

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](#)

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/qq_35284897/article/details/117121262

版权



[CTF](#) 同时被 2 个专栏收录

4 篇文章 0 订阅

订阅专栏



[Bugku](#)

3 篇文章 0 订阅

订阅专栏

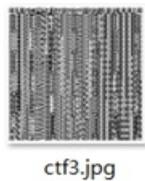
目录:

1. 怀疑人生
2. 一个普通的压缩包
3. 白哥的鸽子
4. 简单套娃
5. 普通的二维码
6. color
7. 一切有为法如梦幻泡影
8. 这是一张单纯的图片
9. 又一张图片, 还单纯吗
10. 眼见非实
11. 啊哒
12. 多种方法解决
12. ok
13. 猜
14. zip伪加密
15. 三色绘恋
16. telnet
17. 闪的好快
18. ping
19. linux
20. 富强民主
21. linux2

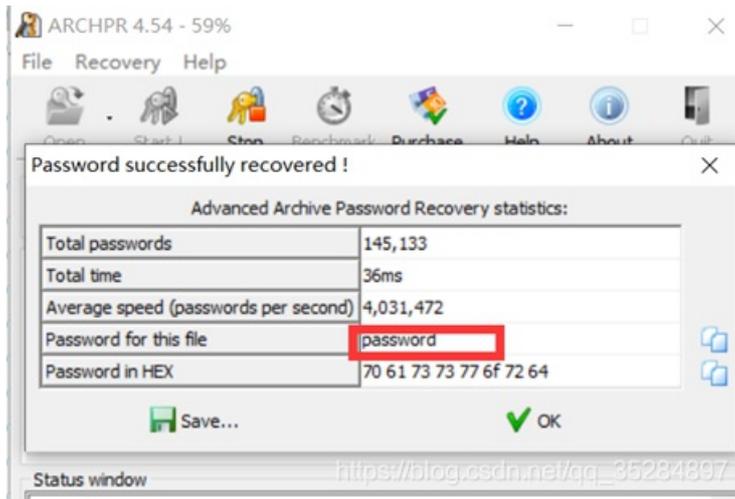
- 22.乌云邀请码
- 23.神秘的文件
- 24.爆照
- 25.隐写3
- 26.隐写2
- 27.一枝独秀
- 28.where is flag
- 29. 听首音乐
- 30.where is flag 2
- 31.悲伤的故事
- 32.where is flag 3
- 33.小美的秘密
- 34.低位的色彩
- 35.可爱的故事
- 36. easy_nbt
- 37.赛博朋克
- 38.random color
- 39. Pokergame
- 40.出其不意
- 41.攻其不备
- 42.答案
- 43. FileStoragedat
- 44.聊天
- 45.细心的大象
- 46.贝斯手

1.怀疑人生

下载附件得到



ctf1有密码，暴力破解得password



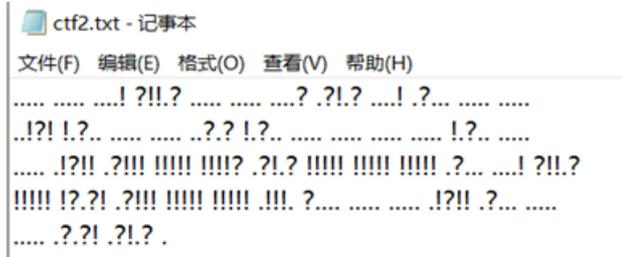
解压得



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}

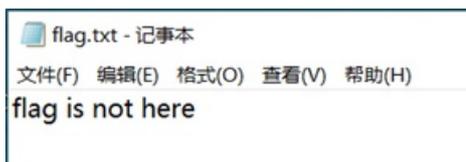


在这里插入图片描述

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



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

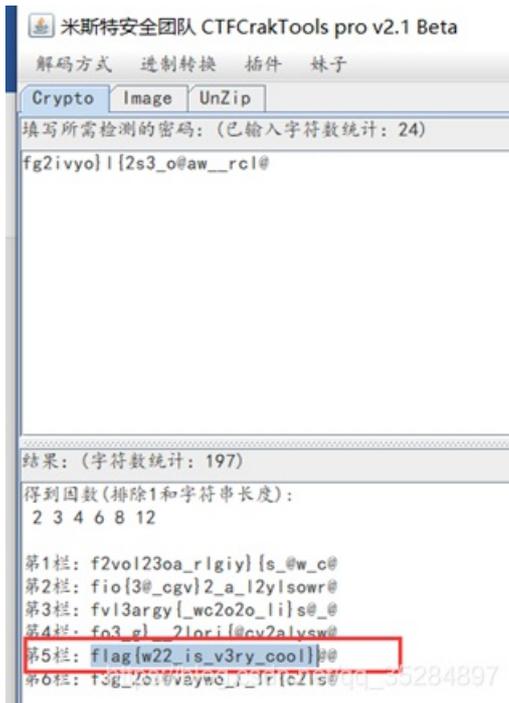


Jpg文件头FF D8 FF 文件尾FF D9

```
78 DC 59 69 DA 8F 64 6E E6 7B A3 57 31 EE 8D DC x0Y10.dnæfEW11.0
: CB 62 45 62 89 EE 5B DC B6 73 01 E3 FF D9 66 67 ÈbEb%i[Üŕs.äyÛfg
: 32 69 76 79 6F 7D 6C 7B 32 73 33 5F 6F 40 61 77 2ivyo}l{2s3_o@aw
: 5F 5F 72 63 6C 40 _rcl@
```

发现尾部多了一串字符串，

分析 fg2ivyo}|{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

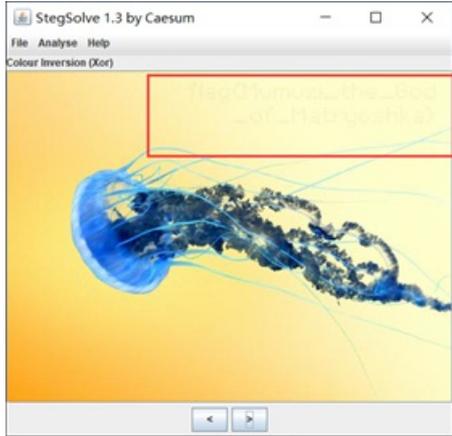


4.简单套娃

下载得到Jellyfish.jpg, 扔到010Editor发现有二个jpg文件头

```
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 60 00yà..JFIF....`
00 60 00 00 FF ED 00 78 50 68 6F 74 6F 73 68 6F ..yi.xPhotosho
70 20 33 2E 30 00 38 42 49 4D 04 04 00 00 00 00 p 3.0.8BIM.....
00 31 1C 02 00 00 02 00 02 1C 02 50 00 09 48 61 .1.....P..Ha
6E 67 20 51 75 61 6E 1C 02 74 00 17 A9 20 4D 69 ng Quan..t.© Mi
63 72 6F 73 6F 66 74 20 43 6F 72 70 6F 72 61 74 crosoft Corporat
69 6F 6E 00 38 42 49 4D 04 25 00 00 00 00 00 10 ion.8BIM.%.....
9E 39 BE 0C 3C 94 F9 B7 86 59 FE 9B A1 26 16 E1 ž9%.<"ù·†Yp>;&.á
38 42 49 4D 04 0A 00 00 00 00 00 01 01 00 FF EC 8BIM.....yi
00 11 44 75 63 6B 79 00 01 00 04 00 00 00 64 00 ..Ducky.....d.
00 FF E1 53 16 45 78 69 66 00 00 4D 4D 00 2A 00 .yáS.Exif..MM.*.
00 00 08 00 05 01 32 00 02 00 00 00 14 00 00 00 .....2.....
4A 47 46 00 03 00 00 00 01 00 05 00 00 47 49 00 JGF.....GI.
03 00 00 00 01 00 58 00 00 82 98 00 02 00 00 00 .....X.,~.....
16 00 00 00 5E 87 69 00 04 00 00 00 01 00 00 00 .....^+i.....
74 00 00 00 D2 32 30 30 39 3A 30 33 3A 31 32 20 t...ò2009:03:12
31 33 3A 34 38 3A 32 33 00 4D 69 63 72 6F 73 6F 13:48:23.Microso
66 74 20 43 6F 72 70 6F 72 61 74 69 6F 6E 00 00 ft Corporation..
04 90 03 00 02 00 00 00 14 00 00 00 AA 90 04 00 .....^.....
02 00 00 00 14 00 00 00 BE 92 91 00 02 00 00 00 .....%'\.....
03 30 38 00 00 92 92 00 02 00 00 00 03 30 38 00 .08..'.....08.
00 00 00 00 00 32 30 30 38 3A 30 32 3A 31 31 20 ....2008:02:11
31 31 3A 33 32 3A 32 34 00 32 30 30 38 3A 30 32 11:32:24.2008:02
3A 31 31 20 31 31 3A 33 32 3A 32 34 00 00 05 01 :11 11:32:24....
03 00 03 00 00 01 00 06 00 00 01 1A 00 05 00 .....
00 00 01 00 00 01 14 01 1B 00 05 00 00 00 01 00 .....
00 01 1C 02 01 00 04 00 00 00 01 00 00 01 24 02 .....$.
02 00 04 00 00 01 00 00 51 EA 00 00 00 00 00 .....Qè.....
00 00 48 00 00 01 00 00 00 48 00 00 00 01 FF ..h.....h.....y
D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01 00 00yà..JFIF.....
01 00 00 FF DB 00 43 00 08 06 06 07 06 05 08 07 https://blog.csdn.net/qq_35284897
07 07 09 09 08 0A 0C 14 0D 0C 0B 0B 0C 19 12 13 .....
```

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



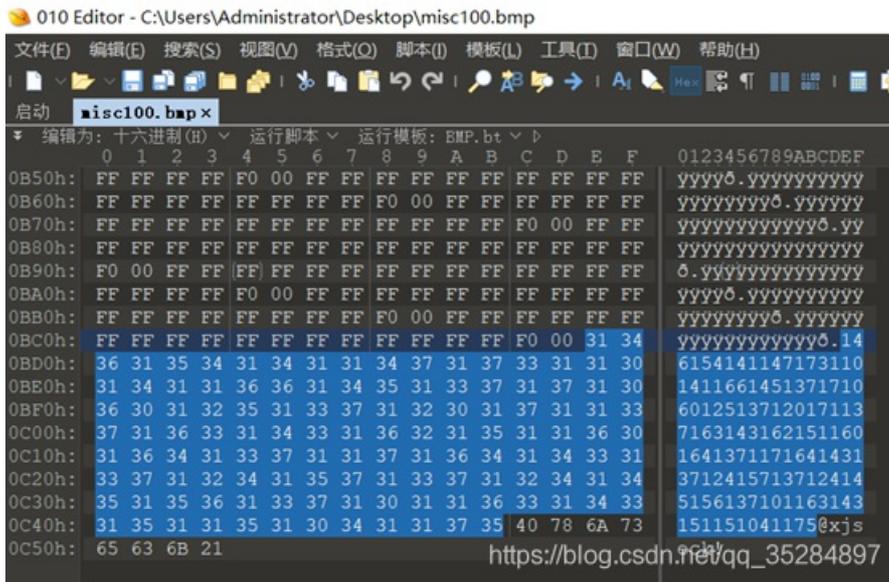
5.普通的二维码

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

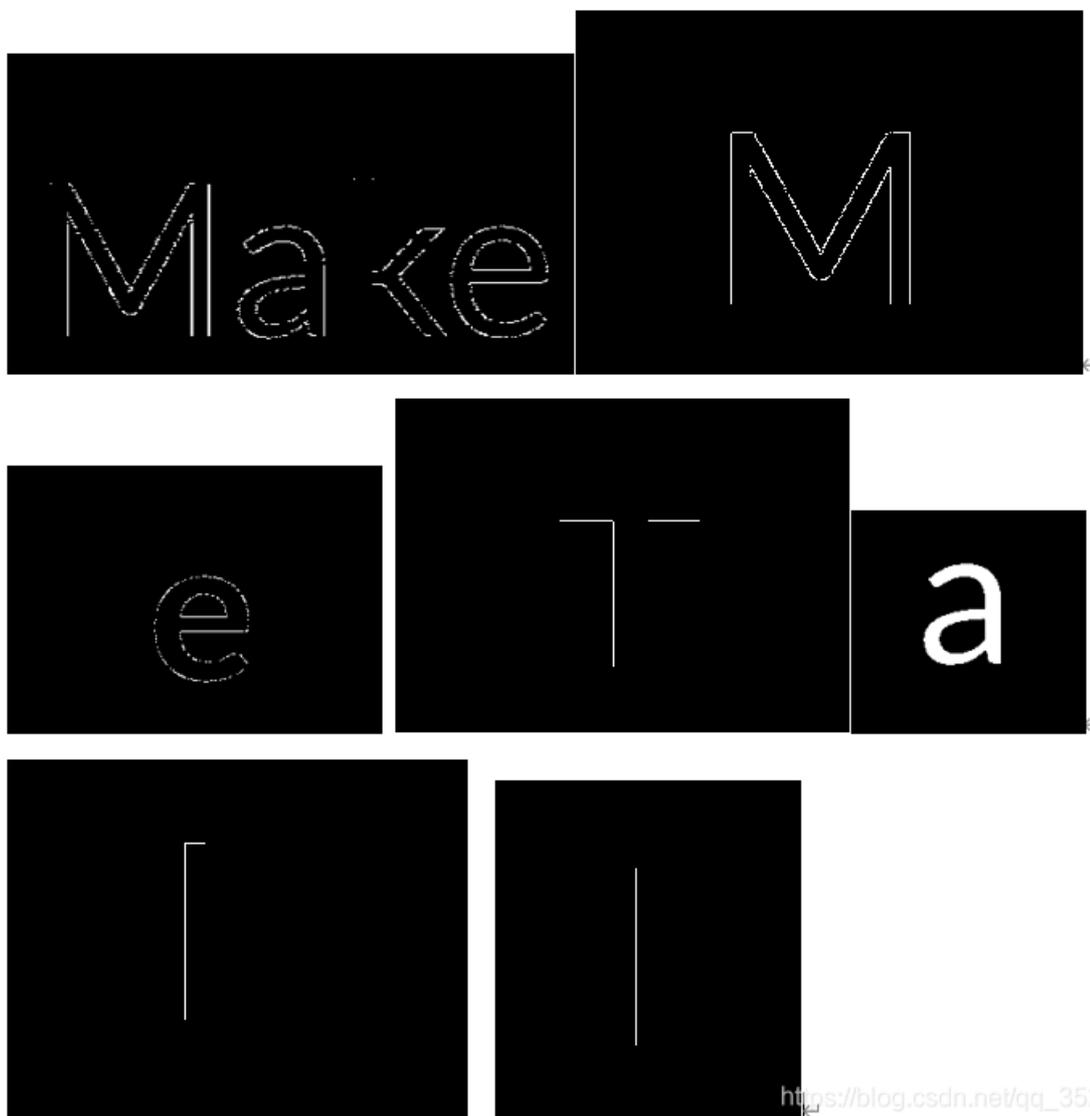
```

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 = '00' + 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：



https://blog.csdn.net/qq_35284897

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（IHDR）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

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
11111011111111011111
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 = '11111011111111011111'
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
文件尾: 50 4B	ZIP Archive (zip),	文件头: 504B0304

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。

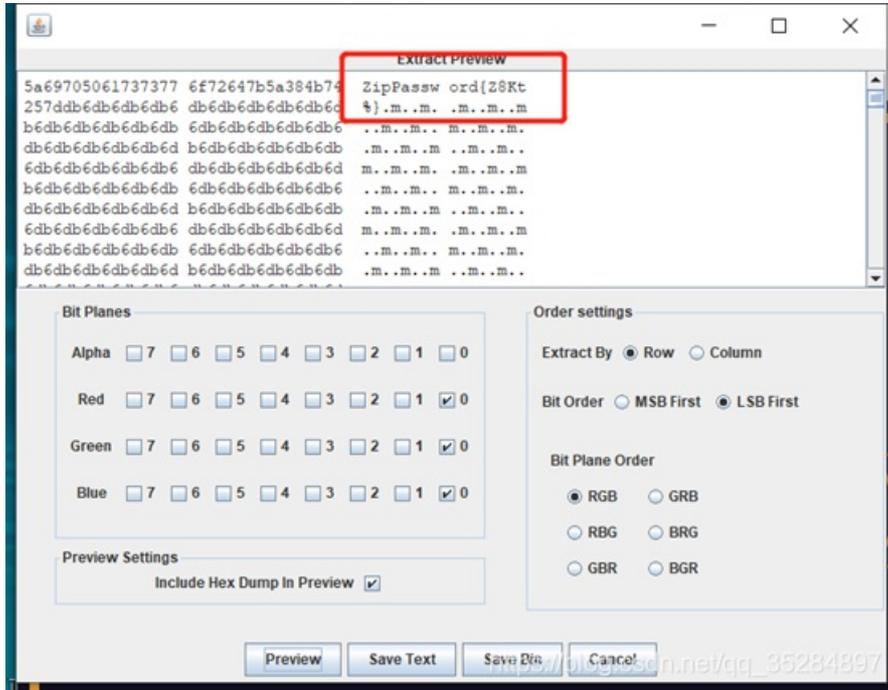


得到密码42，解压得“《探》.zip”（加密压缩包）和“one.png”，将“one.png”丢在010Editor分析一下，同上可得“第2个隐藏压缩包.zip”，解压得“感.png”

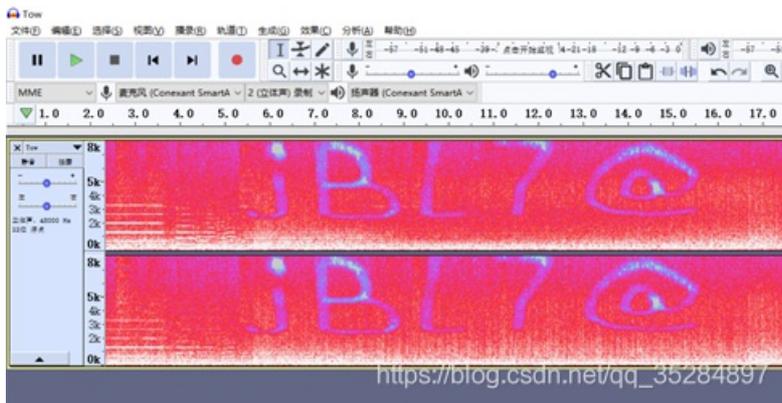
3. 同样套路010分析“感.png”，一切正常，暴力破解“《探》.zip”（加密压缩包）和伪加密也无果。

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=”

```

010 Editor - C:\Users\Administrator\Desktop\一切有为法如梦幻泡影\《家》\《探》\《末》\第4个隐藏压缩包.
文件(F) 编辑(E) 搜索(S) 视图(V) 格式(O) 脚本(I) 模板(L) 工具(T) 窗口(W) 帮助(H)
启动 问.png 第2个加密压缩包.zip 思.jpg 第3个隐藏压缩包.zip 第4个隐藏压缩包.jpg x
编辑力: 十六进制(H) 运行脚本 运行模板
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
1:1C20h: B5 B0 A1 B7 C7 B0 C3 E6 B5 C4 CC E2 C4 BF D6 D0 µ;·Ç"ÀspAîÀA;OD
1:1C30h: D2 FE B2 D8 D7 C5 B4 F2 BF AA CB FC B5 C4 D4 BF Óp;Ø×Å'ò;·ÈupAÖ;
1:1C40h: B3 D7 2E 7A 69 70 0A 00 20 00 00 00 00 01 00 *x.zip..
1:1C50h: 18 00 D9 93 B0 84 C7 40 D7 01 38 F7 20 EF C7 40 ..Ù"°,ç@x.8÷ 1Çè
1:1C60h: D7 01 DD 6C B0 84 C7 40 D7 01 75 70 6A 00 01 E7 ×.Yl",ç@x.upj..ç
1:1C70h: AB EC B3 E3 80 8A E8 BF 99 E4 B8 8E 66 6C 61 67 «i"æSè;~a 3flag
1:1C80h: E6 B2 A1 E6 9C 89 E5 85 B3 E7 B3 BB EF BC 8C E5 a";ææã...ç"»1«Eä
1:1C90h: 8F AA E6 98 AF E4 B8 80 E4 B8 AA E5 B0 8F E5 BD ."=~_a_ea_ã"ã_ãH
1:1CA0h: A9 E8 9B 8B E3 80 8B E5 89 8D E9 9D A2 E7 9A 84 èè×æ<ãt.é.ççš,
1:1CB0h: E9 A2 98 E7 9B AE E4 B8 AD E9 9A 90 E8 97 8F E7 ée~ç>æa,-és.e-.ç
1:1CC0h: 9D 80 E6 89 93 E5 BC 80 E5 AE 83 E7 9A 84 B9 92 .eæh"ãæãøfçš,é'
1:1CD0h: A5 B5 8C 99 2E 7A 69 70 50 4B 01 02 14 00 14 00 YáØm.zipPK.....
1:1CE0h: 00 00 08 00 FC 8A A4 52 5C 6C 3C CC 21 1A 01 00 ...uSøR\l;i!...
1:1CF0h: E1 C4 01 00 06 00 34 00 00 00 00 00 00 00 20 00 áA...4.....
1:1D00h: 00 00 7D 01 00 00 D2 C9 2E 6A 70 67 0A 00 20 00 ..)...Óè.jpg...
1:1D10h: 00 00 00 00 01 00 18 00 84 4D AC 34 C7 40 D7 01 .....M-4Ç@x.
1:1D20h: 7D DC BF 34 C7 40 D7 01 41 D8 1E 34 C7 40 D7 01 }Ü;4Ç@x.AØ.4Ç@x.
1:1D30h: 75 70 0C 00 01 DB 8D 75 F3 E7 96 91 2E 6A 70 67 up...Ù.uóç-`.jpg
1:1D40h: 50 4B 05 06 00 00 00 02 00 02 00 6E 01 00 00 PK.....n...
1:1D50h: D2 1B 01 00 00 0A 59 6E 56 6E 61 33 56 37 64 Ó.....YnVna3V7d
1:1D60h: 32 6C 7A 61 48 6C 76 64 57 46 6F 59 58 42 77 65 2lzaHlvdWFoYXBwe
1:1D70h: 57 52 68 65 58 30 3D

```

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

```
</w:t>
- <w:r>
  <w:t>在这里哟! </w:t>
</w:r>
</w:p>
- <w:p w:rsidDefault="002B3D8D" w:rsidR="002B3D8D" w:rsidPr="002B3D8D">
  - <w:pPr>
    - <w:rPr>
      <w:Fonts w:hint="eastAsia"/>
      <w:vanish/>
    </w:rPr>
  </w:pPr>
  - <w:r w:rsidPr="002B3D8D">
    - <w:rPr>
      <w:vanish/>
    </w:rPr>
    <w:t>[img(F1dgy)]</w:t>
  </w:r>
  <w:bookmarkStart w:id="0" w:name="_GoBack"/>

```

11. 啊哒

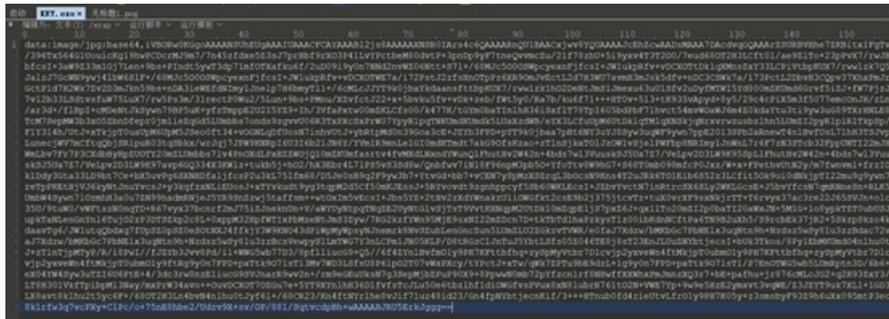
ada.jpg用O10分析，发现后面又压缩包。分离出压缩包，解压需要密码。可以尝试一下爆破。解压密码在ada.jpg文件的属性里，照相机型号是16进制，转为字符串即为密码sdnisc_2018。



解压得flag

12. 多种方法解决

下载附件得KEY.exe，O10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.jsuapi.com/base64pic.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

```
管理员: 命令提示符
Microsoft Windows [版本 10.0.18362.30]
(c) 2019 Microsoft Corporation. 保留所有权利。

C:\Users\Administrator>cd Desktop

C:\Users\Administrator\Desktop>java -jar "ZipCenOp (java -jar ZipCenOp.jar r X.zip) .jar" r file.zip
success 1 flag(s) found
C:\Users\Administrator\Desktop>
```

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

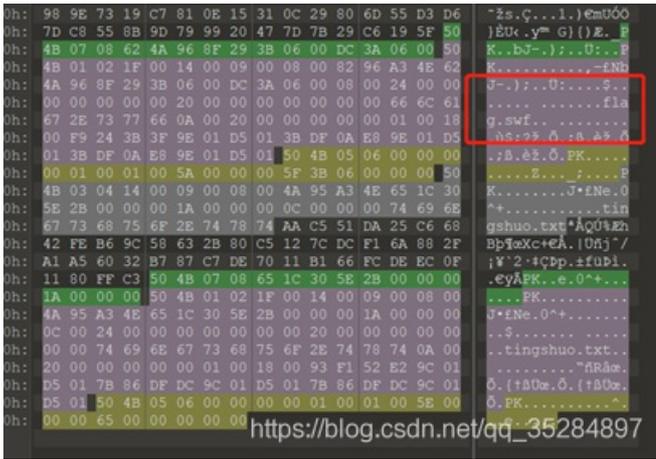


16. 不简单的压缩包

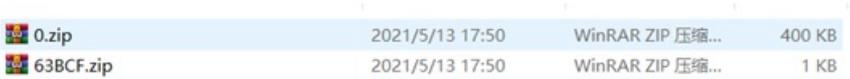
下载得到加密压缩包，里面藏有txt文件



010分析，发现似乎还隐藏了另外一个压缩包。



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)

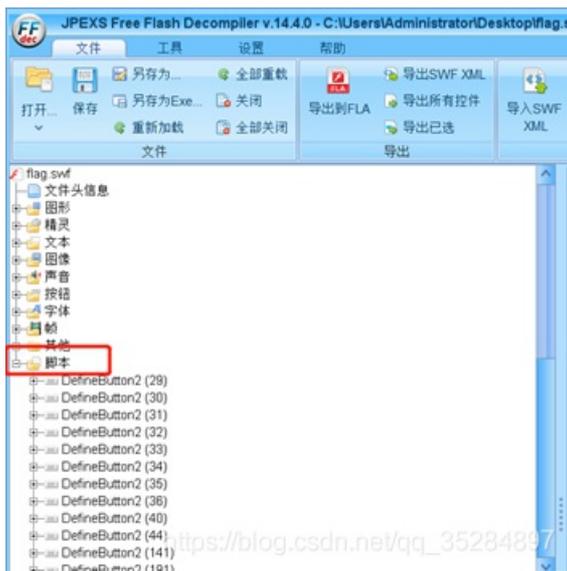
```

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

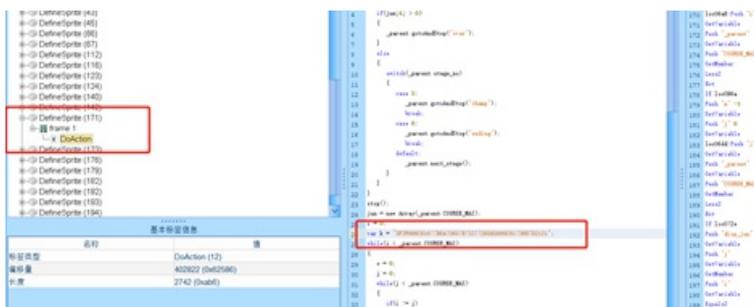


解压得flag.swf

swf文件，用JPEXSFreeFlashDecompiler(反编译swf工具)，尝试一下



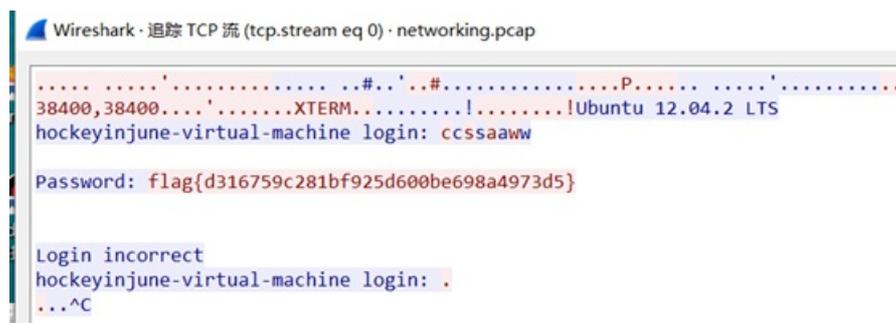
在脚本中一个一个过，最终在171处发现一串16进制代码



转为字符串，得到flag

16.telnet

Wireshark打开，右键追踪TCP流，得到flag

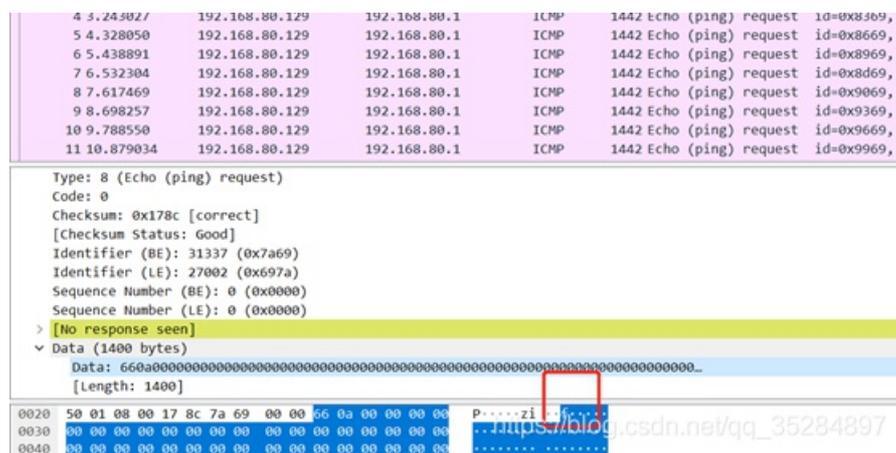


17.闪的好快

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>



核心价值观编码

社会主义核心价值观: 富强、民主、文明、和谐; 自由、平等、公正、法治; 爱国、敬业、诚信、友善

flag[0003c775199926]

编码

解码

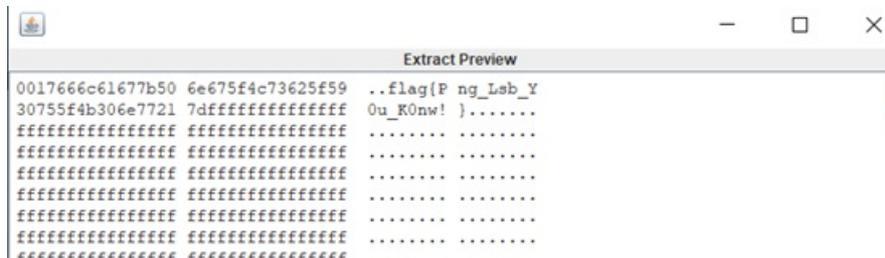
公正 公正 公正 诚信 文明 公正 民主 公正 法治 法治 友善 平等 和谐 敬业 和谐 富强 和谐 富强 和谐 文明 和谐 平等 公正 公正 和谐 法治 公正 公正 文明 和谐 民主 和谐 敬业 和谐 平等 和谐 敬业 和谐 和谐 和谐 公正 法治 友善 法治

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。

名称



2018山东省大学生网络安全技能大赛决赛writeup.docx *

logo.png *

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

名称	修改日期	类型	大小
8	2017/10/28 1:15	文件	91 KB
88	2017/10/28 11:02	文件	16 KB
888	2017/10/28 1:41	文件	19 KB
8888	2017/10/28 2:02	文件	12 KB
88888	2017/10/28 1:00	文件	91 KB
888888	2017/10/28 1:00	文件	91 KB
8888888	2017/10/28 1:00	文件	91 KB
88888888	2017/10/28 1:00	文件	91 KB
愉快的排序吧哈哈.gif	2017/10/28 10:32	GIF 文件	58 KB

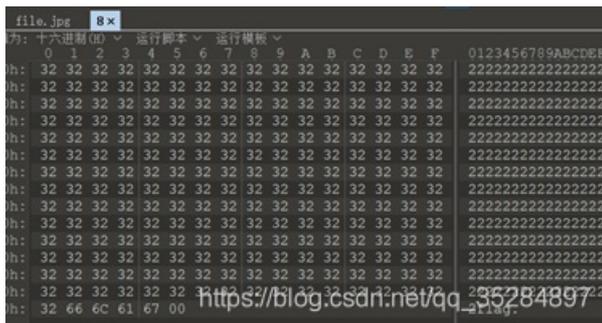
https://blog.csdn.net/qq_35284897

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

告诉你们一个秘密，密码是3个数。

查理曼：查理曼，法兰克王国国王，征服了西欧与中欧大部分土地，具有至高无上的权威，下令全国人民信仰基督教，查理曼征服了西罗马帝国。
雅典娜：女神帕拉斯·雅典娜，是希腊神话中的女战神也是智慧女神，雅典是以她命名的。
三斯潘特：奥林匹斯神话中的人物，是宙斯王后赫拉女神中的一员，看上去就是一个清秀俊俏的种小伙子。由于传说中他是一名出色的射手，因此他被称为神箭手。三斯潘特与三后之恋导致了他与宙斯王之间的战争。
Hint:
其实斗地主最好玩的。

密码是3个数，爆破一下得到password: 871



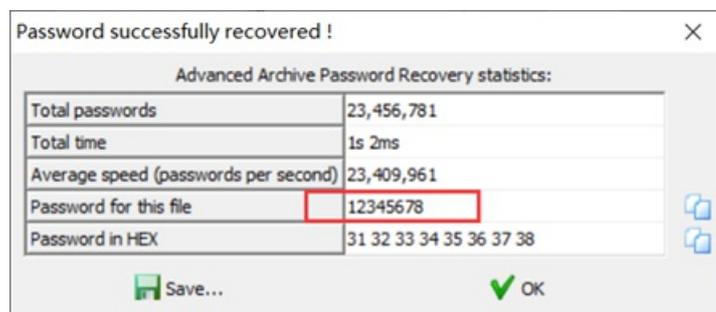
解压得3.jpg, 010分析在最后得到flag: f1@g{eTB1IEFyZSBhIGhAY2tlciE=} 提交不对, 内部是base64加密, 解密得y0u Are a h@cker!



27.一枝独秀



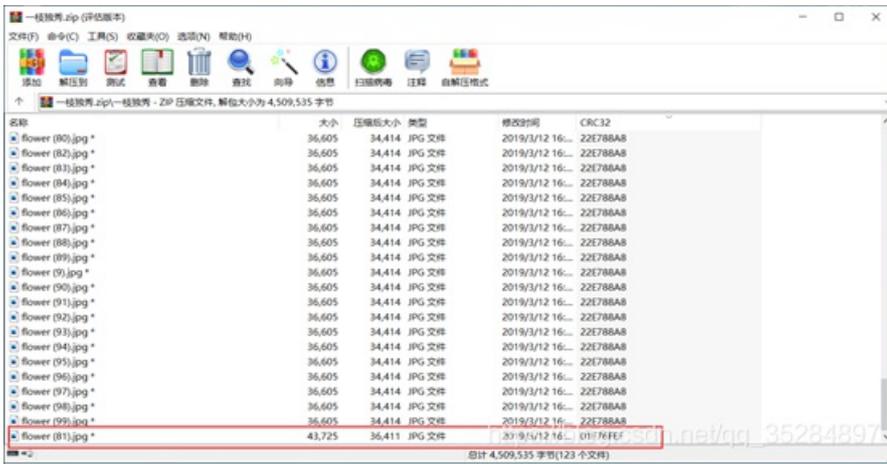
下载附件解压得一张有问题的png图片, 010分析一下发现PK, zip压缩包, 修改后缀, 得到一个加密的压缩包。暴力破解一下, 得到解压密码



解压得123张flower图片，一模一样.....



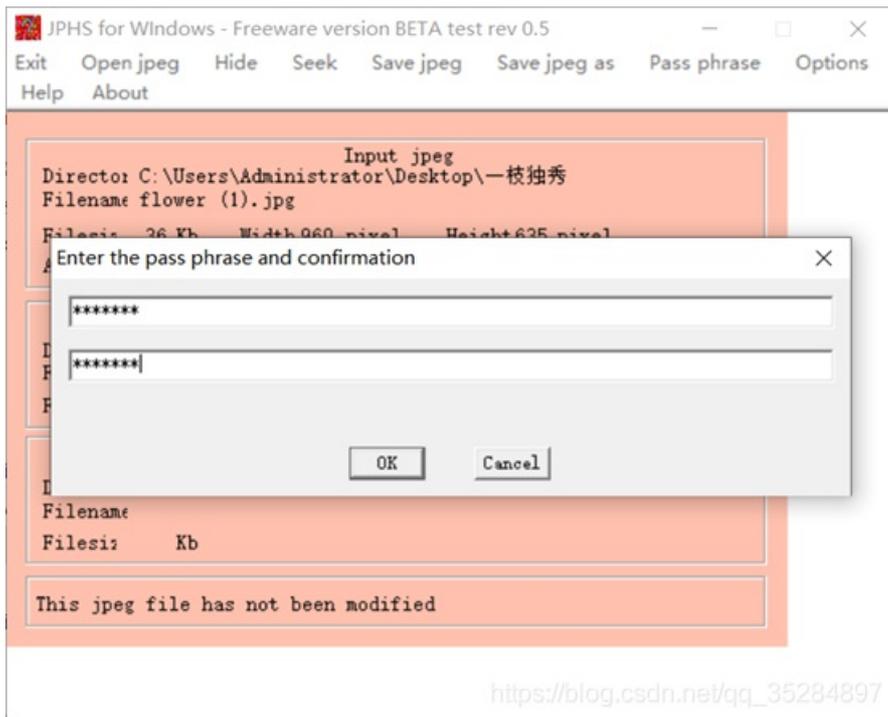
根据经验，解题点应该藏在其中某一张或者几张图片中，接下来寻找图片的不同（如大小等.....）
打开原来的压缩包，比较图片的不同



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。

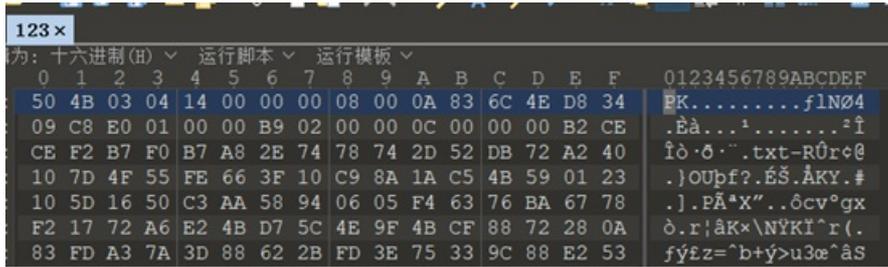
把81拿出来，O10分析一下，没有发现异常。由于是jpg文件，想到了处理jpg和jpeg文件的神器，Jphs，但是还缺少密码。

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

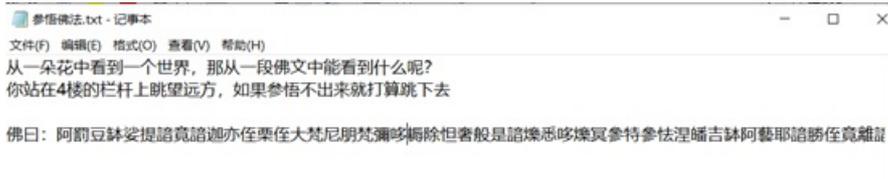


用Jphs从成功从81图片中分离出一个文件，命名为123

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

与佛论禅

H-hDs100ZL31hIZZbeRSbbbVRZNm32W2X33mGm3Txt999RdV9hx0

听佛说宇宙的真谛

参悟佛所言的真意

普度众生

本来无一物，何处惹尘埃

佛曰：阿罰豆鉢娑提諸真語迦亦任粟任大梵尼朋其彌吟攝除但奢般是諸熾悉吟熾冥參特參祛涅囉吉鉢阿藝耶諳勝任竟雜誑。其究吟攝虛他炬明漫究吟得吟藕集能冥盡滿知俱朋怯室神奢羅姪豆罰帝遠蘇明其苦奢密任曰鉢者特吟呼勝蘇不冥死等那阿冥悉奢羅豆涅鉢波罰。罰摩任故罰夢鉢恐編寫誑聞舍吟得波舌奢印罰恐冥道一吟究其呼冥聞吟上罰兩罰誑寫冥依誑者吟游故吟吟夾吾任曰吟逝至編佛誑耶

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

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

16进制转Ascii

ASCII转换到 ASCII (例: a b c)

bugku{You_can't_imagine_the_happiness_of_hiding_the_flag!!!}

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

6275676b757b596f755f63616e27745f696d6167696e655f7468655f68617070696e6573735f6f665f686964696e675f7468655f666c61672121217d

https://blog.csdn.net/qq_35284897

31.悲伤的故事



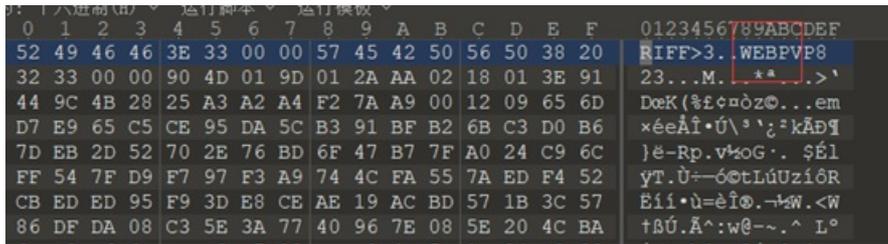
加密压缩包，



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

一个悲伤的故事 > 2158646223

名称	#	标题	参与创作的艺术家	唱片集
有一种悲伤.....exe				
这是一首歌，请静...		5个数字，我永远忘不掉它	郭静	

C:\Users\FD\Desktop\一个悲伤的故事\2158646223\有一种悲伤.....exe

请输入那串我永远忘不掉的数字:

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?



2019年3月4日，为电视剧《只为遇见你》演唱的同名主题曲《只为遇见你》上线^[45]；5月30日，为电视剧《我们都要好好的》演唱的爱情密码剧终曲《83721》（《不想去爱你》）发布^[46]；6月27日，为电视剧《那片花那片海》演唱的主题曲《手心》正式上线。

C:\Users\FD\Desktop\一个悲伤的故事\2158646223\有一种悲伤.....exe

请输入那串我永远忘不掉的数字: 12345
看来你并不了解我，再给你一次机会吧！
请输入那串我永远忘不掉的数字: 83721
flag{1_I0ve_7ou_F0ever}
请按任意键退出...

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 9:09:08

时间转时间戳

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

2021 年 5 月 21 日
8 时 14 分 09 秒

转换成时间戳

时间戳 1621556049

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

前言.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

女神小美邀请你到她家做客，并想对你说一些话。兴奋不已的你背起了行囊，往她家奔赴而去。

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

每组字数 11 加密 解密

KeyIs(\$key2987)

KeyIs{\$key2987}

即为小美家.zip密钥

客厅	2021/5/25 8:32	文件夹
储物间.zip	2021/5/25 10:03	ZIP 压缩文件
卧室.zip	2021/5/25 10:02	ZIP 压缩文件

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，

repairhead	2021/5/25 8:29	文件	40 KB
神奇的字符串	2021/5/25 8:27	文件	40 KB

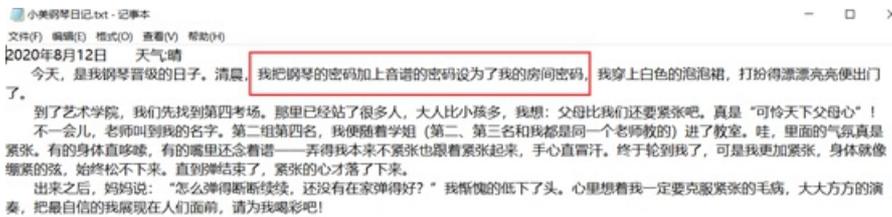
010分析两个文件，发现是被损坏的jpg文件，修复文件头，更改后缀，恢复jpg文件
将两张图像拼接在一起



得到** BugKu233 ,即为储物间的密钥

001	2021/5/25 9:28	文件夹	
002	2021/5/25 9:28	文件夹	
小美钢琴日记.txt	2021/5/25 10:03	文本文档	2 KB

打开小美钢琴日记



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2:





无字天书

查看EXIF信息得到 [/b4f2dLg130Tqg4Q/T0haucaZpwqP](#)

日记3:



组合起来得到

[U2FsdGVkX18qyg4WuEtWtffwxKvgUnUdax/b4f2dLg130Tqg4Q/T0haucaZpwqP/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



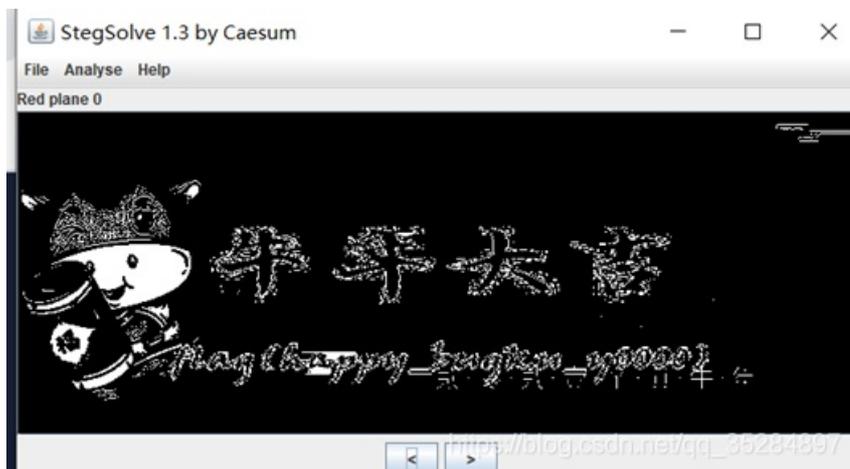
得到密钥 `misc`
AES解密得flag

<code>flag(My_secret_1s_Y0u_@re_x1@ng_peach)</code>	加密算法: <input checked="" type="radio"/> AES <input type="radio"/> DES <input type="radio"/> RC4 <input type="radio"/> Rabbit <input type="radio"/> TripleDes 密码: <input type="text" value="misc"/> <input type="button" value="加密: >"/> <input type="button" value="解密: <"/>	<code>UZFsdGVhX18qyg4WuE7WfF wxKvgUrtJdaxb4G2dl.g00Tpp4Q70hau caZpwqP9jQz3BAf2zkCxlBONRz94A:</code>
---	--	---

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

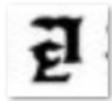


所以正确flag为flag{red_black_happy_bugku_y0000}

35.可爱的故事



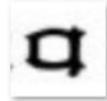
A



B



C



D



E



F



G



H



I



L



M



N



O



P



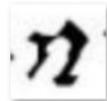
R



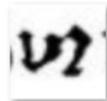
S



T



U



W



Y

https://blog.csdn.net/qq_35284897

翻译一下即可找到flag

36. easy_nbt

名称	修改日期	类型	大小
advancements	2020/12/14 15:45	文件夹	
data	2020/12/14 15:45	文件夹	
DIM1	2020/12/14 15:44	文件夹	
DIM-1	2020/12/14 15:44	文件夹	
playerdata	2020/12/14 15:55	文件夹	
region	2020/12/14 15:44	文件夹	
stats	2020/12/14 15:45	文件夹	
icon.png	2020/12/14 15:45	PNG 文件	4 KB
level.dat	2020/12/14 15:55	DAT 文件	2 KB
level.dat_old	2020/12/14 15:55	DAT_OLD 文件	2 KB
session.lock	2020/12/14 15:54	LOCK 文件	1 KB

NBT (二进制命名标签)

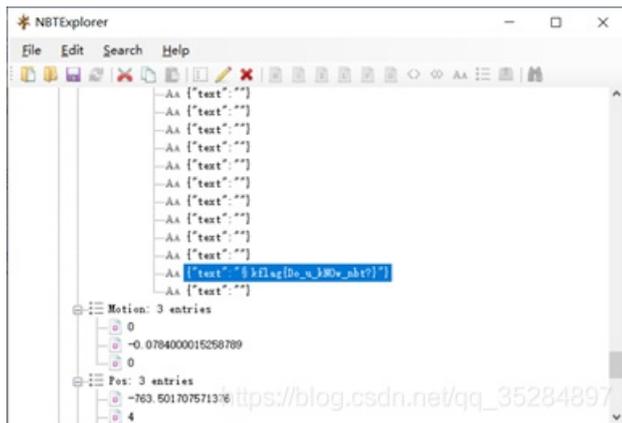
[编辑](#) [讨论](#) [上传视频](#)

本词条缺少概述图，补充相关内容使词条更完整，还能快速升级，赶紧来编辑吧！

我的世界二进制命名标签（Name Binary Tag），**NBT**格式为Minecraft中用于向文件中存储数据的一种存储格式，NBT格式以树形结构并配以许多标签的形式存储数据，所有的标签都有一个独立的ID和名称，最初版本如Minecraft Beta1.3中所示为19132个标签，但是随着铁砧的引入，增加了一个整形指针变量，标签数量增加至19133个。在NBT格式最初在Minecraft Indev的版本中只有0到10这11个标签可用。

<https://blog.csdn.net/Monuffer>

NBTEditor 打开level.dat 找一找，就找到了



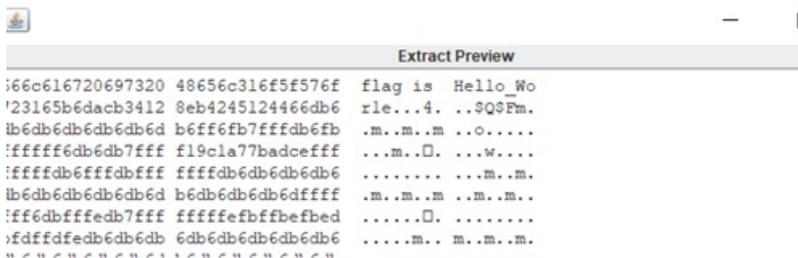
37.赛博朋克

zip伪加密

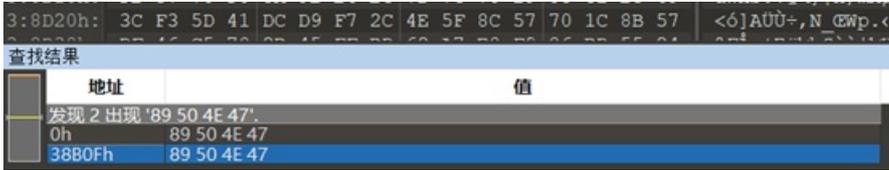
修复后解压得到txt文件，010分析发现是png文件，文件尾部有提示

Stegsolve打开，最低有效位提取

得到flag,注意格式1和要区分 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

名称	压缩后大小	原始大小	类型
code.txt	16,234	21,654	文本文档

再看kinglet.jpg，分离得到：

名称	修改日期	类型	大小
7225.7z	2021/6/3 22:41	WinRAR 压缩文件	2
9268	2021/6/3 22:41	文件	23
9268.zlib	2021/6/3 22:41	ZLIB 文件	1

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

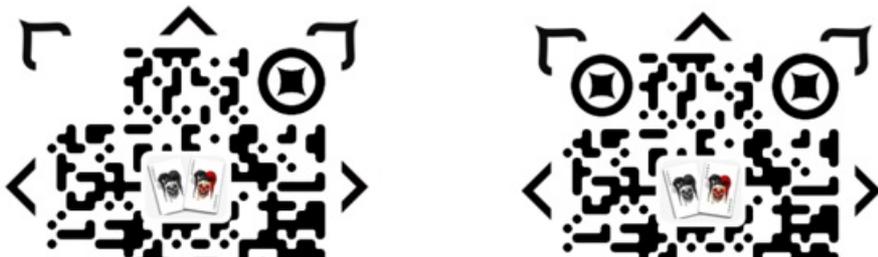
再看大王分离出得压缩包，尝试爆破无果后，尝试伪加密，成功解压得到code.txt

```
code.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAAMgAAAGQCAIAAABkLjnAAAAAXNSR0IArs4c6QAAAAARnQU1BAACxjww
8YQUAAAACjEhZcwAADsMAAA7DAcdvqGQAAD7zSURBVHhe7ZOJYBRF2v4zM7kPgcSkCtcAcJ9h8jlgbjquuB8OmQ
+1cEFgHlUEAI13qgyLXoeqAI7ifroJ+r4rt4gCDIKYsQzpbWbQJOCg9mfyfmxoJc3R3enq6eazT/jHGqppq6qrUz96qqe6x1BbW
+unoyM3Rvq/jo6s6MSUQRdWdQkoAtLRxF0Yekogi4sHUXQhaWjCLqwdBRBF5aOlujCOIEEXVg6iqALS0cRdGHpKlluLB1F0Iwlowi6s
HQURReWjilLowtJRBF1YooqgC0tHEXrh65iCLiwdRdCFpaMlurB0FEEXlo4i6MSUQRdWdQKYBWW2WzWn
+Cgly/GkpkSF//rX6dPn7ZYL5mo+Mxpla33PLCIC179+zp179/bFycwWCgd3R0PMD0y88/FxQUnd9//uiRI7379o3TtaUjB6bqykr8D
+PguXPnjmdm9uzVK6FpU/aejo5kTKYb9gnz97Nnz548cSK1W7dmzZqxRB0dadwUoFC2crKzs06f7k1a7PERErV0XEFB2EBaCv7jWUUI
TEpCRK1dFxE2dhgVo/vzNZWTBdHT1Stk1pSMJDMExoK2zOTkdO3ZMat6cknR0RMMRLIDJFrTvoVOn5rq2dNxE5FggC3YrOxvagt0S
yqej44p1ixs9l9xRppUm4upTkCbWVnZbG5vO471RGJafq0a59Mn96te/cTx49fvHirKh3BOvHUqVNdunZNTeZUtdWwqK6uttRYTCYT
xdXCTHHJRpiili1bjicnW7V14QK94wgmW3g3tVu3ps2a6dpqEFy6dOnzTZ9//933sXGx8fHxIKoaFou1kZVvdV3W7cO6t8/wGdgfAUZUJ
MHDz6wf39NTQ0roqNBysvLf/rpp5deemn4sOFtW7ed9OdJRYVf9J6KWD2idcBsQtpAwY4SaruFWQypQ8adODAAV1bEsBnmIHzDHA
OKS6aWjCqOtmBQyz2Zydnb36r6vv//39Xbt0bda0WUR4RKeOnf7xj39QEXVx/pEm9Hbbjz+
+Mnv2nl9+oSRHMF36dNnXerVqamp6o/cDRRC9dylLudu3b9+1a9eZ7DPXCq5hAgIDAgNCQ0Cw0Jxv9CQ0Lw/
+DgoGAQFBwUFBIED0yfv7+/OWg02f4ZDda9mbhquFLVSurKisrSstKioqlzZ84c
+vXQ1atX4uLoTN23Lvvvvt5W83TFDCrgK0X/9C53784QdhhfXq1WvVO
+9gyqVr5xhc/rNnz65z2bz5sLCgowTsFW1V14zFYZ0A0Ug391URbws/2zBmyZWak6rJbhhGsqrb+ozdsxMTETJ8+ffyE8RRXF
+6fIUPI99/P3f0Fn927YkR/xNph49e0JbWE7q2uKjRkzsp//5z8KFC3OycyoqKihVldL50pawWN6+fxuKqww3zRT4cAwfMWLe/Pn9Bg
ygJEFMNTUHDX4cP27cr7/
+ig8lperYUUVJSnbt2snPTz5x/IT6qsLA2n9Af2+pCgjdPtpitsy5s/vP2CAqxEG0NOvBw9fO405KkZotuswoKQtm7csmL8gPz
+fc0xQmuTk5FF3jaKIN6jn9oy2q3+vfHqE9JdkBbBw8ceH7ixH379unaqgOn5cD
+A/Pnz79+/TolqU7Hjh379e9HEW9Qj7AA01bffb0451LQ0769e6c+//yePXt0bTgwLlu
+fPnly5e9YqsA1pi33HILRbyEad68eRTkp23btq1atTp58mRubi7nybpw4cLRI0dS0ndu3rw557ZelC5+vHHYGsStvNBE4EBATEx8e3bN
UyK5JgdjYWKzdoeKimiRpeHERER4eDk0w100QjCDAQBQB+FDQf3+smigA8C7OtuvnOswsbOiwOQMHDq54N3Djx8a//
+67jLiz9+7ZYzabKcmRAQMHLn711UFpaZjZiMBenruuee++OcXrncJ0kIPIT7//77r79OgRtCQCOSvKbfeqKsrlX 35224897
```

很明显得base64转图片，在线工具转一下<https://tool.jsuapi.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





https://blog.csdn.net/vqq_45284897

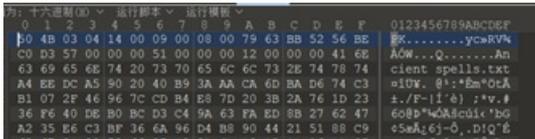
扫码得到 key{P0ke_Paper}

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

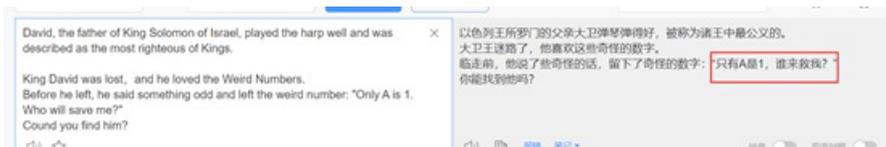
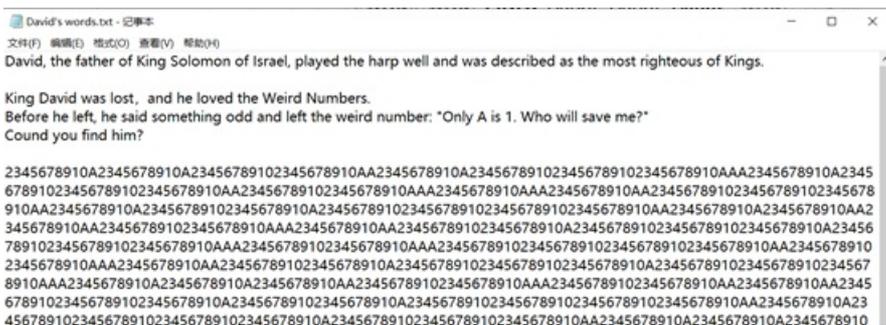


修改后缀，解压发现是加密压缩包

寻找解压密码

其他图片暂未看出什么异样

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



SGFwcHkgdG8gdGVsbCB5b3Uga2V5IGlzIEtleXtPTUdfWW91ZG9pdH0=

附代码

```

str = '010100110100011101000110011101110110001101001000011010110110011101100100010001110011100001100111011001000
10001110101011001110011011000100100001101000010001101010110001000110011010101011001110110000100110010010101100
0110101010010010100011101101100011110100100100101000101011101000110110001100101010110000111010001010000010101000
1010101011001000110011001010111010101110011100100110001010110100100011100111001011100000110010001001000001100000
0111101'
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



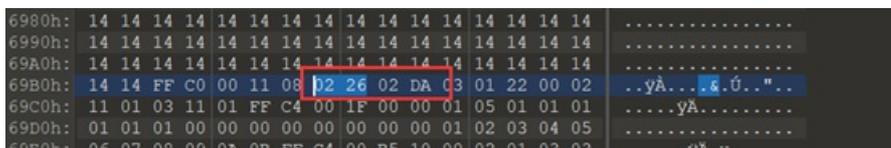
要修好它，得到的flag还是反向的

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里搜索老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



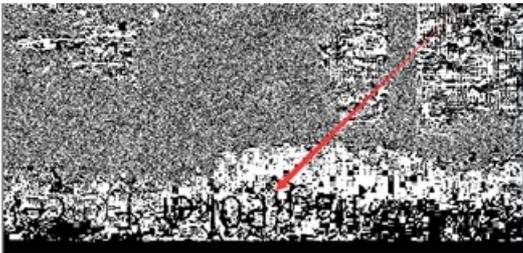
修改高度

得到

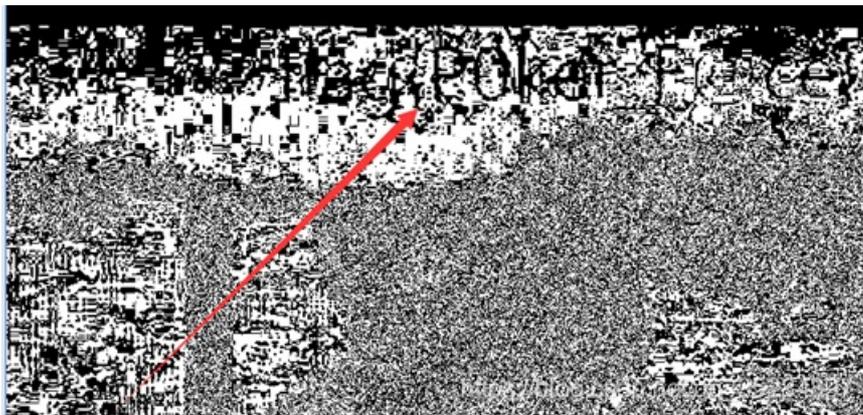




不规则的地方。应该藏有东西
Stegsolve跑一下



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

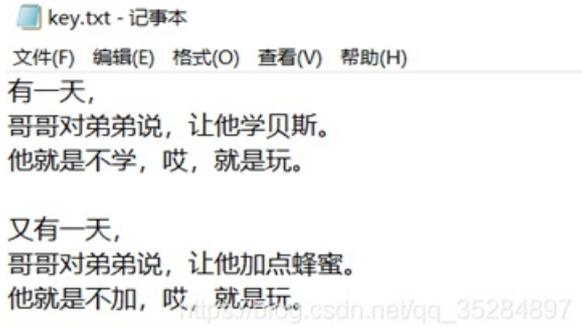
key	2021/5/25 11:10	文件	41 KB
画X的既不是黑也不是白.zip	2021/5/25 11:01	ZIP 压缩文件	3 KB

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

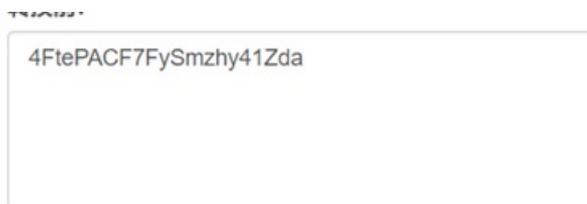


多番尝试，在文件属性发现

属性	值
说明	
标题	我的贝斯好像掉了6颗螺丝
主题	
分级	☆☆☆☆

镜头制造商	
镜头型号	
闪光灯制造商	4FtePACF7FySmzhy41Zda
闪光灯型号	

Base64掉了6颗螺丝，base58，

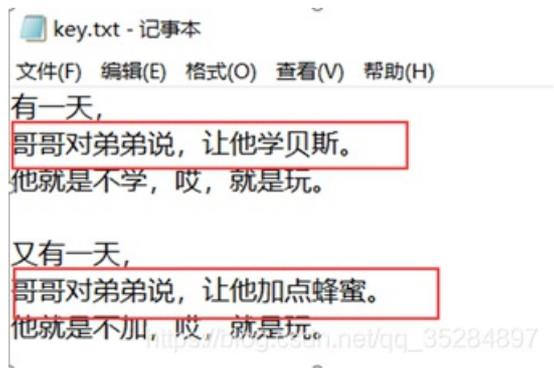


编码Base58> 解码Base58>

转换后:

thisisawrongkey
https://blog.csdn.net/qq_35284897

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

4FtePACF7FySmzhy41Zda

编码Base58> 解码Base58>

转换后:

4DSXTA3yFHGib83QejmSdsnLRNDfn
https://blog.csdn.net/qq_35284897

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

一进制转字符串得到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



这逼装的

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

```
abcdefghijklmnopqrstuvwxyz
```

编码

解码

复制结果



HTTP	FILENAME	SIZE	EXTENSION
我说这个东西没你信吗? .zip	2021/6/7 19:16	ZIP 压缩文件	127 KB
我说这就是一个word你信吗? .rar	2021/6/9 10:46	RAR 压缩文件	12 KB

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**



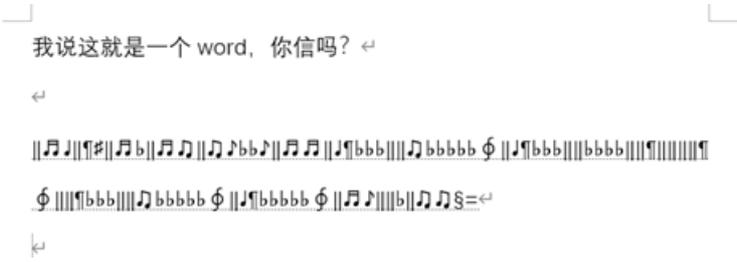
错的key

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/wenbenjiامي.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



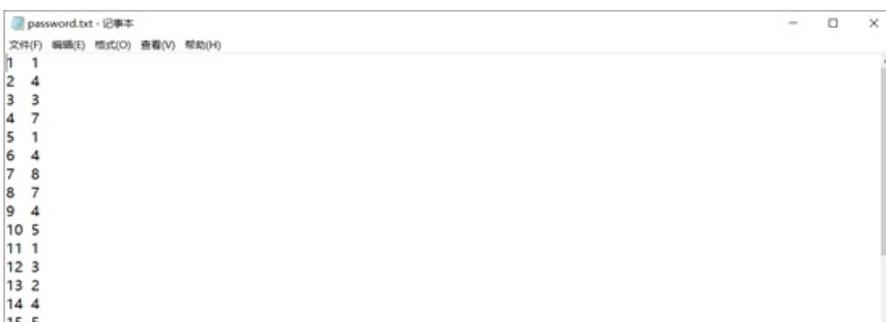
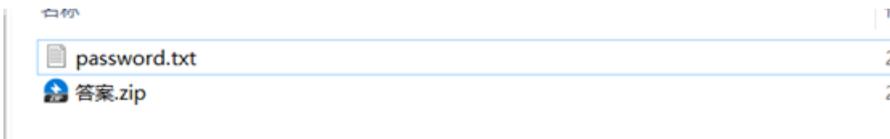
与佛论禅解密

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



```
16 2
17 5
18 3
36 1
38 3
40 5
42 7
44 9
```

在password.txt底部，发现tip

```
password.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

tip:
#####
##你听过《青花》吗?##
#####
```

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

大家好，我是时间财富网智能客服时间君，上述问题将由我为大家进行解答。以微信为例，其filestorage文件夹可以删除，但不建议删除，因为微信目录中的FileStorage文件夹是用来保存接收文件和图片的文件夹，如果您将文件夹中的文件全部删除的话，那么在微信App中将无法查看图片或者视频。

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'
```

Address	Size	Permissions	Path
0x000000027e7a300	16	0 R--r--	\Device\HarddiskVolume1\Users\IEUser\AppData\Local\Temp\1623897562.jpg
0x00000003d0a42f0	16	0 R--r--	\Device\HarddiskVolume1\Program Files (x86)\Tencent\QQ\Bin\xpng_dll.dll
0x00000003d0e0070	16	0 R--r--	\Device\HarddiskVolume1\Users\IEUser\Documents\WeChat Files\ALL Users\3213b982b11987a3460c2bde6fa08870.jpg
0x00000003da55070	15	0 R--r--	\Device\HarddiskVolume1\Users\IEUser\Documents\Tencent Files\54297198\ImageGroup2\Q\OT\OX07L7I0\HMJIN-GN7(3\Y0.gif
0x00000003da69e80	16	0 R--r--	\Device\HarddiskVolume1\Users\IEUser\AppData\Roaming\Tencent\QQ\Misc\ClientType\Phone14.png
0x00000003db64c20	16	0 R--rw-	\Device\HarddiskVolume1\Program Files (x86)\Tencent\QQ\Bin\xpng_dll.dll
0x00000003de18be0	15	0 R--rwd	\Device\HarddiskVolume1\Windows\System32\pngfilt.dll
0x00000003df7a800	14	0 R--rwd	\Device\HarddiskVolume1\Windows\System32\pngfilt.dll
0x00000003e1a5dd0	15	0 R--r--	\Device\HarddiskVolume1\ProgramData\Microsoft\User Account Pictures\user.bmp
0x00000003fcb1e20	4	0 R--r--	\Device\HarddiskVolume1\Users\IEUser\AppData\Local\Temp\8GInfo.bmp
0x00000003fe5d070	16	0 R--r--	\Device\HarddiskVolume1\Users\IEUser\Documents\WeChat Files\ALL Users\8aa9cc51622dae7d755c3b00deec0a5.jpg
0x00000003fe84070	8	0 R--r-d	\Device\HarddiskVolume1\Program Files (x86)\Tencent\QQ\Bin\libpng.dll
0x00000003fe84a30	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/Desktop
```

```
Volatility Foundation Volatility Framework 2.6
```

```
DataSectionObject 0x27e7a300 None \Device\HarddiskVolume1\Users\IEUser\AppData\Local\Temp\1623897562.jpg
```



密码是：Q1Da1A1qINGDeT0KeI1

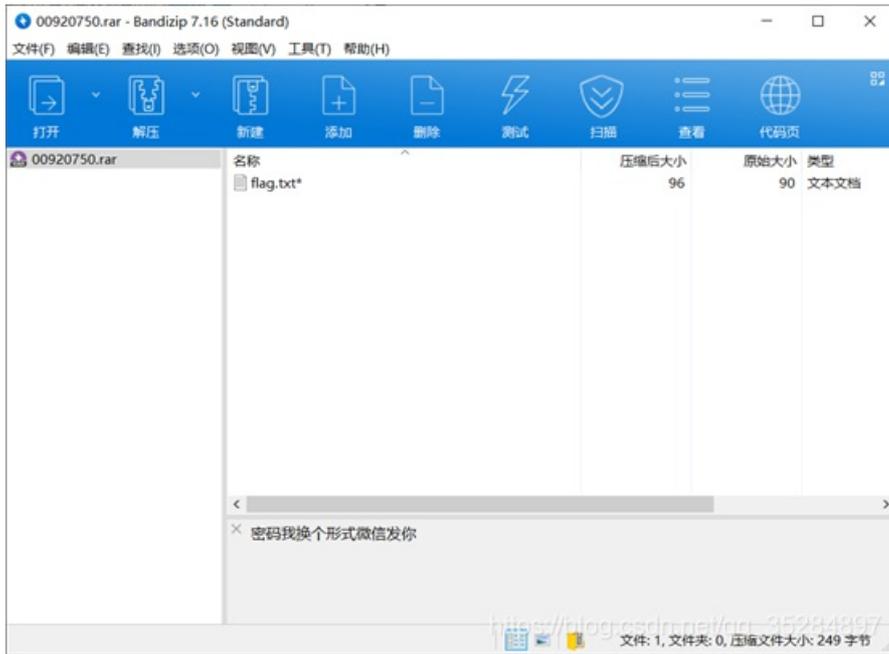
得到jpg文件，有个密码，尝试jpg的几种隐写，无果，那可能是压缩包的密码了
 filescaan压缩包zip rar
 发现疑似flag的压缩包f16g.rar

```
root@kali:~# volatility -f '/root/Desktop/win7.vmem' --profile=Win7SP1x64 filescaan | grep -E "rar"
Volatility Foundation Volatility Framework 2.6
0x0000000033b54c0 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

avi	2021/6/19 10:34	文件夹
bmp	2021/6/19 10:34	文件夹
dll	2021/6/19 10:34	文件夹
doc	2021/6/19 10:33	文件夹
docx	2021/6/19 10:33	文件夹
exe	2021/6/19 10:34	文件夹
gif	2021/6/19 10:34	文件夹
htm	2021/6/19 10:34	文件夹
jar	2021/6/19 10:33	文件夹
jpg	2021/6/19 10:34	文件夹
mbd	2021/6/19 10:33	文件夹
mov	2021/6/19 10:33	文件夹
mp4	2021/6/19 10:33	文件夹
mpg	2021/6/19 10:33	文件夹
ole	2021/6/19 10:34	文件夹
pdf	2021/6/19 10:34	文件夹
png	2021/6/19 10:34	文件夹
ppt	2021/6/19 10:33	文件夹
pptx	2021/6/19 10:33	文件夹
rar	2021/6/19 10:35	文件夹
rif	2021/6/19 10:33	文件夹
sdw	2021/6/19 10:33	文件夹
sx	2021/6/19 10:33	文件夹
sxc	2021/6/19 10:33	文件夹
sxi	2021/6/19 10:33	文件夹
...

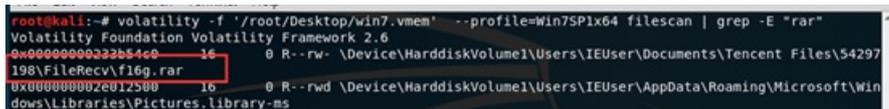
找到rar



用上图密码解压，得到flag.txt

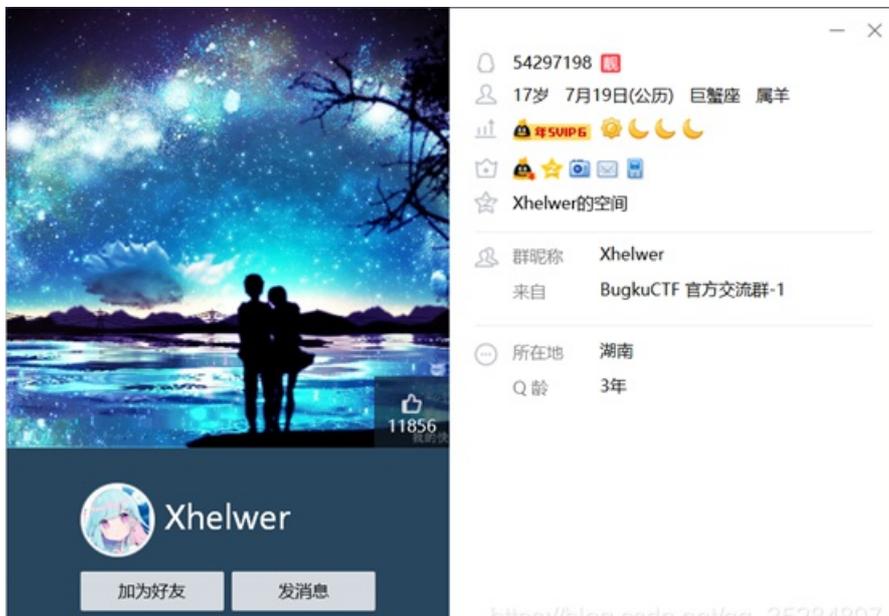


qqnumber即为54297198(第一次还试了试Tokeii师傅的QQ.....hhh)



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

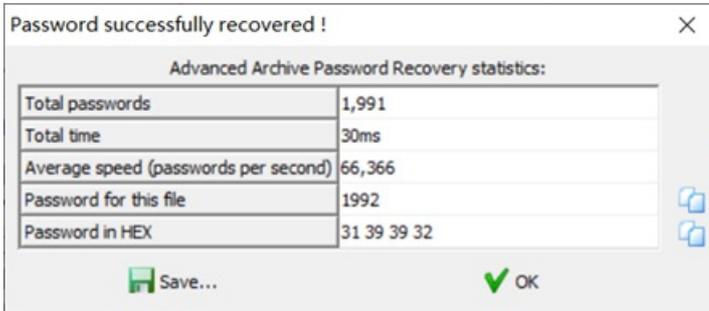
加压的png图片，修改高度得flag



BUGKU{a1e5aSA}

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



flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
5+58==327a6c4304ad5938eaf0efb6cc3e53dcCFmZknmK3SDEcMEue1wrsJdqqt7dXLuS

5+58为md5+base58



CFmZknmK3SDEcMEue1wrsJdqqt7dXLuS

编码Base58> 解码Base58>

转换后:

{this_is_md5_and_base58}
http://www.bug-cs9n.net/qq_35284897