下(python2 binwalk -e file.zip)，得到两个加密压缩包



两个都加密，先解决1KB简单的，暴力破解一下，得到密码“0” ……我傻了

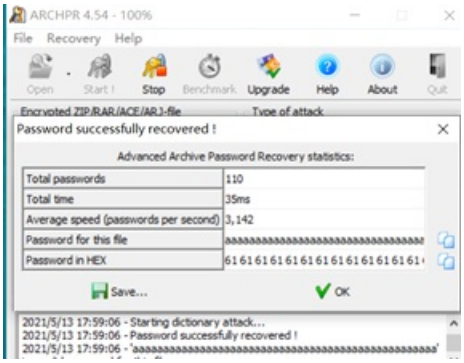


解压得tingshuo.txt，发现是日语，翻译一下

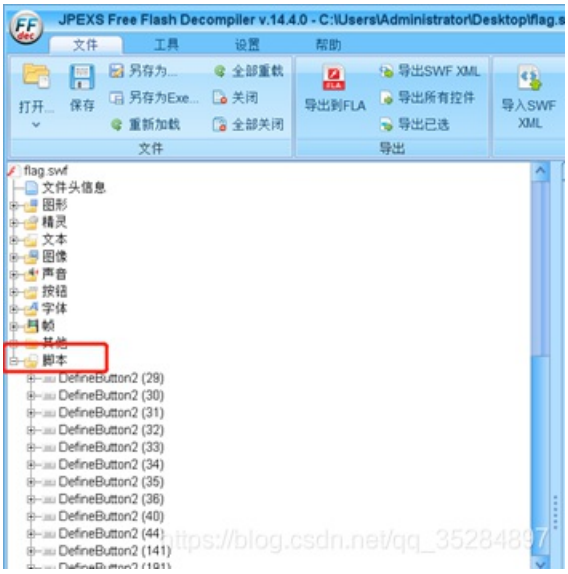
50位的密码……，组合的话破解难度太大，先试试同样的，搞个字典破解一下，脚本如下

```
li = ['0','1','2','3','4','5','6','7','8','9','a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q
','r','s','t','u','v','w','x','y','z']
for i in range(0,len(li)):
    c = li[i]*50
    print(c)
```

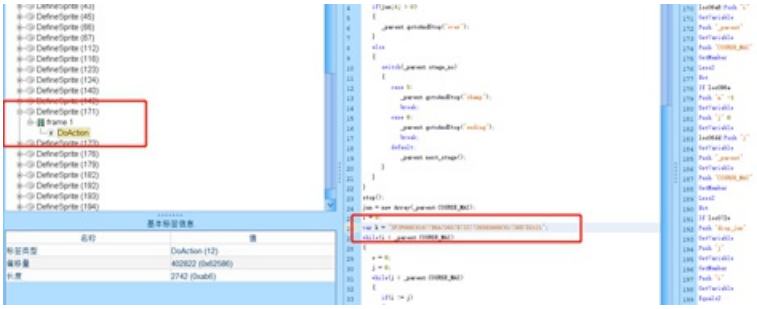
结果存在txt文档里，记得修改后缀位dic
字典破解一下，得到密码50个a ……



解压得flag.swf
swf文件，用JPEXSFreeFlashDecompiler(反编译swf工具)，尝试一下



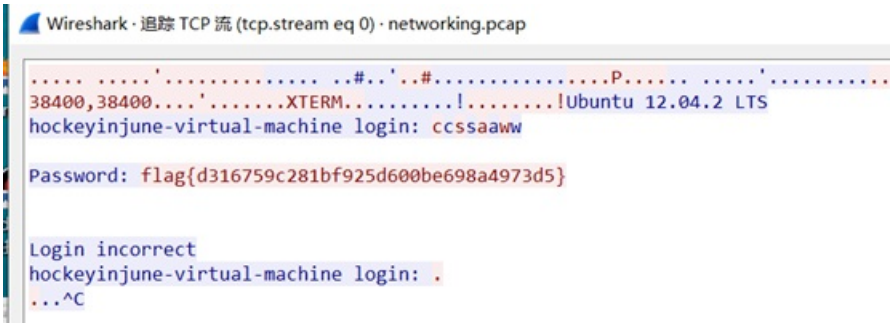
在脚本中一个一个过，最终在171处发现一串16进制代码



转为字符串，得到flag

16.telnet

Wireshark打开，右键追踪TCP流，得到flag

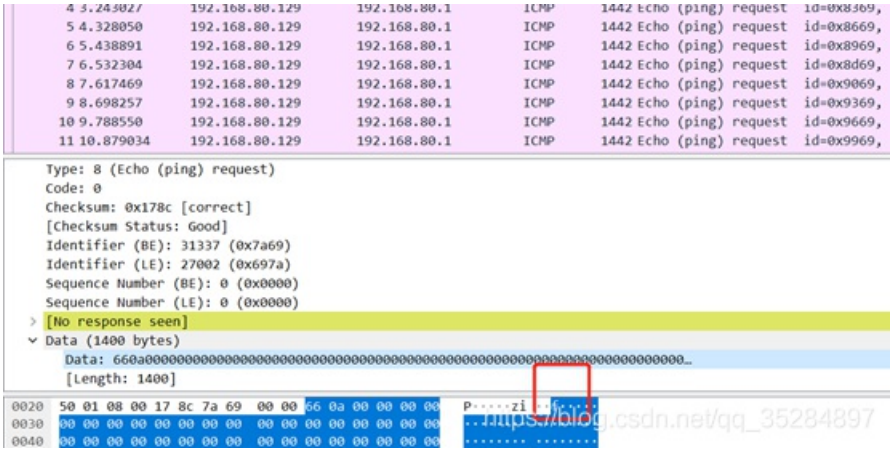


17.闪的好快

动态图分解https://tu.sioe.cn/gj/fenjie/，扫码得flag

18.ping

用wireshark打开，点击第一个数据包，点击data字段，发现显示f字母，依次点击数据包，拼成flag



19.linux

Linux下的压缩包文件1.tar.gz，解压搜索key得到flag

20.富强民主

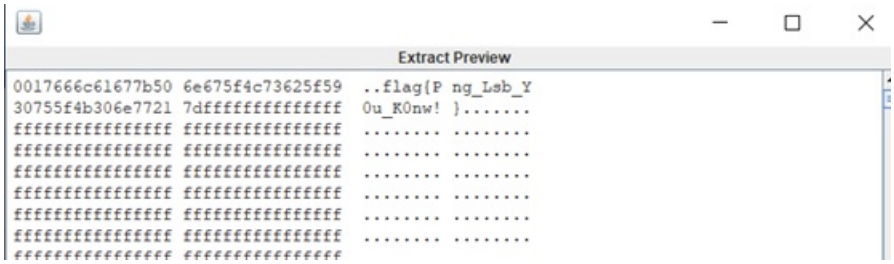
核心价值观编码 http://ctf.ssleye.com/cvencode.html

21.linux2

解压，txt打开，搜索KEY，得到flag

22.乌云邀请码

下载附件得到png图片，010分析无异常，Stegsolve跑一下，打开Stegsolve->Analyse->Data Extract，选取相应颜色通道，更改

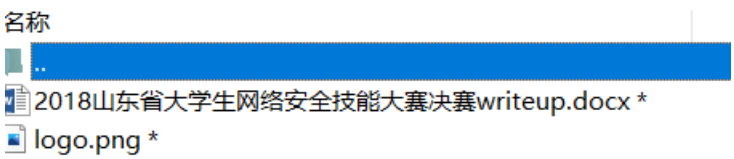


Bit Plane Order，得到flag

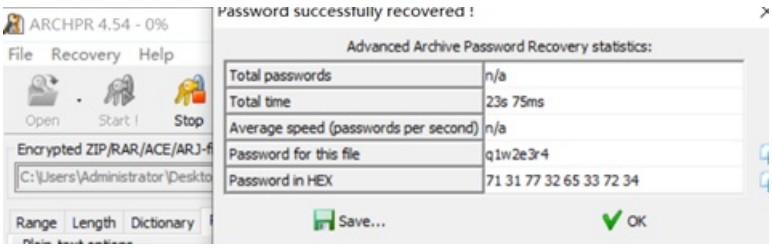
23.神秘的文件

本题很常规

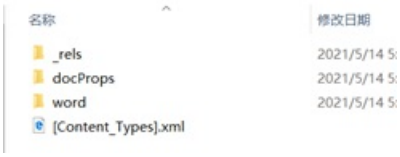
下载附件解压得到flag.zip和logo.png，打开压缩包发现加密，压缩包里也有一个名为logo.png的图片。猜测zip明文攻击。



将logo.png压缩为logo.zip（注意这里要用WinRAR，360压缩尝试不成功，因为压缩算法不一样）
利用ARPHCR明文攻击，得到解压密码q1w2e3r4



2018山东省大学生网络安全技能大赛决赛writeup.doc文件，打开发现问题，010分析发现是zip压缩包，修改后缀解压得



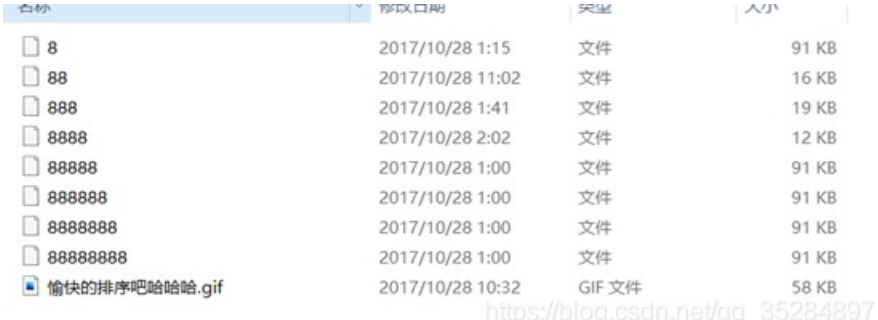
第一反应，打开word文件夹，在document.xml寻找答案

竟然不对,被调戏了……
重新寻找其他文件夹，在docProps中找到flag.txt，打开发现base64加密，解密得flag

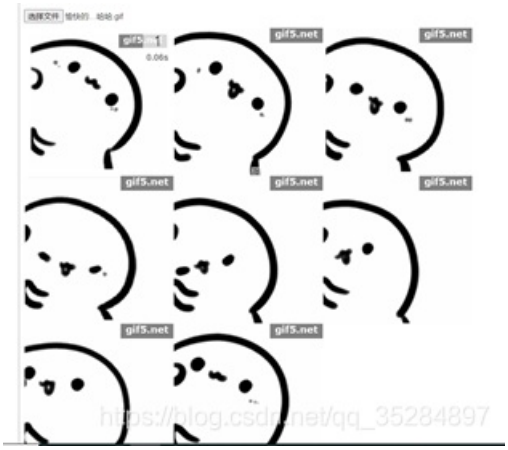
24.爆照

根据flag格式提示，flag应该分三段
下载附件，得到jpg图片

010分析一下，发现隐藏有zip压缩包,binwalk分离出压缩包，解压得



有一个gif动态图，分解一下，得到8张图片，并没有什么信息。



愉快的排序吧……，应该就是那8个88888888888888文件了……
（1）010分析8文件，在末尾发现flag字符串，其他无异常

（2）010分析88文件，发现是jpg图片，加上后缀为88.jpg，得到如下图片

扫码得bilibili，这应该就是flag三段中的第一段
（3）010分析888文件，发现是jpg图片，加上后缀为888.jpg，得到如下图片

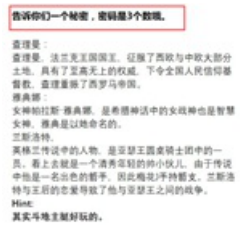
没有发现什么信息……
（4）继续010分析8888文件，发现是jpg图片后隐藏了zip压缩包。加上后缀为8888.jpg，binwalk分离得到压缩包，解压的二维码图片，扫码得panama,这应该是flag的第二段
（5）继续分析88888/888888/8888888/88888888四个文件，都没有发现什么信息，也不是图片
（6）既然88和8888文件出现了有用信息，那么猜测888文件中一定也存在一定信息，且888为jpg图片。最终在888.jpg的属性中发现一串base64加密的字符串，解base64得silisili,flag的第二段拿到
最终按照格式组合起来即得flag

25.隐写3

010修改png图片高度得flag

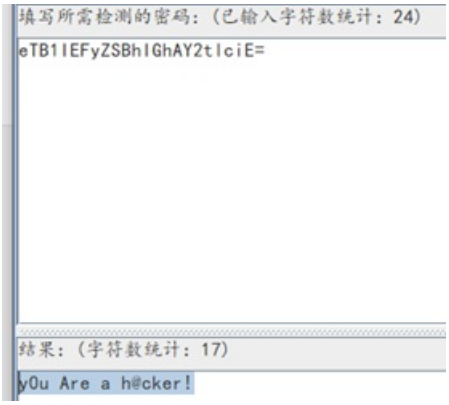
26.隐写2

下载附件得welcome.jpg，010分析发现隐藏有zip压缩包，binwak分离一下，解压得到flag.rar和提示.jpg



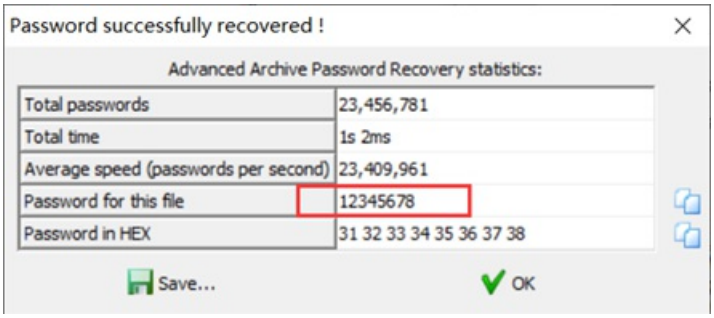
密码是3个数，爆破一下得到password: 871

解压得3.jpg，010分析在最后得到flag： f1@g{eTB1lEFyZSBhlGhAY2tlciE=}
提交不对，内部是base64加密，解密得y0u Are a h@cker!



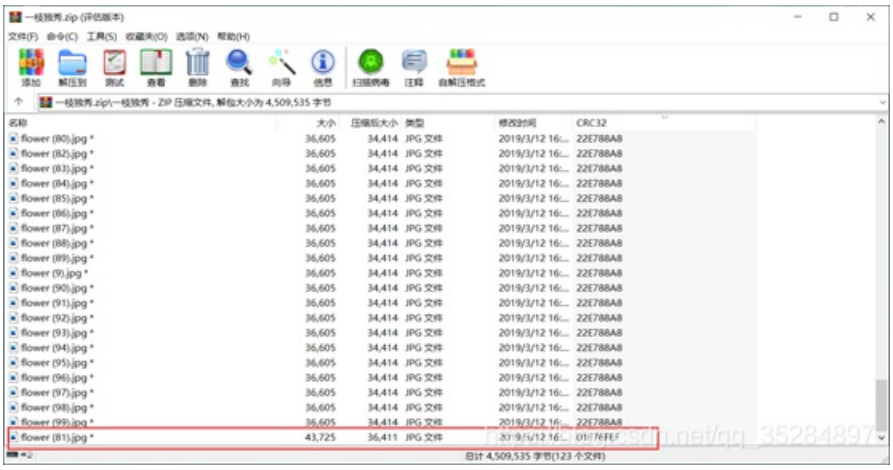
27.一枝独秀

下载附件解压得一张有问题的png图片，010分析一下发现PK，zip压缩包，修改后缀，得到一个加密的压缩包。
暴力破解一下，得到解压密码

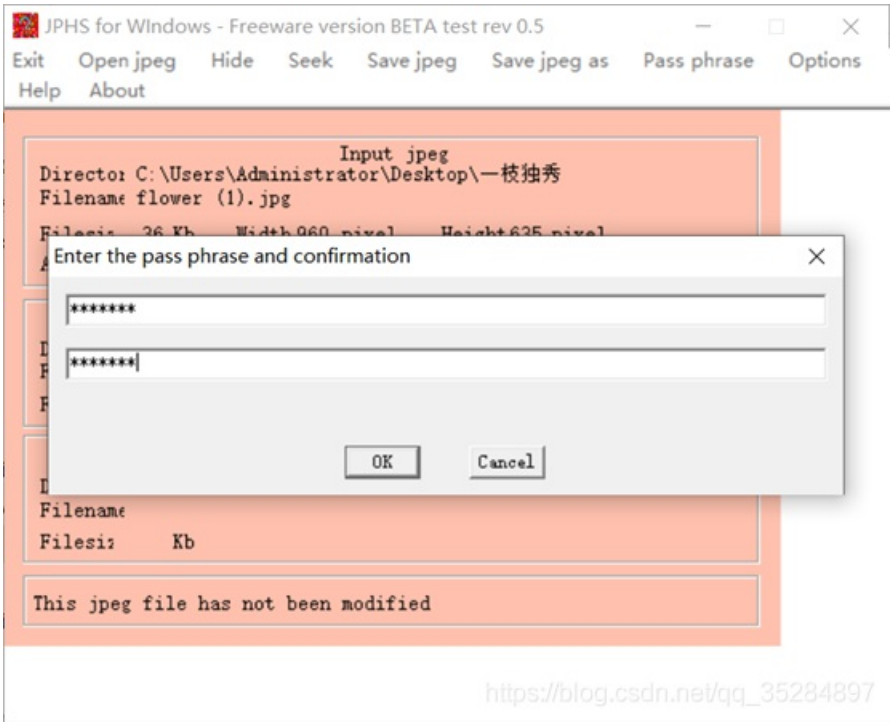


解压得123张flower图片，一模一样.....

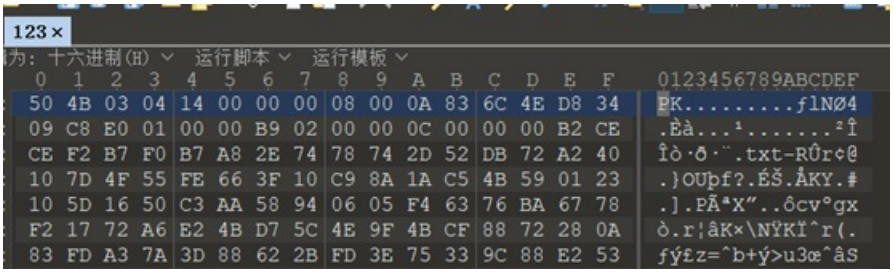
根据经验，解题点应该藏在其中某一张或者几张图片中，接下来寻找图片的不同（如大小等.....）
打开原来的压缩包，比较图片的不同



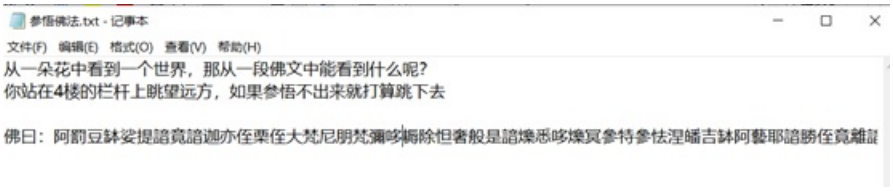
发现了flower(81)的格格不入……，比其他图片要大，且crc32校验码也不同。
把81拿出来，010分析一下，没有发现异常。由于是jpg文件，想到了处理jpg和jpeg文件的神器，Jphs，但是还缺少密码。
用刚刚爆破出来的压缩包密码12345678尝试，发现不对。苦苦寻找，最终在81图片的属性里发现了主题位：flowers，对比一下其他图片文件，没有这个主题，猜测应该是password



用Jphs从成功从81图片中分离出一个文件，命名为123
用010分析一下123文件



zip压缩包……，更改文件后缀，解压得一个参悟佛法.txt文档



佛法……与佛论禅，解密得

得到一串加密字符串，根据文档提示“4楼得栏杆”以及题目提示“翻过四个栅栏即可得到flag”，应该是栅栏密码了，且每组字数应为 4

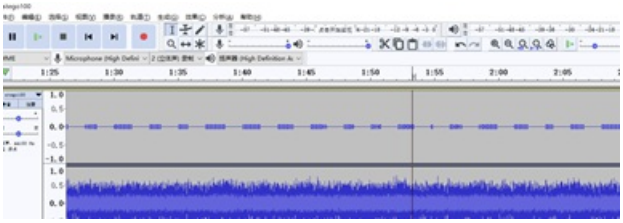
后面Zm开头，应该是base64了，解密得flag
注意：解base64时要把前面得HINT-去掉

28.where is flag

附件得到10个空白的txt,根据题目提示“每个文件都不太一样”
都是空白的有什么不一样呢
010打开分析，发现每个文件的16进制长度不太一样，记录每个16进制长度转Ascii即得flag

29. 听首音乐

Audacity分析



摩斯密码
… -… -.-. ----. …— … -… …- ----. -.-. -… ----- .---- —… —… …-. … …— . -… .---- --… -… --… ----- ----. …— ----. .---- ----. .---- -.-.
解码得flag

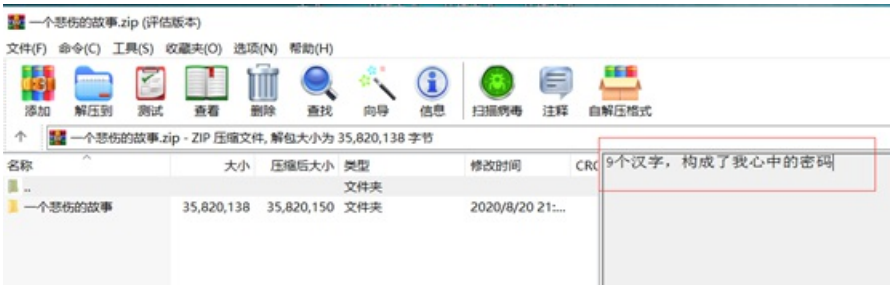
30.where is flag 2

CRC32
... 6275676B
... 757B596F
... 755F6361
... 6E27745F
... 696D6167
... 696E655F
... 7468655F
... 68617070
... 696E6573
... 735F6F66
... 5F686964
... 696E675F
... 7468655F
... 666C6167
... 2121217D

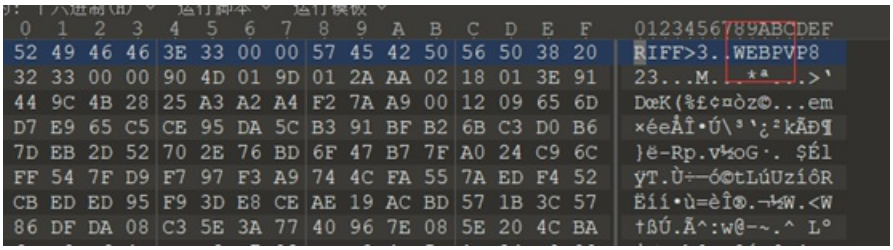
16进制转Ascii

31.悲伤的故事

加密压缩包，



密码应该就在右边这个文件中
“你有看过这个电影吗”刚好9个汉字，尝试发现不对
010分析这个无后缀文件



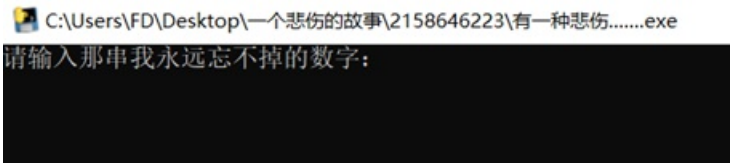
Webp格式文件
修改后缀

这个电影…… 比悲伤更悲伤的故事 9个汉字应该就是密码了
解压得到加密压缩包

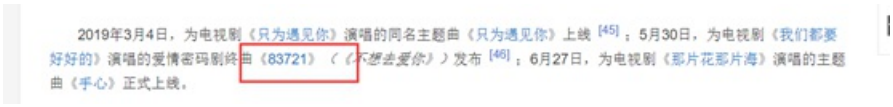
XXyueXXri
XX为加密，yue ri ……是日期
文件名字是一串数字。2158646223
最后发现竟然是一个QQ号

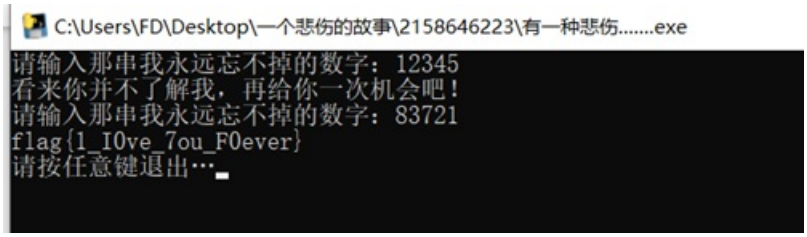
进入空间

7月21日，密码应该就是7yue21ri
解压得



5个数字……
Audacity分析发现不是摩斯密码和频谱图隐写
转换思路
……郭静是谁？





32.where is flag 3

名称	压缩后大小	原始大小	类型	修改日期
fake0.txt*	252	243	文本文档	2021/5/21 8:15:12
fake1.txt*	100	22	文本文档	2021/5/21 8:15:19
fake2.txt*	220	138	文本文档	2021/5/21 8:15:00
fake3.txt*	360	327	文本文档	2021/5/21 8:15:05
fake4.txt*	412	385	文本文档	2021/5/21 8:15:15
fake5.txt*	260	195	文本文档	2021/5/21 8:14:25
fake6.txt*	360	299	文本文档	2021/5/21 8:15:08
fake7.txt*	320	260	文本文档	2021/5/21 8:15:16
fake8.txt*	360	321	文本文档	2021/5/21 8:14:10
fake9.txt*	432	413	文本文档	2021/5/21 8:14:10
fakf0.txt*	284	217	文本文档	2021/5/21 8:14:16
fakf1.txt*	468	477	文本文档	2021/5/21 8:14:15
fakf2.txt*	164	88	文本文档	2021/5/21 8:14:09
fakf3.txt*	252	243	文本文档	2021/5/21 8:14:10
fakf4.txt*	224	160	文本文档	2021/5/21 8:14:11
fakf5.txt*	168	127	文本文档	2021/5/21 8:14:08
fakf6.txt*	520	861	文本文档	2021/5/21 8:14:12
fakf7.txt*	140	63	文本文档	2021/5/21 8:14:11
flag is here .png*	1,767,872	1,771,459	PNG 文件	2021/5/21 9:09:03

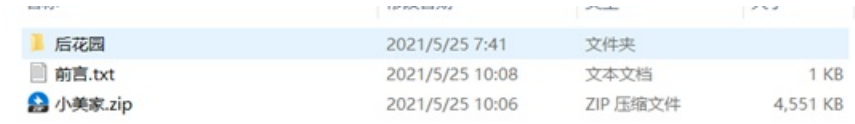
时间转时间戳

https://www.beijing-time.org/shijianchuo/

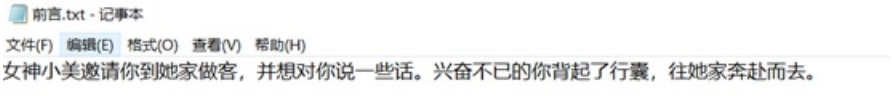
最后3位转Ascii即可得pwdisAlt2287123043

解压的flag

33.小美的秘密



后花园	2021/5/25 7:41	文件夹	
前言.txt	2021/5/25 10:08	文本文档	1 KB
小美家.zip	2021/5/25 10:06	ZIP 压缩文件	4,551 KB



但是小美正好出去了，你被堵在了家门口，作为杂项绝活哥的你，相信很快就能找到小美家的钥匙。

hint:去garden看看?

hint:小美家.zip 的密钥在garden里

后花园里得到一张图片

```
D:\python27\Scripts>python2 binwalk fence.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
79054         0x134CE         JPEG image data, JFIF standard 1.01
79084         0x134EC         TIFF image data, big-endian, offset of first image directory: 8
```

binwalk分析，发现隐藏有图片，foremost提取得到jpg图像

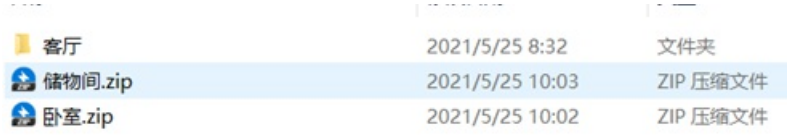
修改图片高度得到（**注意：jpg文件高度更改搜索FF C0，后面的即为宽高**）

`K9e8y7I}s{$key2`

字符串中含有Key,考虑栅栏密码，fence.jpg 图像中由11根栅栏，即为栅栏加密栏数

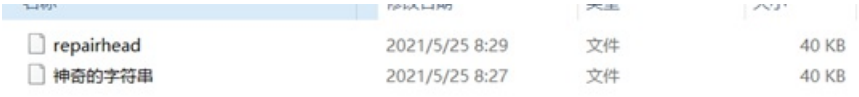
```
K9e8y7I}s{$key2
```

`KeyIs{$key2987}`
即为小美家.zip密钥



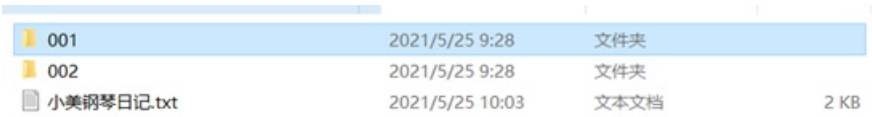
储物间和卧室为加密文件。在客厅寻找密钥

两张jpg图像为迷惑，无用
垃圾桶中，

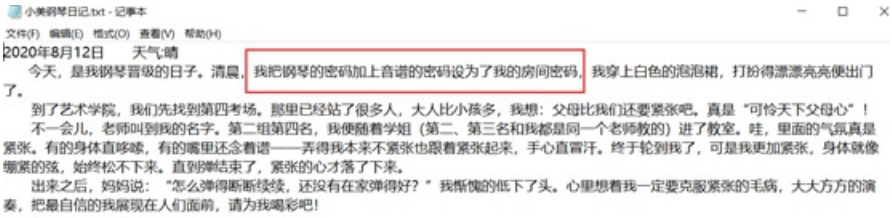


010分析两个文件，发现是被损坏的jpg文件，修复文件头，更改后缀，恢复jpg文件
将两张图像拼接在一起

得到**`BugKu233`,即为储物间的密钥



打开小美钢琴日记


小美钢琴日记.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

2020年8月12日　天气:晴

今天，是我钢琴晋级的日子。清晨，我把钢琴的密码加上音谱的密码设为了我的房间密码，我穿上白色的泡泡裙，打扮得漂漂亮亮便出门了。

到了艺术学院，我们先找到第四考场。那里已经站了很多人，大人比小孩多，我想：父母比我们还要紧张吧。真是“可怜天下父母心”！

不一会儿，老师叫到我的名字。第二组第四名，我便随着学姐（第二、第三名和我都是同一个老师教的）进了教室。哇，里面的气氛真是紧张。有的身体直哆嗦，有的嘴里还念着谱——弄得我本来不紧张也跟着紧张起来，手心直冒汗。终于轮到我了，可是我更加紧张，身体就像绷紧的弦，始终松不下来。直到弹结束了，紧张的心才落了下来。

出来之后，妈妈说：“怎么弹得断断续续，还没有在家弹得好？”我惭愧的低下了头。心里想着我一定要克服紧张的毛病，大大方方的演奏，把最自信的我展现在人们面前，请为我喝彩吧！

卧室的密钥是：`钢琴的密码加上音谱的密码`

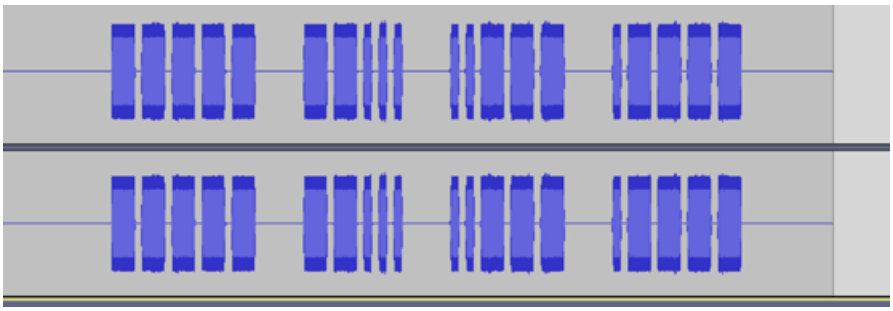
010分析001文件夹piano2.jpg，发现文件尾藏有rar文件

分离出rar文件，解压得一张二维码图像

扫码得 `roomkey`

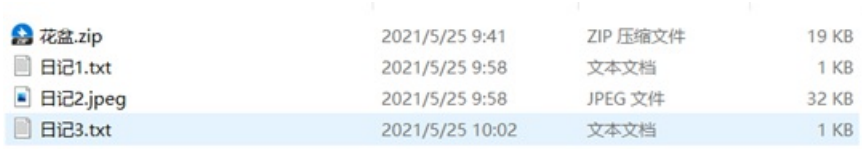
002文件夹中是音频文件

Audacity分析，发现摩斯密码



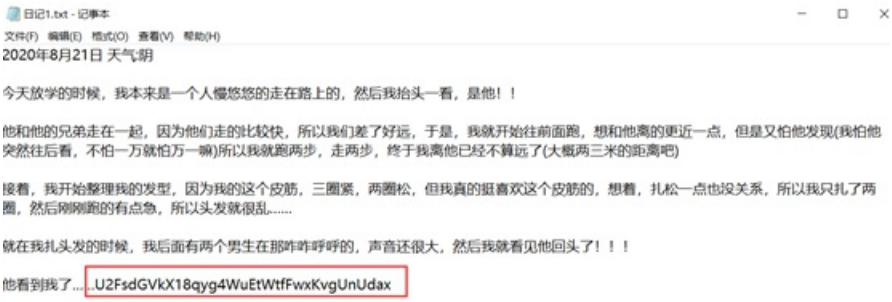
`----- --... ..--- .----` 解密得0721

组合起来，卧室的密钥为 `roomkey0721`



花盆.zip	2021/5/25 9:41	ZIP 压缩文件	19 KB
日记1.txt	2021/5/25 9:58	文本文档	1 KB
日记2.jpeg	2021/5/25 9:58	JPEG 文件	32 KB
日记3.txt	2021/5/25 10:02	文本文档	1 KB

日记1：


日记1.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

2020年8月21日 天气:阴

今天放学的时候，我本来是一个人慢悠悠的走在路上的，然后我抬头一看，是他！！

他和他的兄弟走在一起，因为他们走的比较快，所以我们差了好远，于是，我就开始往前面跑，想和他离的更近一点，但是又怕他发现(我怕他突然往后看，不怕一万就怕万一嘛)所以我就跑两步，走两步，终于我离他已经不算远了(大概两三米的距离吧)

接着，我开始整理我的发型，因为我的这个皮筋，三圈紧，两圈松，但我真的挺喜欢这个皮筋的，想着，扎松一点也没关系，所以我只扎了两圈，然后刚刚跑的有点急，所以头发就很乱.....

就在我扎头发的时候，我后面有两个男生在那咋咋呼呼的，声音还很大，然后我就看见他回头了！！！

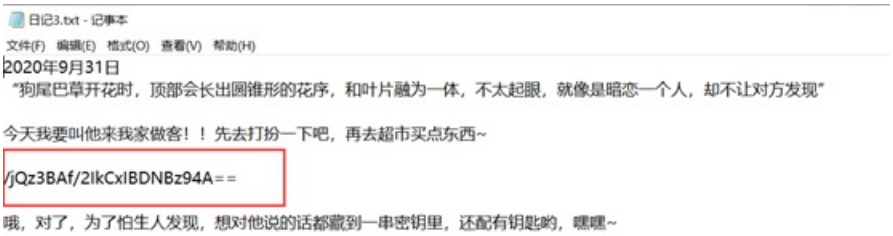
他看到我了.....U2FsdGVkX18qyg4WuEtWtfFwxKvgUnUdax

日记2：

无字天书

查看EXIF信息得到 `/b4f2dLgl30Tqg4Q/TOhaucaZpwqP`

日记3：



组合起来得到

`U2FsdGVkX18qyg4WuEtWtfFwxKvgUnUdax/b4f2dLgl30Tqg4Q/TOhaucaZpwqP/jQz3BAf/2IkCxIBDNBz94A==`

U2F开头，猜测AES加密，但还缺少密钥

想到还有花盆.zip还没用

分析发现是伪加密

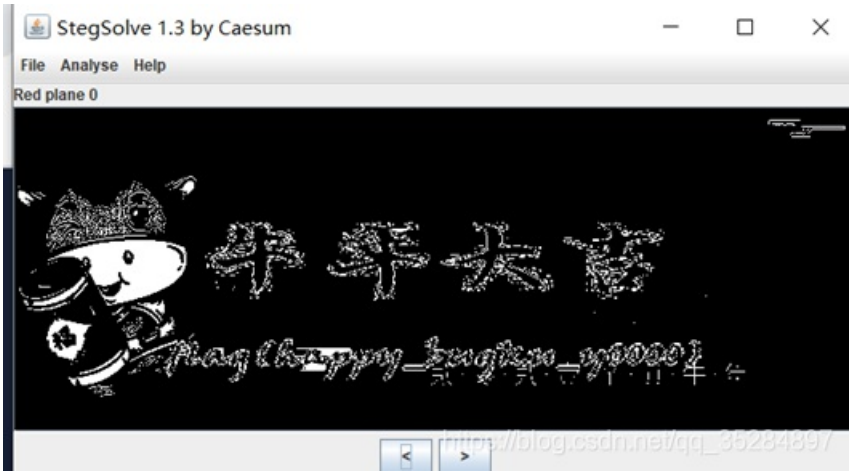
解密得

修改图片高度

得到密钥 `misc`
AES解密得flag

34.低位的色彩

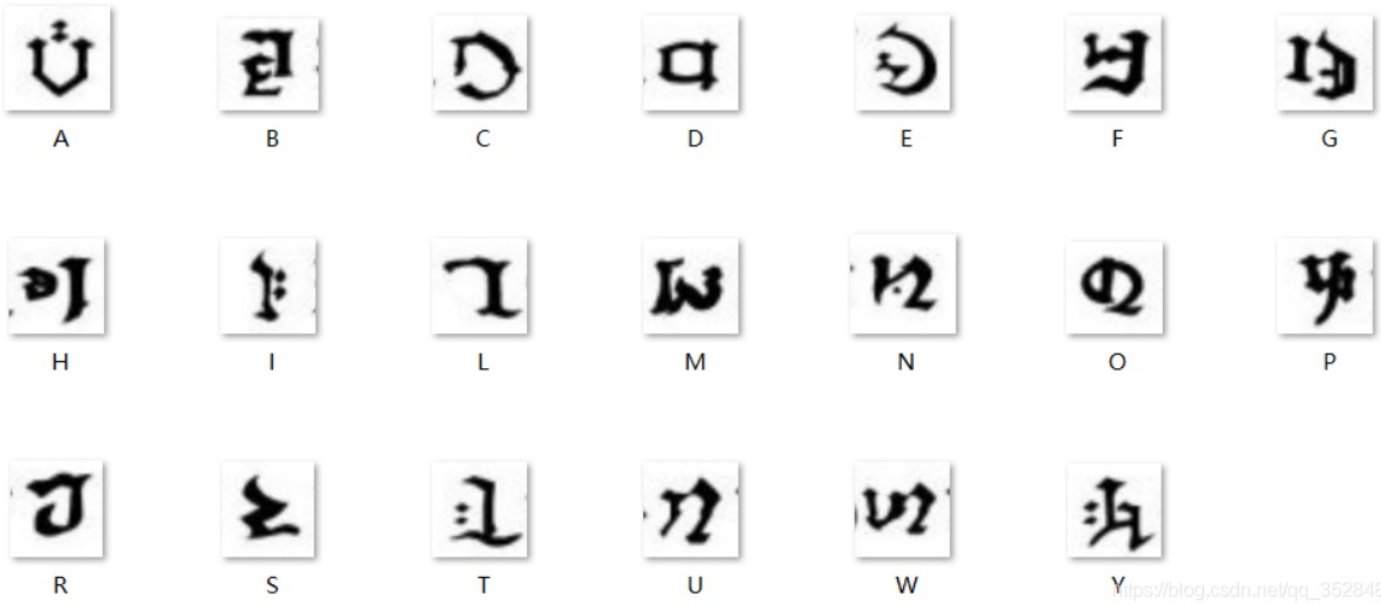
低位，尝试用StegSolve调至红绿蓝最低位



发现flag{happy_bugku_y0000}
根据flag.txt提示

所以正确flag为flag{red_black_happy_bugku_y0000}

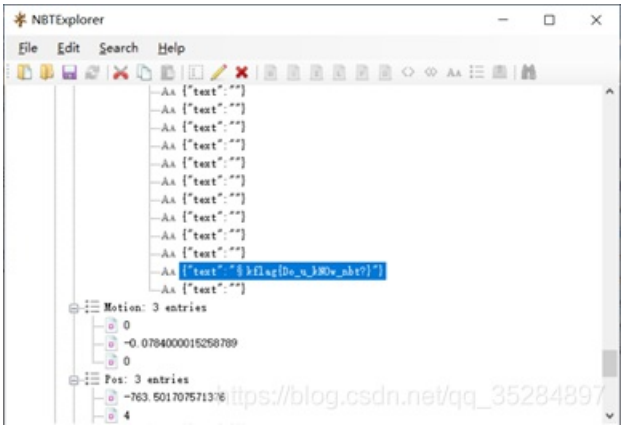
35.可爱的故事



翻译一下即可找到flag

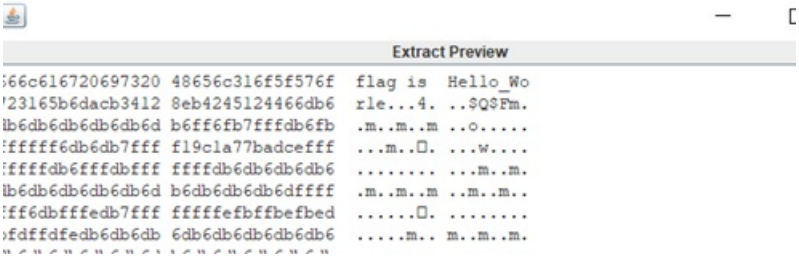
36. easy_nbt

NBTExplorer 打开level.dat 找一找，就找到了

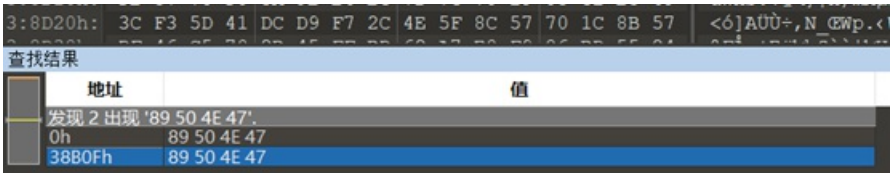


37.赛博朋克

zip伪加密
修复后解压得到txt文件，010分析发现是png文件，文件尾部有提示
Stegsolves打开，最低有效位提取
得到flag,注意格式1和l要区分 flag{Hel1o_Wor1e}



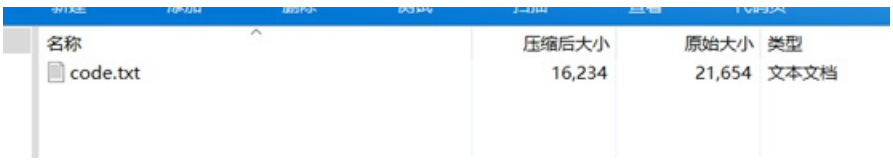
38.random color



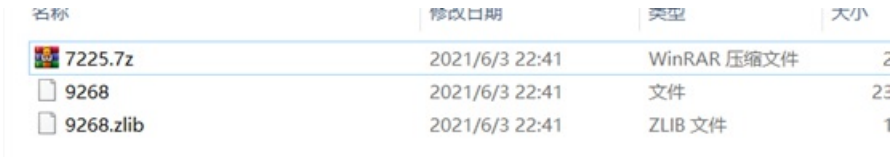
尾部藏有另外一张图像
分离出来，steg Xor一下
得到二维码
扫码得flag

39. Pokergame

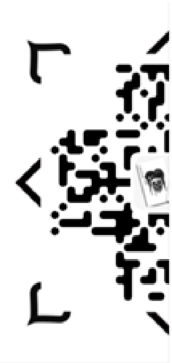
010分析king.jpg和kinglet.jpg后面都隐藏有内容
分离一下
从king.jpg分离得到：
加密压缩包，加密了code.txt



再看kinglet.jpg，分离得到：



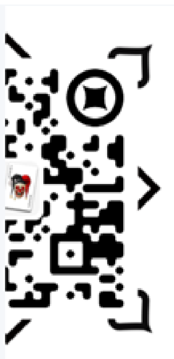
7z压缩包，打开发现文件错误，010分析，尾部是png文件尾
分离出png文件，得到



那一半应该就在大王里隐藏了
再看大王分离出得压缩包，尝试爆破无果后，尝试伪加密，成功
解压得到code.txt

8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAD7zSURBVHhe7Z0JYBRF2v4zM7kPcgcSkCtcAcJ9h8jlgbjqquuB8Omq
+1cEFgHlUEAI13qgyLXoeqAl7ilfroJ+rrt4gCDIKYsQzpBwBQIJOcg9mfyfmXoJc3R3enq6ezqT/jHGqpqq6qruZ96qeqe6x1BbW
+unoyM3Rvq/jo6s6MLSUQRdWDqKoAtLRxF0Yekogi4sHUXQhaWjCLqwdBRBF5aOlujC0lEEXVg6iqALS0cRdGHpKIluLB1F0lWlowi6s
HQUQReWjiLowtJRBF1YOoqgC0tHEXRh6SiCLiwdRdCFpaMlurB0FEEXlo4i6MLSUQRdWDqKYBWW2WzWn
+Cgly/GkpKSf//rX6dPn7ZYLJSmo+Mxpla33PLClCl79+zp179/bFycwWCgd3R0PMD0y88/FxQUnD9//uiRI7379o3TtaUjB6bqykr8D
+PguXPnjmdm9uzVK6FpU/aejo5kTKYb9gnz97Nnz548cSK1W7dmzZqxRB0dadwUFoC2crKzs06f7tK1a7PERErV0XEfB2EBaCv7jWUIJ
TEpCRK1dFxE2dhgVo/vzNZWTBdHTt1StK1pSMJDmExoK2zOTkdO3ZMat6cknR0RMMrLIDJFrTVoVOn5rq2dNxESFggC3YrOxvagt0S
yqej44gplixs9JgxRpPpUm4upTkCbWVnZbG5vO471RGJafq0aS9Mn96te/cTx49fvHiRkh3BOvHUqVNdunZNTEzUtdWwqK6uttRYTCYT
xdXCtHHjRpiili1bJicnW7V14QK94wgmW3g3tVu3ps2a6dpqEFy6dOnzTZ9//933z7FOyDvgZ8E2ABggNqK2Ofoul1kZVVdV3W7cO6t8/wGDgfAUZjU
MHDz6wf39NTQ0roqNBysvLf/rpp5deemn4sOFtW7ed9OdJRYVF9J6KWD2idcBsQltpAwY4SaruFWQypQ8adODAAV1bEsBnmlHzDHA
OKS6aWjlCqOtmbQyz2Zydnb36r6vv//39XbtEbda0WUR4RKeOnf7xj39QEXVx/pEm9Hbbjz+
+Mnv2nl9+oSRHMFr36dNnxerVqamp6o/cDRRc9dyLudu3b9+1a9eZ7DPXCq5hfAgIDAgNCQ0NCw0Jxv9CQ0Lw/
+DgoGAQFBwUFBiEDOyfv7+/0Wg02f4ZDda9mbhquFLV5urKisrSstKioqIzZ84c
+vXQ1atXi4uLoTN23Lvvvvvt5W83TfDCrgKOX/9Cs3784QdhbfXq1WvVO
+9gyqVrSxhc/rNnz65Zs2bzl5sLCgowTsFW1V14zFYZ0A0Ug391URbws/2zBmyZWak6rJbhhiGsqrb+ozdsxMTETJ8+ffyE8RRXF
+6flUPiD99/P3fOnF9276YkR/xNph49e0JbWE7q2uKjrKzsP//5z8KFC3OycyoqKihVLWN6+fXuKqwv3zRT4cAwfMWLe/Pn9Bg
ygJEfMNTUHDx4cP27cr7/
+ig8lperYUVJSsnbt2snPTz5x/lT6qsLA2n9Af2+pCgjdpTPittsy5s/vP2CAqxEG0NOvBw9OfO45KKzOtuswoKQtm7csmL8gPz
+fc0xQmuTk5FF3jaKIN6jn9i9oy2q3+vfHqE9JdkBbBw8ceH7ixix379+unaqgOn5cD
+A/Pnz79+/TolqU7Hjh379e9HEW9Qj7AA01bffv0451LQ0769e6c+//xlu
+fPnly5e9YqsA1pi33HILRbyEad68eRTkp23btq1atTp58mRubi7nybpw4cLRI0dSOndu3rw557jZeIC5+vHHHyGsStvNBE4EBATEx8e3bN
UyKSkJgdjYWWKzdoqKimjRpEhERER4eDk0w10OQjcDAQBQB+FQDf3+smigA8C7OtuvnOSwsbOiwoQMHDqS4N3Djx8a//
+67jLlz9+7ZYzabKcmRAQMHLn711UFpaZzjiMBenruuee++OcXrmcJ0kIPT7//7t79OgRQOCOSvKbsrLrX

很明显得base64转图片，在线工具转一下https://tool.jisuapi.com/base642pic.html
得到另一半二维码

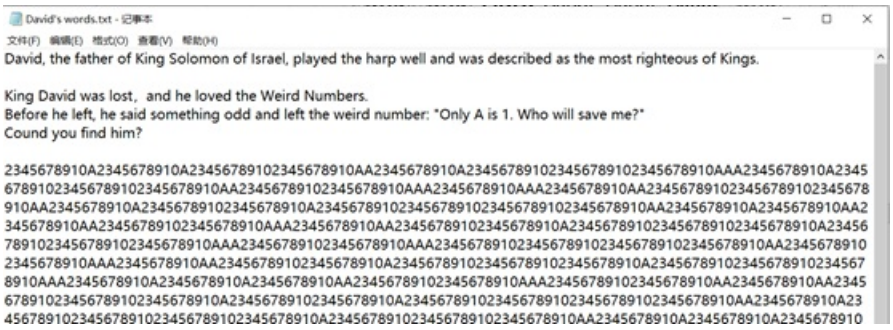


组合起来发现缺少定位符，手动补齐一下

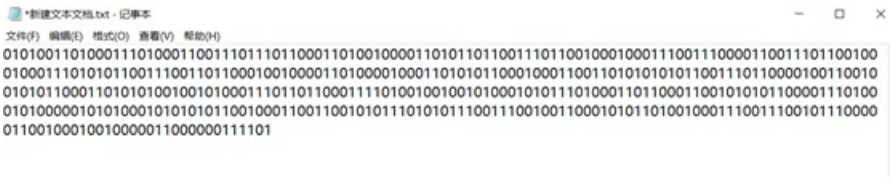
扫码得到 key{P0ke_Paper}
得到第一步Poke.zip加密压缩包得解压密码
解压Poke.zip得

老K(K.jpg)明显有问题，打不开。010分析下，发现是zip文件

修改后缀，解压发现是加密压缩包
寻找解压密码
其他图片暂没看出什么异样
分析David’s words.txt



只有A是1，那其他全是0了？（此处请教了V3师傅）
将A改为1，2345678910改为0，得到二进制字符串



8位一组转Ascii得

SGFwcHkgdG8gdGVsbCB5b3Uga2V5IGlzIEtleXtPTUdfWW91ZG9pdH0=

附代码

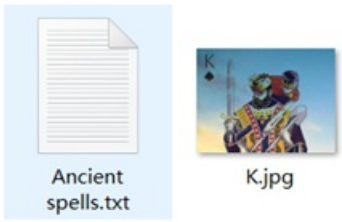
```
str = '01010011010001110100011001110111011000110100100001101011011001110110010001000111001110000110011101100100010001110101011001110011011000100100001101000010001101010110001000110011010101010110011101110000100110010010101100011010101001001010001110110110000111101001001001010001010111010001101100011001010101100001110100010100000101010001010101011001000110011001010111010101110011100100110001010110100100011100111001011100000110010001001000001100000111101'
flag = ''
res = ''
for i in str:
    res = res + i
    if len(res)==8:
        flag = flag + chr(int(res,2))
        res=''
print(flag)
```

将得到字符串，解base64得

Happy to tell you key is Key{OMG_Youdoit}

得到K.zip的解压密码

解压得



要修好它，得到的flag还是反向的

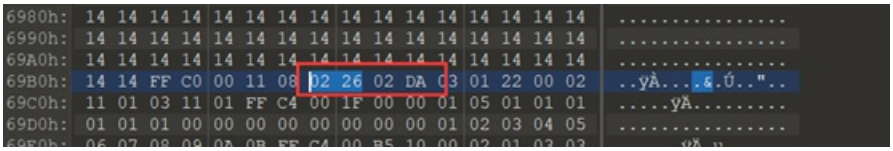
很明显，老K的下面缺少一部分，那就拉高

这里跟V3师傅学习了一招，修改jpg文件的宽高，直接将其宽高值转为16进制去010里搜

查看老K详细信息。得到宽高为730×550

转为16进制就是 2DA×226

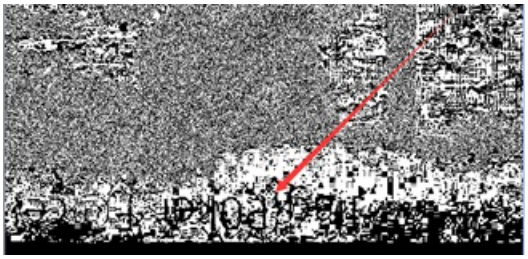
010搜索 02 26



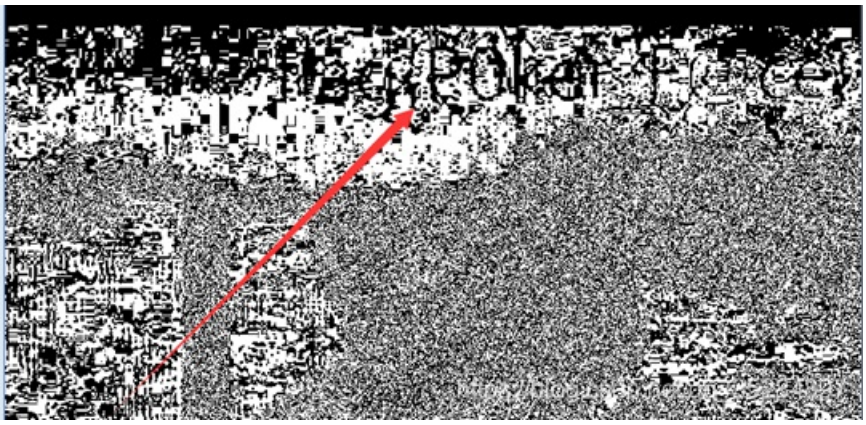
修改高度

得到

不规则的地方。应该藏有东西
Stegsolve跑一下

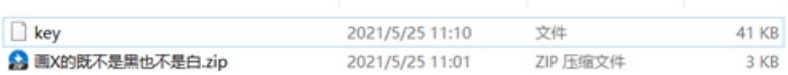


有信息，但是字母是反着的，将图片转向一下

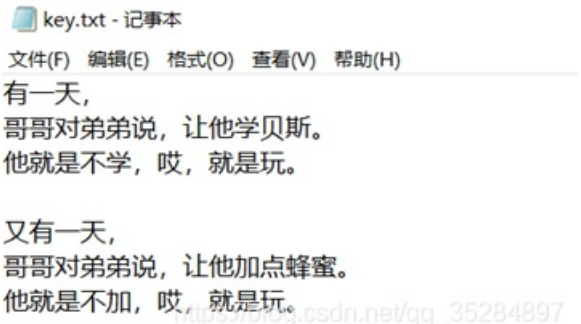


隐约可以看清,再结合题目名字和题目提示，
得flag{Poker_F@ce}

40.出其不意

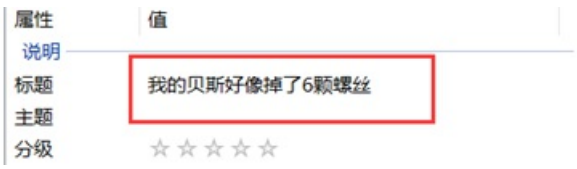


加密压缩包
010分析key
发现是jpg图片，藏有压缩包
分离出来,解压得到key.txt

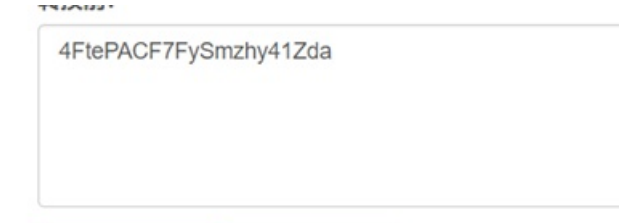


文字游戏，贝斯为base加密，其他没有思路（蜂蜜考虑过蜜罐）
原来的key文件是jpg图像，修改后缀为jpg

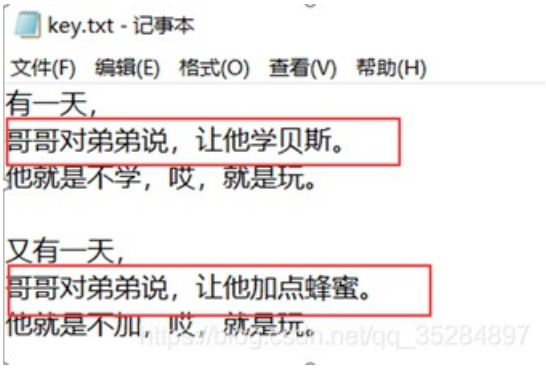
多番尝试，在文件属性发现



Base64掉了6颗螺丝，base58，



解base58得到一个错误的key,思路不对
继续看得到的key.txt



后来才知道，加点蜂蜜就是 加密的意思 ……
base58加密，得到的结果即为解压密码

4DSXTA3yFHGib83QejmSdsnLRNDfn

黑白转为1和0，X根据题目提示，既不是黑也不是白得到
1100110 1101100 1100001 1100111 1111011 1000001 110001 1011111 111001 1011111 110101 1101000 110001 1011111 1110111 1100001 1101110 1111101
二进制转字符串得到flag

二进制转字符串得到flag

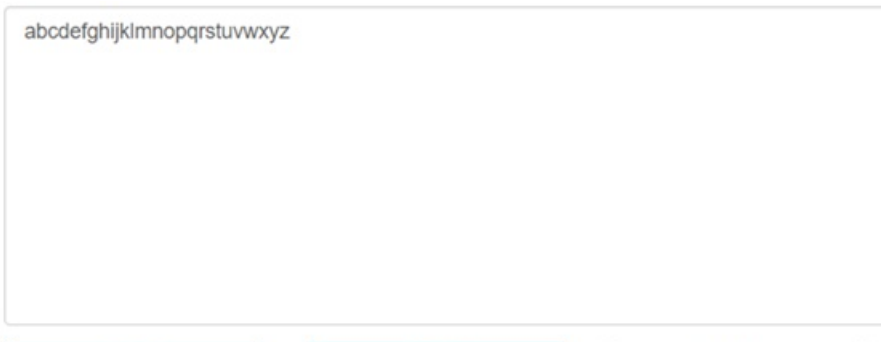
41.攻其不备

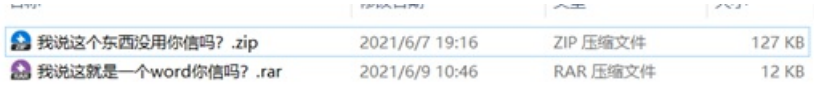
我说这里只有一张图片你信吗？.pdf	108,051	119,045	Adobe Acrob
最好看的萝莉.rar	141,852	141,852	RAR 压缩文件

pdf和加密压缩包，密钥应该就在pdf文件中
只有一张图片？肯定不信
打开pdf，发现一张辣眼睛的图。既然不止一张图，用foremost提取，得到另一张图

分析之后并无信息，方向错误。
重新回到pdf，第二张图010分析既然不在尾部，那就应该在第一张图的下面。用pdf编辑器把第一张图delete,果然得到第二张图。把第二张图也delete，得到另一片天地

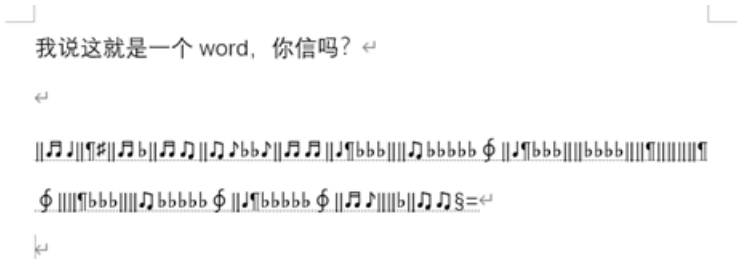
emoji编码，粘贴不了，只能自己手动解了
这里用vol师傅写好的对照表





解码得`mumuziyyds`，即得压缩包密码
zip文件打开后里面有key.txt，但压缩包加密了。没有其他提示信息，不是伪加密，也不是crc32爆破，尝试直接暴力破解 得到密钥`666666`

错的key
果然没用
继续尝试暴力破解rar
得到密钥是一个空格`“ ”`
解压得到



‖♬♩‖¶♯‖♬♭‖♬♫‖♫♭♭♪‖♬♬‖♩¶♭♭♭‖‖♫♭♭♭♭♭𝄞‖♩¶♭♭♭‖‖♭♭♭♭‖‖¶‖‖‖‖¶𝄞‖‖¶♭♭♭‖‖♬♭♭♭♭♭𝄞‖♩¶♭♭♭♭♭𝄞‖♬♪‖‖♭‖♫♫§=

音符解密(https://www.qqxiuzi.cn/bianma/wenbenjiami.php?s=yinyue)得flag

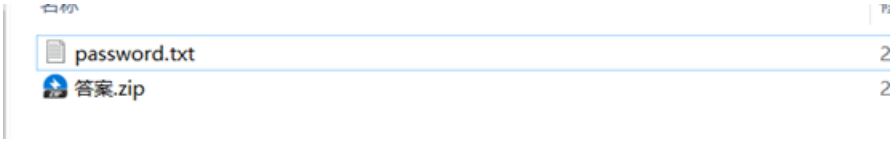
42.答案

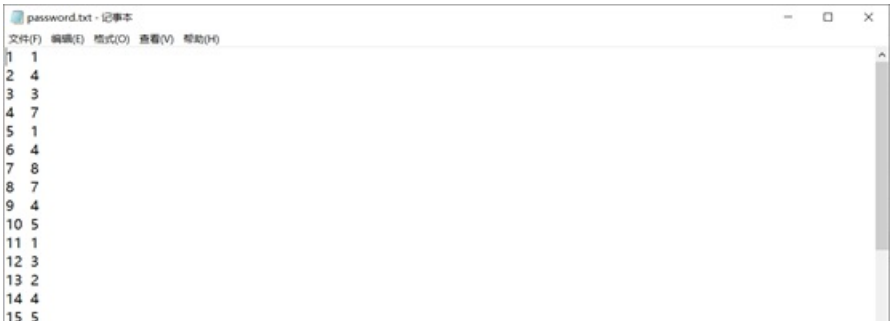
解压得到无后缀文件，010分析发现是jpg文件，且后面隐藏有压缩包
加上后缀jpg，分理处zip压缩包，发现是加密的
在jpg图片的属性里，发现佛语

与佛论禅解密
注意：要用bugku里的与佛论禅工具 https://ctf.bugku.com/tool/todousharp
百度里第一条常用的解不出来这个，应该是算法不一样

得到压缩包密码： 美乐蒂卡哇伊

解压得





在password.txt底部，发现tip

搜索《青花》歌词

歌手：周传雄(小刚)

专辑：蓝色土耳其

三月走过柳絮散落

恋人们匆匆

我的爱情闻风不动

翻阅昨日仍有温度

蒙尘的心事

恍恍惚惚已经隔世

遗憾无法说惊觉心一缩

紧紧握着青花信物

信守着承诺

离别总在失意中度过

每行两个数字对应歌词一个字，获得压缩密码：

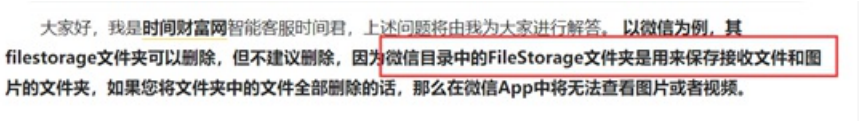
三匆爱温蒙惚心信承失记愈的逢过濡善着记回寞神梦

解压得

010分析，在尾部得到base64字符串，解密得flag

43. FileStoragedat

题目描述说标题有用，附件是一个dat文件



微信PC版存储的本地文件格式为DAT格式, 而且是加密过的,用解密工具（`https://lindi.cc/archives/301`）

44.聊天

拿到win7.vmem，内存取证

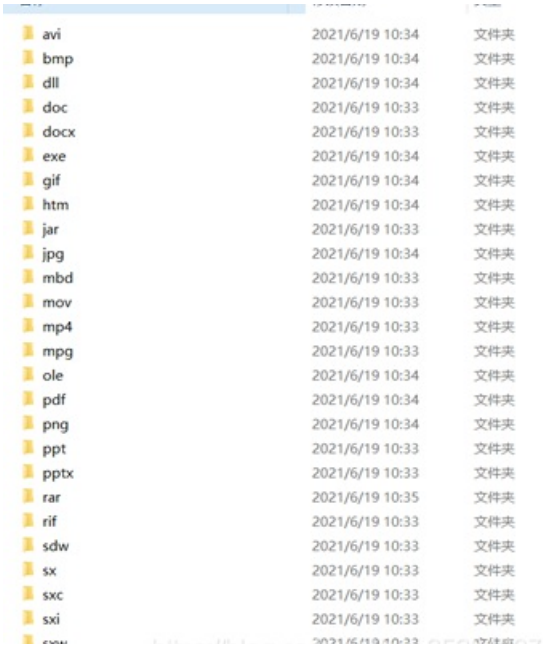
```
root@kali:~# volatility -f '/root/Desktop/win7.vmem'  --profile=Win7SP1x64 filescan | grep -E 'jpg|png|jpeg|bmp|gif'
Volatility Foundation Volatility Framework 2.6
0x000000027e7a300     16      0 RWD--- \Device\HarddiskVolume1\Users\IEUser\AppData\Local\Temp\1623897562.jpg
0x000000003d6a42f0     16      0 R--r-d \Device\HarddiskVolume1\Program Files (x86)\Tencent\QQ\Bin\xpng_dll.dll
0x000000003da06070     16      0 R--r-- \Device\HarddiskVolume1\Users\IEUser\Documents\WeChat Files\All Users\3213b982
b11987a3460c2bde6fa08870.jpg
0x000000003da55070     15      0 R--r-- \Device\HarddiskVolume1\Users\IEUser\Documents\Tencent Files\54297198\Image\Gr
oup2\QX\OT\QXOT7LI0()HMIN~GN7{3%Y0.gif
0x000000003da69e80     16      0 R--r-- \Device\HarddiskVolume1\Users\IEUser\AppData\Roaming\Tencent\QQ\Misc\ClientTyp
e\Phone14.png
0x000000003db64c20     16      0 R--rw- \Device\HarddiskVolume1\Program Files (x86)\Tencent\QQ\Bin\xpng_dll.dll
0x000000003de18be0     15      0 R--rwd \Device\HarddiskVolume1\Windows\SysWOW64\pngfilt.dll
0x000000003df7a800     14      0 R--rwd \Device\HarddiskVolume1\Windows\System32\pngfilt.dll
0x000000003e1a5dd0     15      0 R--r-- \Device\HarddiskVolume1\ProgramData\Microsoft\User Account Pictures\user.bmp
0x000000003fcb1e20      4      0 R--r-- \Device\HarddiskVolume1\Users\IEUser\AppData\Local\Temp\BGInfo.bmp
0x000000003fe5d070     16      0 R--r-- \Device\HarddiskVolume1\Users\IEUser\Documents\WeChat Files\All Users\8aa9cc51
622dae7d755c3b00deeac0a5.jpg
0x000000003fe84070      8      0 R--r-d \Device\HarddiskVolume1\Program Files (x86)\Tencent\QQ\Bin\libpng.dll
0x000000003fe84a30     16      0 R--r-d \Device\HarddiskVolume1\Program Files (x86)\Tencent\QQ\Bin\libjpegturbo.dll
```

```
root@kali:~# volatility -f '/root/Desktop/win7.vmem'  --profile=Win7SP1x64 dumpfiles -Q 0x000000027e7a300 -D '/root/D
esktop'
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x27e7a300   None   \Device\HarddiskVolume1\Users\IEUser\AppData\Local\Temp\1623897562.jpg
```

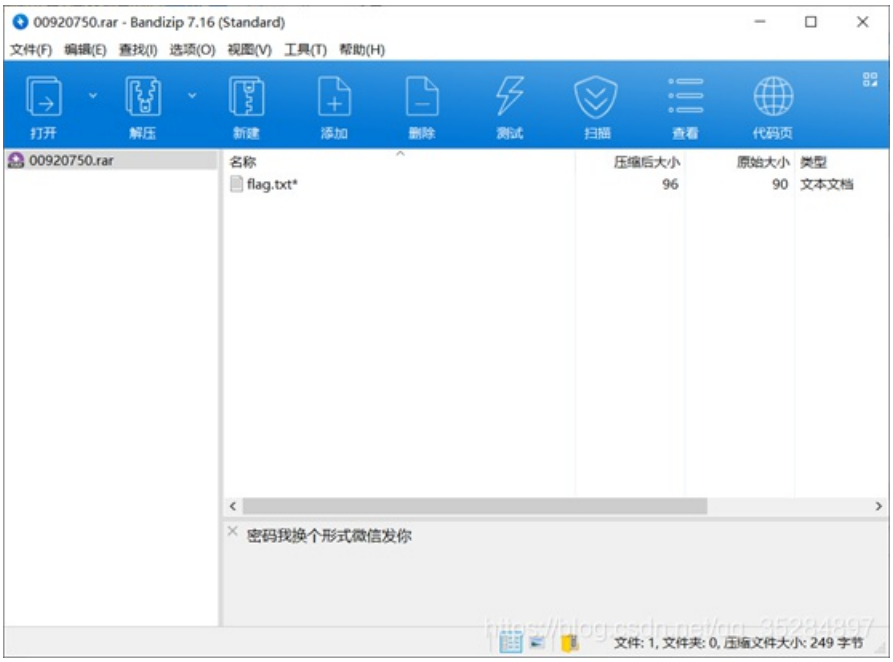
得到jpg文件，有个密码，尝试jpg的几种隐写，无果，那可能是压缩包的密码了
filescan压缩包zip rar
发现疑似flag的压缩包f16g.rar

```
root@kali:~# volatility -f '/root/Desktop/win7.vmem'  --profile=Win7SP1x64 filescan | grep -E "rar"
Volatility Foundation Volatility Framework 2.6
0x000000003e3b54c0     16      0 R--rw- \Device\HarddiskVolume1\Users\IEUser\Documents\Tencent Files\54297
198\FileRecv\f16g.rar
0x000000002e012500     16      0 R--rwd \Device\HarddiskVolume1\Users\IEUser\AppData\Roaming\Microsoft\Win
dows\Libraries\Pictures.library-ms
```

dump下来，发现，kali中竟然把这个rar dump不下来
询问Tokeii师傅才知道原来可以直接foremost 镜像文件，提取rar，涨姿势了
用foremost工具 提取 win7.vmem，得到

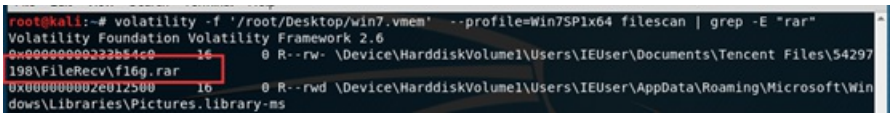


找到rar

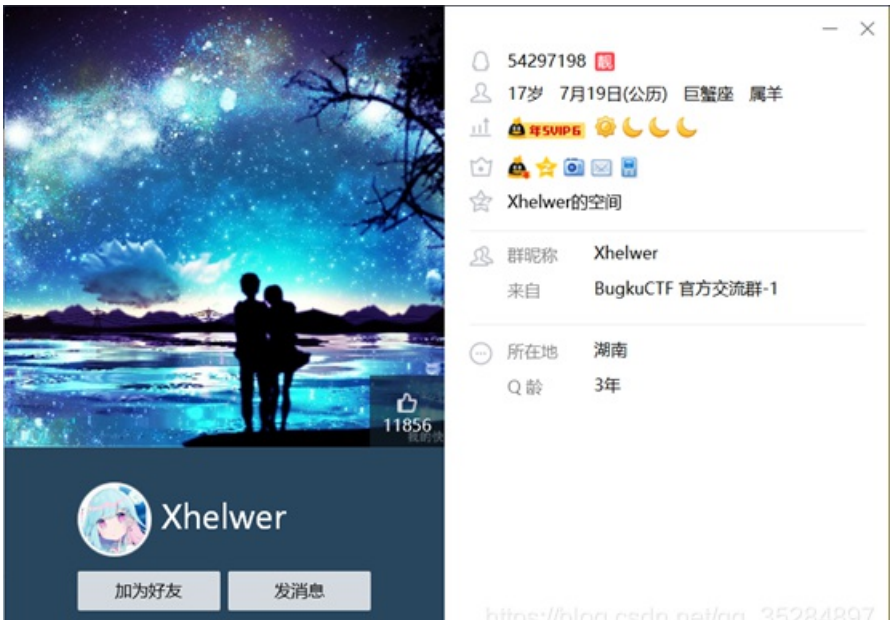


用上图密码解压，得到flag.txt

qqnumber即为54297198(第一次还试了试Tokeii师傅的QQ……hhh)



搜索这个QQ,发现搜索不到……
在bugku的官方群中发现了这个QQ



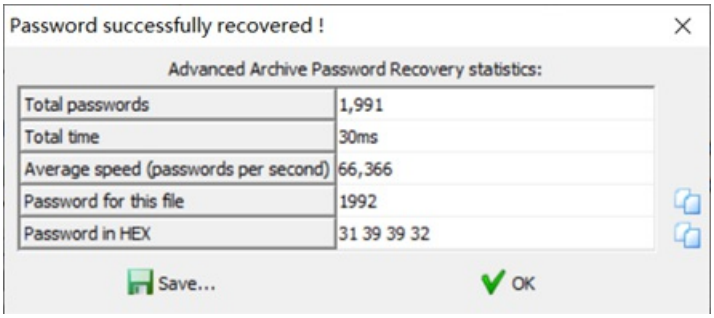
Xor值为00
故flag为
bugku{s1mple_D1gital_f0rens1cs_54297198_Xhelwer_00}

45.细心的大象

Foremost提取，得到加密rar
密钥在图片的属性中，base64解码得到密钥
加压的png图片，修改高度得flag

46.贝斯手

密码我4不会告诉你的，除非你知道我的女神是哪一年出生的
给你个提示：申猴，闰年



5+58为md5+base58