Bugku—MISC题总结

原创

Sn0w/ 于 2019-06-15 18:59:38 发布 2792 收藏 27

分类专栏： CTF_Writeup 文章标签： Bugku MISC

本文链接：https://blog.csdn.net/qq_43431158/article/details/91400662

前言：MISC考脑洞，也考分析和观察能力，总之比较有趣，就总结一下我的做题过程。

这是一张单纯的图片

用winhex打开

```
640  1D 64 06 8A 28 03 D0 A8  A2 8A 00 28 A2 8A 00 28   d Š( Ð¨¢Š (¢Š (
650  A2 8A 00 FF 26 23 31 30  37 3B 26 23 31 30 31 3B  ¢Š ÿ&#107;&#101;
660  26 23 31 32 31 3B 26 23  31 32 33 3B 26 23 31 32  &#121;&#123;&#12
670  31 3B 26 23 31 31 31 3B  26 23 31 31 37 3B 26 23  1;&#111;&#117;&#
680  33 32 3B 26 23 39 37 3B  26 23 31 31 34 3B 26 23  32;&#97;&#114;&#
690  31 30 31 3B 26 23 33 32  3B 26 23 31 31 34 3B 26  101;&#32;&#114;&
6A0  23 31 30 35 3B 26 23 31  30 33 3B 26 23 31 30 34  #105;&#103;&#104
6B0  3B 26 23 31 31 36 3B 26  23 31 32 35 3B D9 D9      ;&#116;&#125;ÙÙ
```

Unicode编码转换ASCII即可得出flag

隐写

:	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG IHDR
10	00	00	01	F4	00	00	01	A4	08	06	00	00	00	CB	D6	DF	ô ¤ ËÖß
20	8A	00	00	00	09	70	48	59	73	00	00	12	74	00	00	12	Š pHYs t

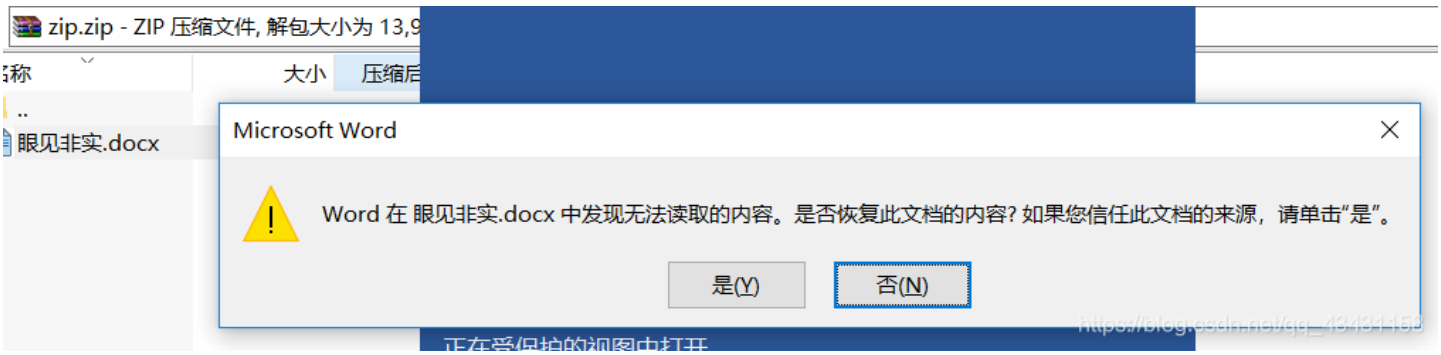
前四位是宽度，后四位是高度。将`A4修改位F4`即可得出flag

telnet

winhex打开就可得出flag

```
17 46 01 D4   À¨Ý€À¨Ý¤ z  F Ô
00 66 6C 61  Nhð*zP   <·  fla
31 62 66 39  g{d316759c281bf9
34 39 37 33  25d600be698a4973
00 00 00 3C  d5}     >¦  <   <
```

眼见非实(ISCCCTF)



下载之后打不开，根据提示眼见非实，将`docx文件改成zip文件`


```
- <w:r>
    <w:t>在这里呦！</w:t>
  </w:r>
</w:p>
<w:p w:rsidRDefault="002B3D8D" w:rsidR="002B3D8D" w:rsidRPr="C
- <w:pPr>
  - <w:rPr>
      <w:rFonts w:hint="eastAsia"/>
      <w:vanish/>
    </w:rPr>
  </w:pPr>
- <w:r w:rsidRPr="002B3D8D">
  - <w:rPr>
      <w:vanish/>
    </w:rPr>
    <w:t>flag{F1@g}</w:t>
  </w:r>
```


即可得出flag

啊哒

用winhex打开，发现隐藏有zip文件，用binwalk进行分离

得到一个加密文本，开始以为是伪加密，但用winhex打开后查看不是伪加密，因为不知道是否含字符、或是几位数，所以暴力破解也是不可取的，回去查看第一张照片，应该还隐藏有信息。

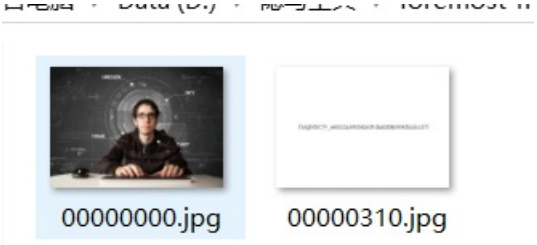
照相机型号 73646E6973635F32303138

果然藏有东西，base16解码即可得出密码`sdnisc_2018`，打开文本即可得出flag

又一张图片，还单纯吗

第一反应便是winhex打开，结果也没有发现什么，用binwalk分离也分离不出来，但确实能看出里面隐藏有文件。这里就需要一个新的工具`foremost-master`分离工具。
输入命令，提取出文件，即可得出flag

```
$ foremost -T 2.jpg
Processing: 2.jpg
|*|
```



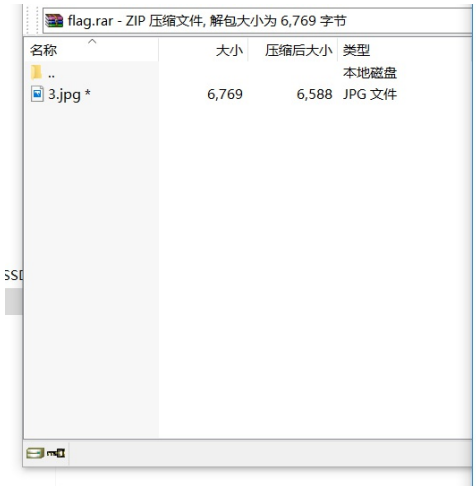
猜
百度识图，直接可以识别是谁，至于flag提示中有

隐写2

winhex查看

```
E 7F  mjàÜÿtyîÿŽÿ ÿ;þ
0 08   »¶Æþ PK   ?
C 1A     8~nK³F÷NL    L
0 00       $
0 00       flag.rar
3 01             /"$ ]Ó
3 01  U   $ ]Ó U   $ ]Ó
E 4B  PK   ?        ø}nK
4 00  †\ Î Y   äh     $
```

binwalk进行分离



告诉你们一个秘密，密码是3个数哦。

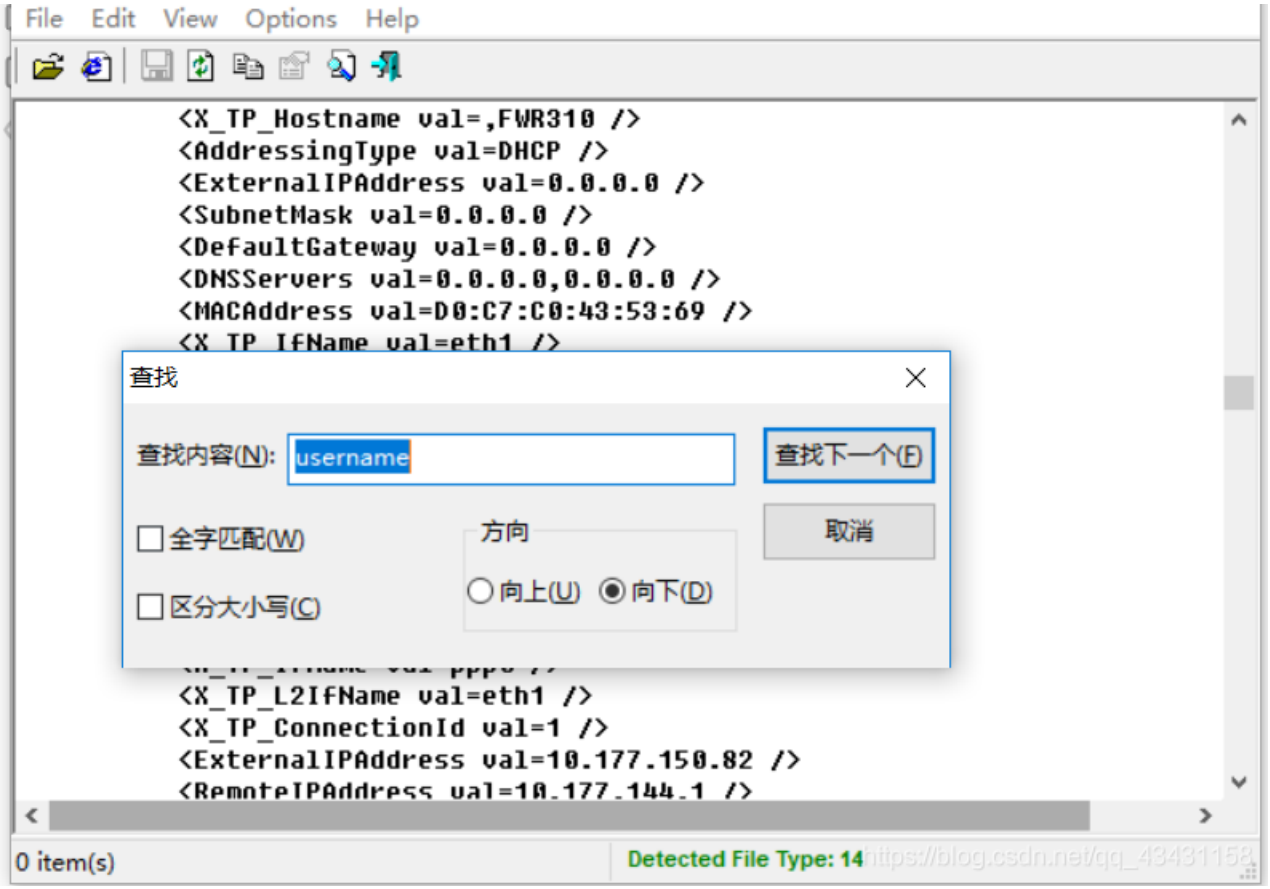
查理曼：
查理曼，法兰克王国国王，征服了西欧与中欧大部分土地，具有了至高无上的权威，下令全国人民信仰基督教，查理重振了西罗马帝国。
雅典娜：
女神帕拉斯·雅典娜，是希腊神话中的女战神也是智慧女神，雅典是以她命名的。
兰斯洛特，
英格兰传说中的人物，是亚瑟王圆桌骑士团中的一员。看上去就是一个清秀年轻的帅小伙儿，由于传说中他是一名出色的箭手，因此梅花J手持箭支。兰斯洛特与王后的恋爱导致了他与亚瑟王之间的战争。
Hint:

其实斗地主挺好玩的。

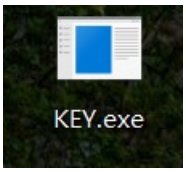
分离出一个加密的图片，和一个提示，既然都告诉我们了密码是3个数，直接暴力破解密码为`871`，即可得出flag

宽带信息泄露

一开始各种方法都试过，实在没思路，回去看题目，**宽带信息泄露**，用文本打开是乱码，说明被加密了，这里就需要一个工具`RouterPassView`来帮助做题了
又提示`flag{宽带用户名}`，打开工具直接查找username，即可得出flag。



多种方法解决



用winhex打开后，发现是base64转图片的格式，在线转图片，即可得出flag

闪的好快

得出一个gif二维码，用神器**Stegsolve**即可得出18张二维码图片，扫码即可得出flag

白哥的鸽子

一开始用winhex打开，没有注意到末尾，尝试了其他方法不行才发现末尾的重要信息。

```
2FD0  74 F7 4B 65 B0 58 2F 01  3A 92 BF 1E 73 2A C7 49  t÷Ke°X/ :'¿ s*ÇI
2FE0  E6 03 A7 9D 14 11 1D 79  D0 9D 28 0E A5 1D 40 20  æ §    yÐ ( ¥ @
2FF0  78 DC 59 69 DA 8F 64 6E  E6 7B A3 57 31 EE 8D DC  xÜYiÚ dnæ{£W1î Ü
3000  CB 62 45 62 89 EE 5B DC  B6 73 01 E3 FF D9 66 67  ËbEb‰î[Ü¶s ãÿÙfg
3010  32 69 76 79 6F 7D 6C 7B  32 73 33 5F 6F 40 61 77  2ivyo}l{2s3_o@aw
3020  5F 5F 72 63 6C 40                                 __rcl@
```

这里可以看到`flag`只是顺序被打乱了，**栅栏加密**，解密即可得出flag

`flag`需去除两个@

隐写3

这道题要敏感，大白怎么可能光一个头，所以应该是改图片的宽高，即可得出flag

```
89 50 4E 47 0D 0A 1A 0A  00 00 00 0D 49 48 44 52  %PNG        IHDR
00 00 02 A7 00 00 02 A7  08 06 00 00 00 6D 7C 71     §   §      m|q
35 00 00 00 01 73 52 47  42 00 AE CE 1C E9 00 00  5    sRGB ®Î é
```

这样才可爱

爆照(08067CTF)

下载图片，用winhex打开后发现隐藏有zip文件，binwalk进行分离。

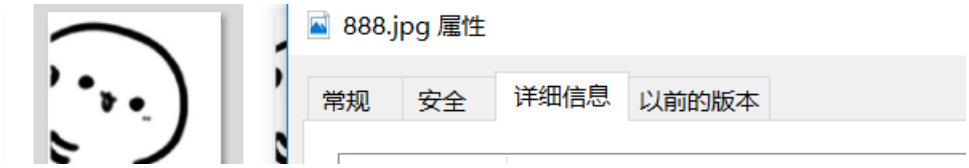
..	本地磁盘				
8	92,278	8,362	文件	2017/10/28 1:...	08B388EA
88	15,739	14,906	文件	2017/10/28 1...	A756F515
888	18,479	11,129	文件	2017/10/28 1:...	76D00172
8888	11,782	10,371	文件	2017/10/28 2:...	06601D...
88888	92,278	6,945	文件	2017/10/28 1:...	42B9AAFB
888888	92,278	6,824	文件	2017/10/28 1:...	1AC014...
8888888	92,278	7,076	文件	2017/10/28 1:...	6F836171
88888888	92,278	8,219	文件	2017/10/28 1:...	2BDC3B31
愉快的排序吧哈...	58,893	52,997	GIF 文件	2017/10/28 1...	08F0DF8D

给了一堆文件，把后缀名改为jpg,看看能显示出什么

发现其中一个有二维码，扫出`bilibili`
再看题目提示答案格式

flag格式 flag{xxx_xxx_xxx}

我们应该还漏掉有其他答案，再回去查看图片

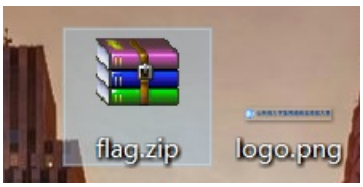


888.jpg发现base64，解密得出`silisili`
应该还有一个
在8888.jpg中发现隐藏有图片，binwalk一下即可

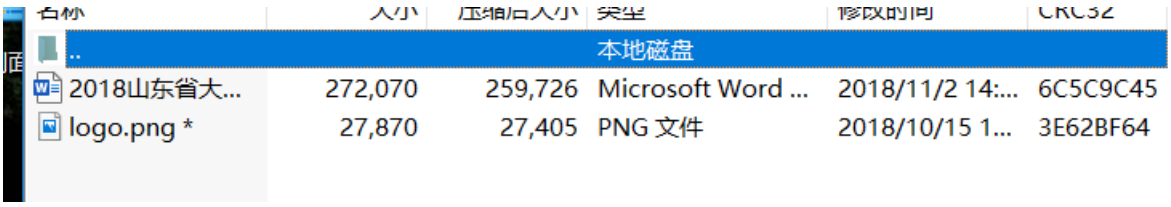
```
00002D70  E3 57 CC 85 AE A2 7B AE  68 C3 E3 BB D3 ED A3 12  ãWÌ…®¢{®hÃã»Óí£
00002D80  AA CA 6A 74 AD C0 F6 60  34 42 74 55 C3 A5 A1 FF  ªÊjt-Àö`4BtUÃ¥¡ÿ
00002D90  50 4B 01 02 3F 00 14 00  00 00 08 00 C9 0D 5C 4B  PK  ?        É \K
00002DA0  D9 3D 00 76 84 02 00 00  B2 04 00 00 0E 00 24 00  Ù= v„    ²       $
00002DB0  00 00 00 00 00 00 20 00  00 00 00 00 00 00 31 35                  15
00002DC0  30 39 31 32 36 33 36 38  2E 70 6E 67 0A 00 20 00  09126368.png
00002DD0  00 00 00 00 01 00 18 00  1C 14 54 7D 4B 4F D3 01              T}KOÓ
00002DE0  2C 60 39 7D 4B 4F D3 01  2C 60 39 7D 4B 4F D3 01  ,`9}KOÓ ,`9}KOÓ
00002DF0  50 4B 05 06 00 00 00 00  01 00 01 00 60 00 00 00  PK            `
00002E00  B0 02 00 00 00 00                                 °
```

得出`panama`
按照题目提示拼接成falg即可

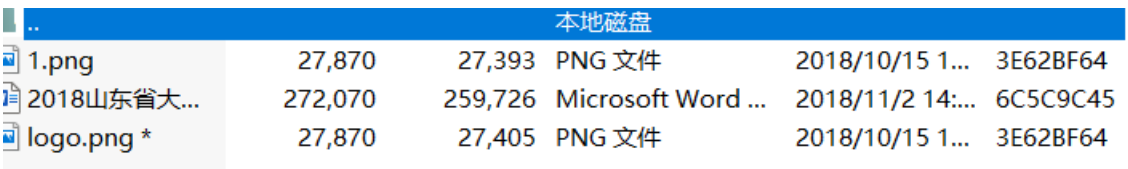
神秘的文件



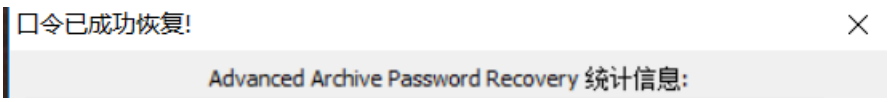
flag压缩包中还有一个logo图片

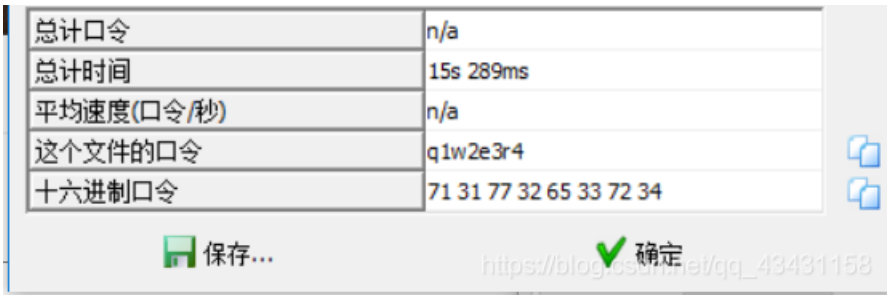


明文攻击，把外面的logo图片也压缩进flag压缩包中



接下来爆破口令



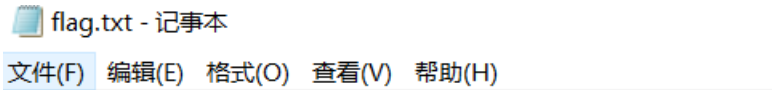


打开word

哪有什么 WriteUP，别想了，老老实实做题吧！

既然找不到flag，把你变成zip格式看看是否隐藏有

找到了

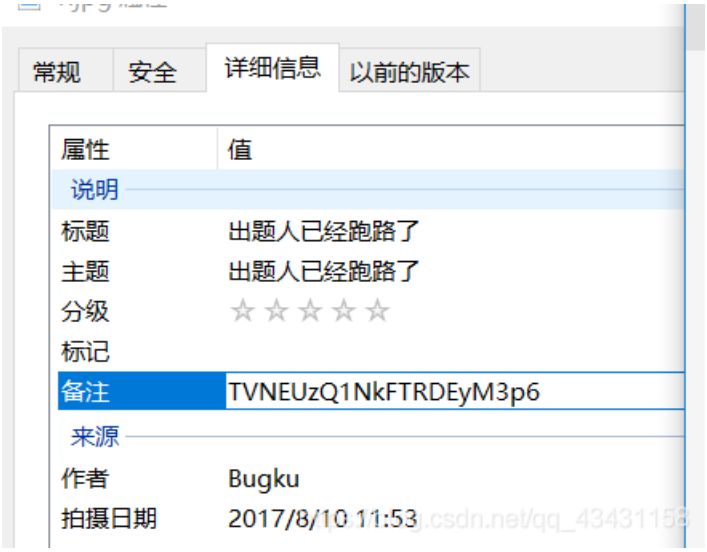


ZmxhZ3tkMGNYXzFzX3ppUF9maWxlfQ==

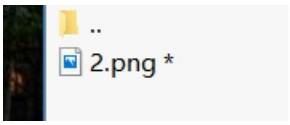
base64解密即可得出flag

细心的大象

细心的大象，要细心，看看照片详细信息隐藏有东西没



果然，这个又是`base64`加密的
接下来，把照片`binwalk`一下，出来一个压缩包，里面一个加密的图片

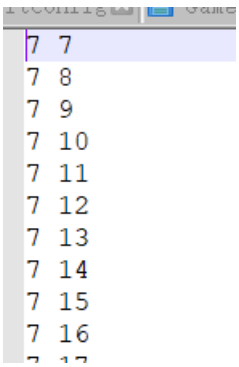


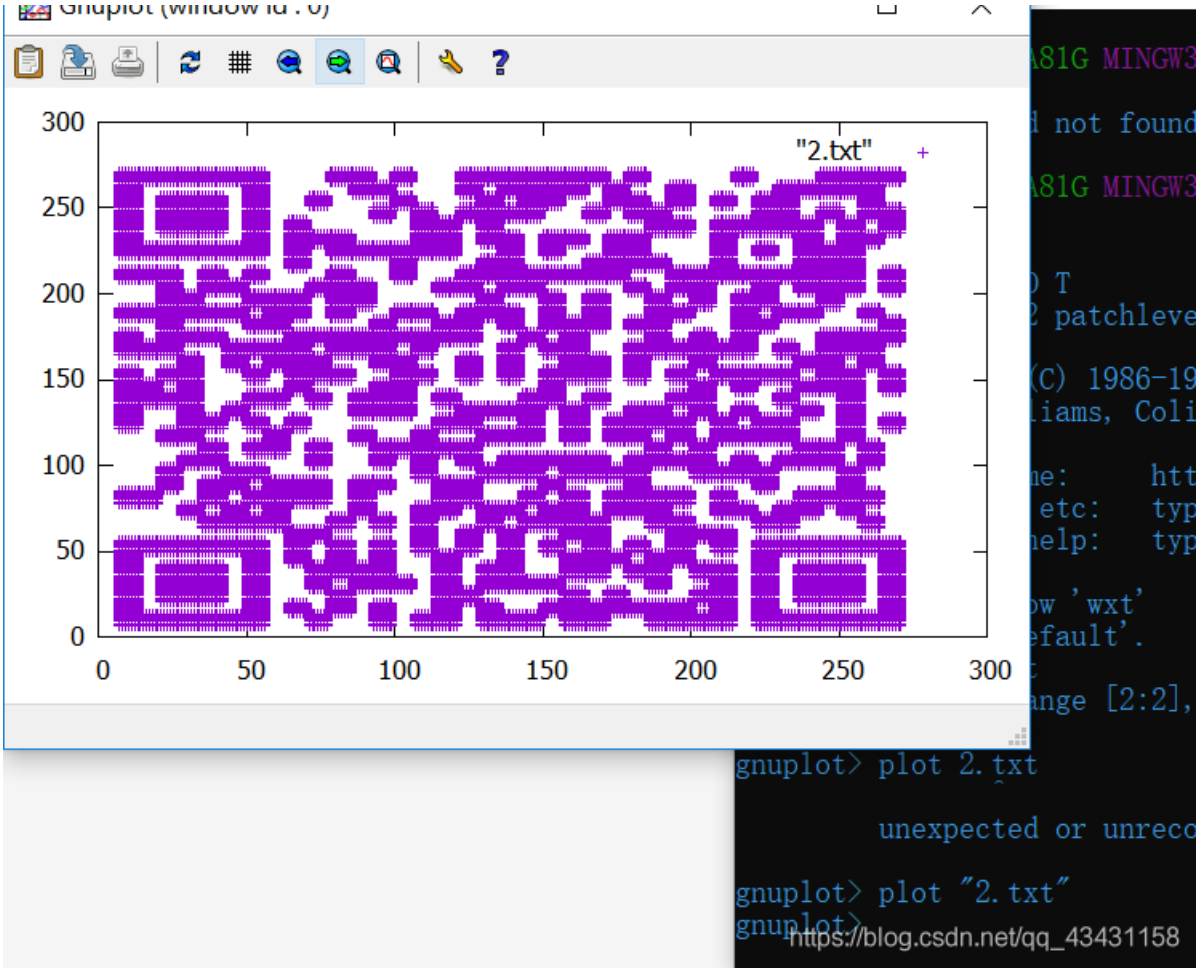
上面base64解密后的密码就是这个照片的密码

跟一开始遇到那道题一样，修改宽高即可得出flag

图穷匕见

之前做过这种题，打开winhex后发现一堆十六进制，在`notepad++`打开后转成ascll，再替换成相应的格式即可画图。





具体做法这里就不细说了，之前总结的也做过这个题。

这次就先总结到这里，另一部分的题写到下一篇博客中。