

CTF_论剑场 misc杂项 WriteUp (持续更新)

原创

[卤蛋啊](#) 于 2019-05-19 00:00:45 发布 8522 收藏 20

分类专栏: [CTF](#)

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_41995976/article/details/90296966

版权



[CTF 专栏收录该内容](#)

3 篇文章 1 订阅

订阅专栏

文章目录

[签到题](#)

[头像](#)

[0和1的故事](#)

[Snake](#)

[这个人真的很高](#)

[你能找到flag吗](#)

[向日葵](#)

[安慰的话语](#)

[画图](#)

[flag在不在这里](#)

[Blind](#)

[火眼金睛](#)

[被截获的电报](#)

[怀疑人生](#)

[500txt](#)

[c2un](#)

[easyzip](#)

[findme](#)

[小明的文件](#)

[二维码](#)

[春节三重礼](#)

[之后的再做了之后更新](#)

签到题

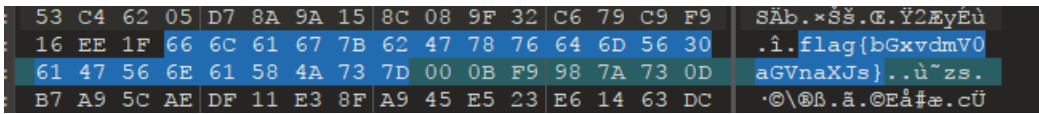
🔒 签到

作者: admin | 已解决: 358 | 一血: admin

签个到吧 flag{abcdABCD1234}

提交这里的flag即可

头像



下载图片 用010打开 找到flag的字符串

用base64转换

加密/解密 散列/哈希 **BASE64** 图片/BASE64转换

明文:

BASE64:

题目中说要用md5加密后 提交

Pass: unicode \$[HEX...]

Salt:

Hash:

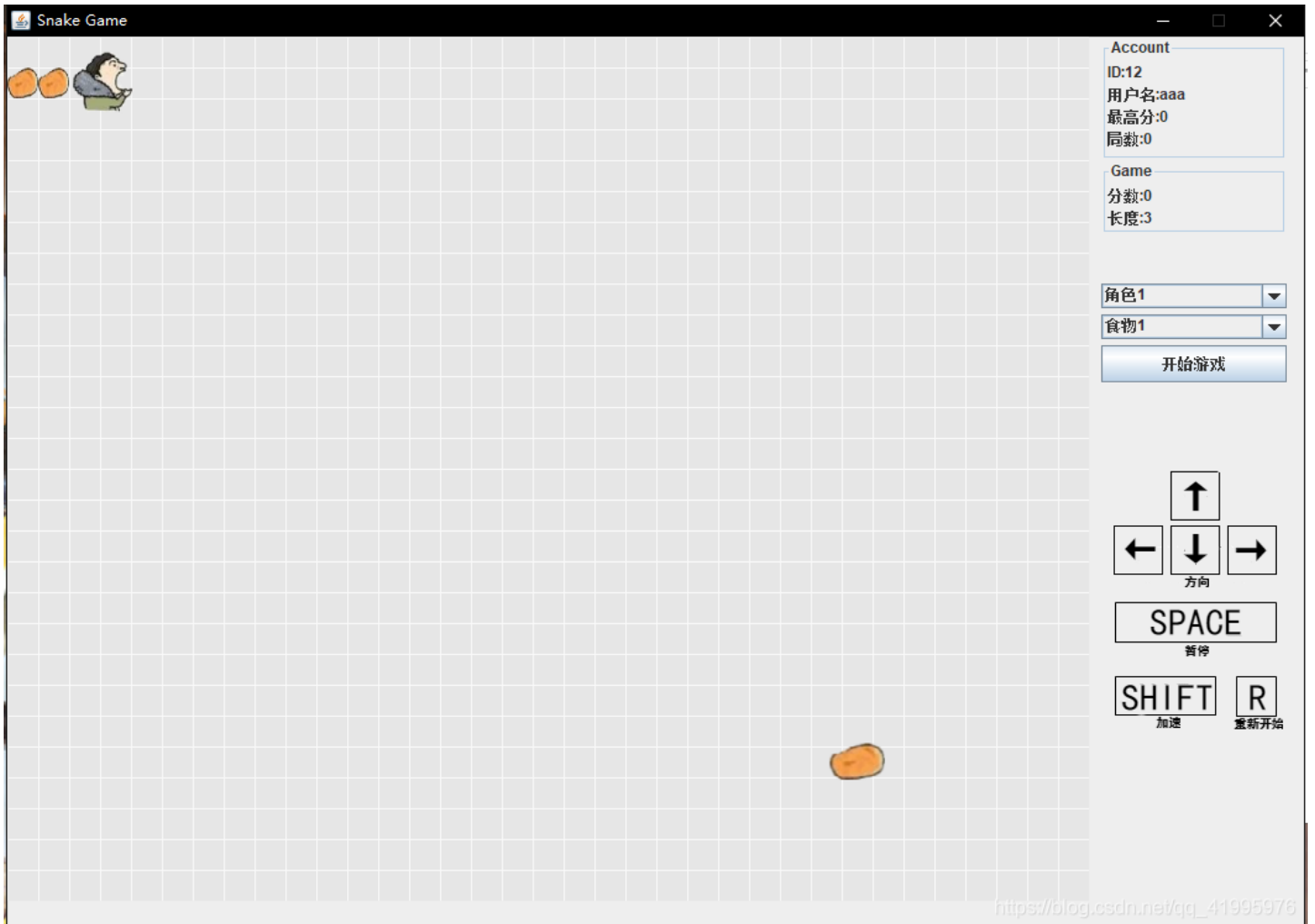
Result: md5: **8ba484e0a0e0a5ee4ffcb791385ddf25**

于是加密后再提交.....

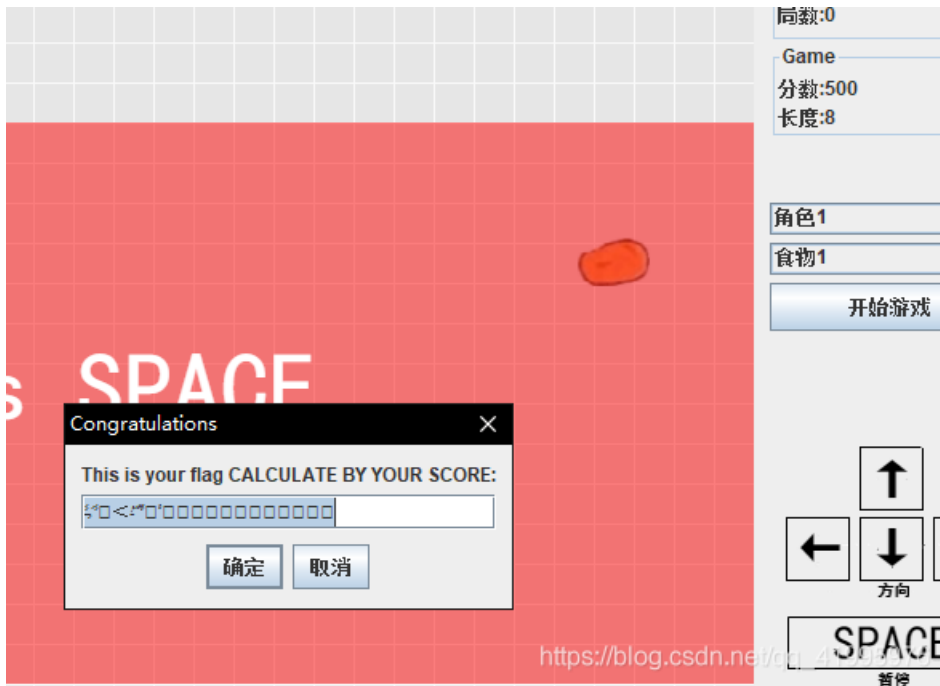
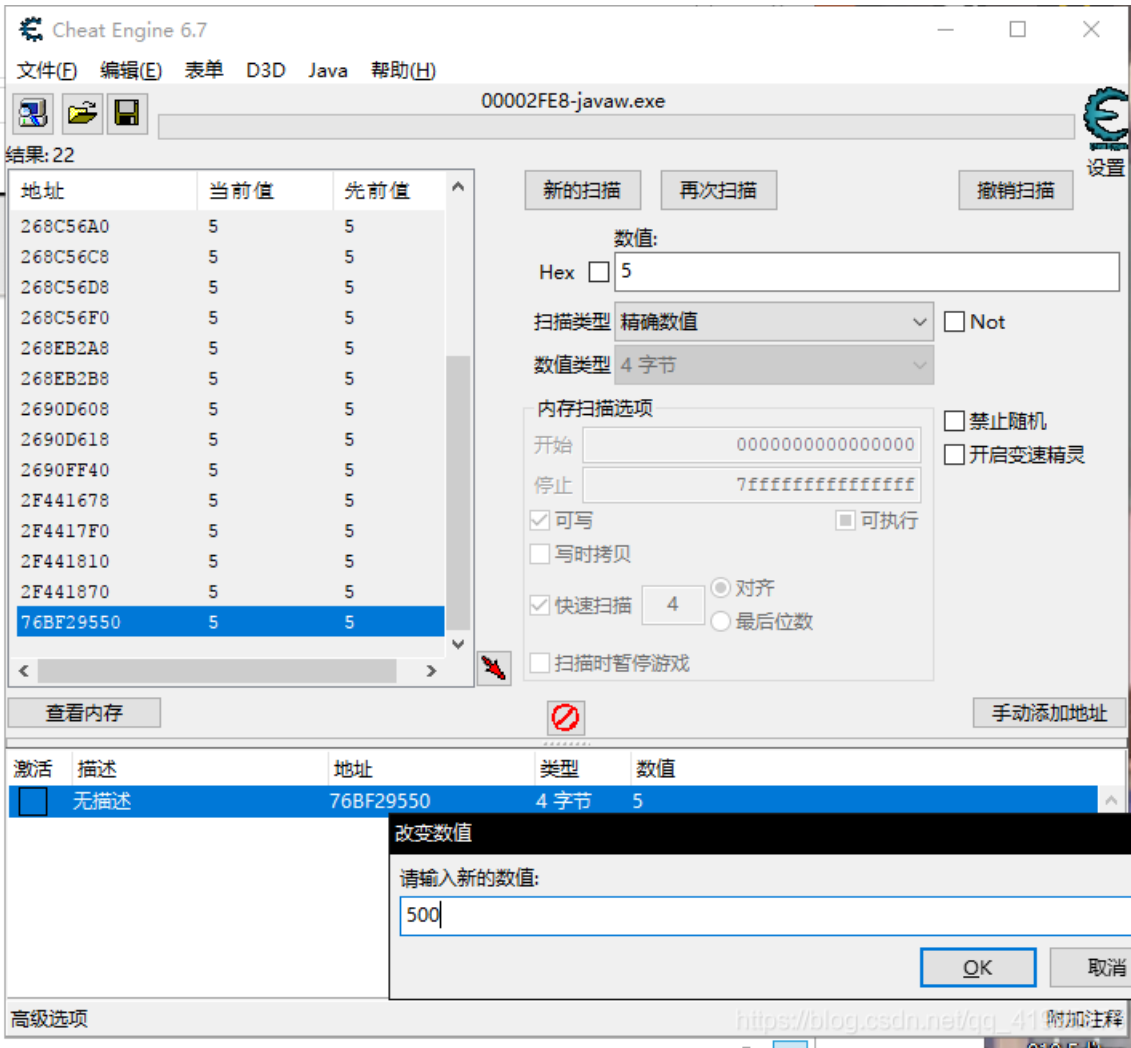
0和1的故事



登录后发现是一个贪吃蛇游戏 并且题千里说要攒够500分就可获得flag



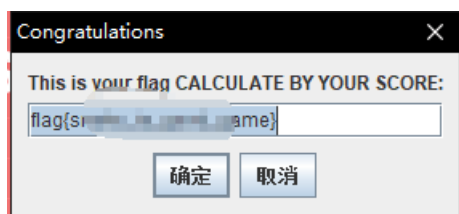
一开始思路是逆向工程 然后找flag 但是根据经验 (并且电脑里正好有CE 就使用CE来改分数了



但是发现改了分数之后的flag为乱码..... 于是又搞了一会儿 发现是长度的问题.....

于是把长度和分数一起修改：

激活	描述	地址	类型	数值
<input type="checkbox"/>	分数	76D084E60	4 字节	500
<input checked="" type="checkbox"/>	长度	76D0A7F24	4 字节	503



成功获得了flag

这个人真的很高

```
C:E820h: 91 66 C9 66 27 C0 BF 17 90 B3 FE FF B1 DE 1E FE  `fEf'Aç..°pÿ±B.p
C:E830h: 98 E5 07 F8 7F 4A 42 01 D7 D7 FD 4E 93 00 00 00  ~å.ø.JB.*xÿN^...
C:E840h: 00 49 45 4E 44 AE 42 60 82 0D 0A 0D 0A 0D 0A 0D  .IEND@B',.....
C:E850h: 0A 0D 0A 0D 0A 0D 0A 0D 0A 0D 0A 0D 0A 0D 0A 0D  .....
C:E860h: 0A 0D 0A 0D 0A 0D 0A 0D 0A 0D 0A 0D 0A 0D 0A 0D  .....
C:E870h: 0A 0D 0A 0D 0A 61 61 62 49 31 31 75 73 31 31 74  ....aabI1lus11t
C:E880h: 73 31 79 79 30 7D                                slyy0}
```

首先下载图片后用editor 010打开发现最后一串字符串
尝试补全提交之后没有成功

失败! 姿势不正确.

CHALLENGES

类型: misc

flag[aabl11us11ts1yy0}

Submit

然后题干中说的 这个人很高 可能是要修改图片的高度

struct PNG_CHUNK chunk[0]	IHDR (Critical, Pu...	8h	19h	Fg:	Bg:
uint32 length	13	8h	4h	Fg:	Bg:
union CTYPE type	IHDR	Ch	4h	Fg:	Bg:
uint32 ctype	49484452h	Ch	4h	Fg:	Bg:
char cname[4]	IHDR	Ch	4h	Fg:	Bg:
struct PNG_CHUNK_IHDR ihdr	499 x 800 (x8)	10h	Dh	Fg:	Bg:
uint32 width	499	10h	4h	Fg:	Bg:
uint32 height	800	14h	4h	Fg:	Bg:
ubyte bits	8	18h	1h	Fg:	Bg:
enum PNG_COLOR_SPAC...	AlphaTrueColor (6)	19h	1h	Fg:	Bg:
enum PNG_COMPR_MET...	Deflate (0)	1Ah	1h	Fg:	Bg:

于是修改后打开图片 发现另外一串字符串



于是又花了好久去想如何去组合 试了一会儿发现可能是栅栏密码
但是！！但是！！出来的最接近的组合是这样的

```
加密 解密 列半加密 列半解密 长度: 1 只列半元素四散的
密文框:
7栏:
firyIlyfus{llyoagalt0EaDaus}lnebsl@

8栏:
firyIly@fus{lly@oagalt0@EaDaus}@lnebsl@@

9栏:
flag{Iss0finDa111}oureally@Easybuty@

10栏:
flag{Iss0@finDa111}@oureally@@Easybuty@@

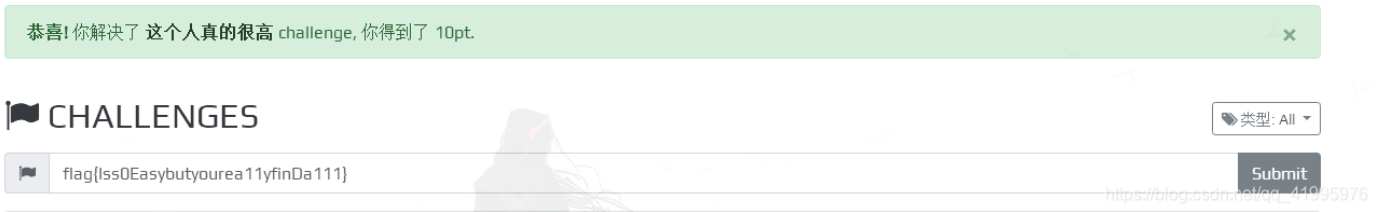
11栏:
flag{Iss0@@finDa111}@@oureally@@@Easybuty@@@

12栏:
fEungyalsty}flarD{blly@oiaseaIull0@

13栏:
```

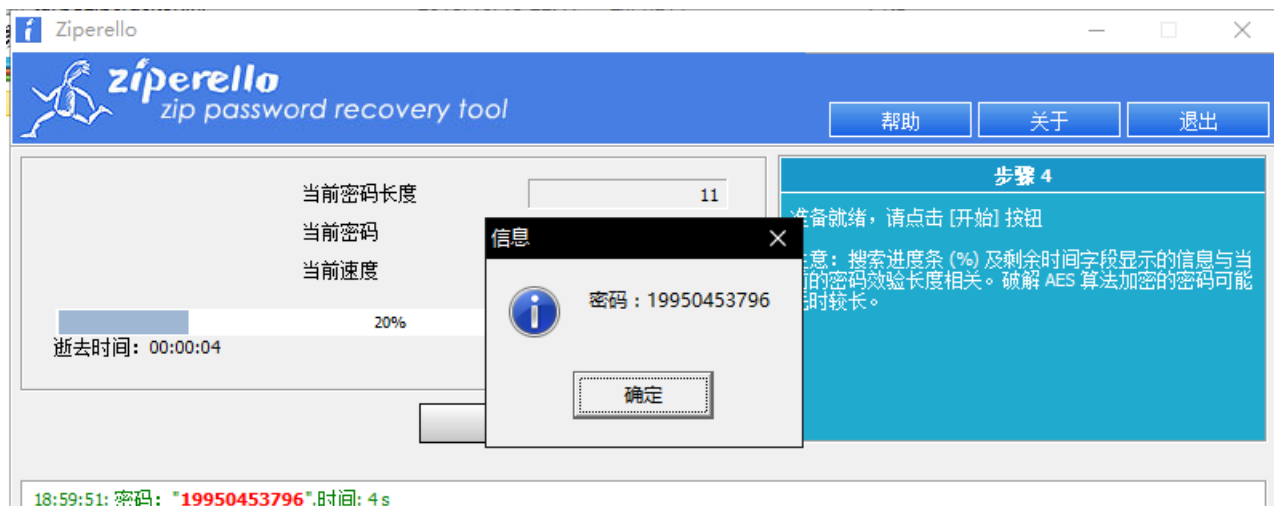
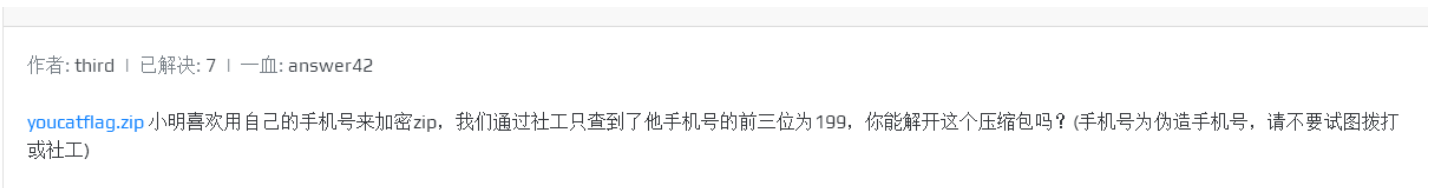
https://blog.csdn.net/qq_41995976

这几个提交了都不对 于是自己按照英语的词义改了位置 修改了文本 于是提交成功了（这谁受得住？）.....



你能找到flag吗

level1根据提示 暴力破解





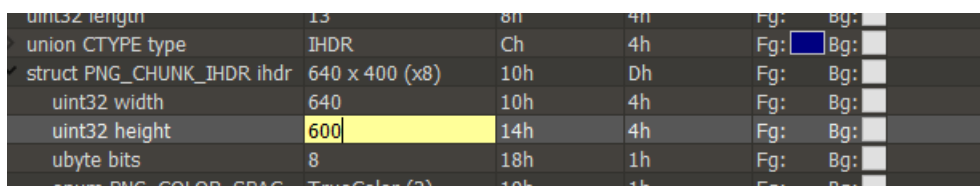
破解获得密码



level2的压缩包和第一个压缩包 有相同的文件 CRC32值 一样 可以用明文攻击



level3是伪加密 解开之后有个图片 修改宽度就可以得到flag了



flag{a8d9...24}

向日葵

图片最后有个RAR的文件

```
00033632 1E E1 B6 64 3C E0 9E 73 FD 6B B8 FF 00 97 F9 3E áq d<áz sýk.ý -ù>
00033648 82 B9 FD 6F FE 42 12 7F D7 25 FE B5 93 A9 26 D5 , 'yopB *%pu"e&ó
00033664 CD 62 67 4C 8B 6F FD 9D 0A 82 40 56 72 01 E7 97 íbgL<oy ,@Vr ç-
00033680 35 AB E2 66 1A 6A A6 98 55 E4 58 63 OD 23 A0 E4 5«áf j;"UäXc # ä
00033696 BB 72 46 3D B3 FA 56 5C 5F F2 12 D3 FF 00 EB 9A »rF="úV\_ò Óy èš
00033712 D6 F7 89 FF 00 E4 61 BC FF 00 AE 87 F9 54 C6 2A Ö-%y äa4y e+ùTÆ*
00033728 53 B3 FE B5 2D E8 9B F4 3C DE DE D1 2E E1 63 20 S'pu-è>ô<PpÑ.ác
00033744 05 83 64 0C E0 8A CF BE D3 C5 99 57 59 33 B8 FD fd àšÍ%ÓÁ"wy3.ý
00033760 D3 D6 BA 5B 9F F8 FB 93 FD FA E7 B5 AF F8 FE 1F ÓÖ°[ÿøú"ýúçp_øp
00033776 EE 8A ED A5 29 7B 4B 5F 42 22 4B 69 2C 86 01 92 išÍ%)(K_B"Ki,t '
00033792 49 07 B1 A2 9B 65 FE A0 FF 00 BD 45 39 45 5C 47 I t<e>ep ý %E9E\G
00033808 FF D9 52 61 72 21 1A 07 01 00 33 92 B5 E5 0A 01 ýÜRar! 3'pã
00033824 05 06 00 05 01 01 80 80 00 8E D0 B5 F7 23 02 03 e€ ŽĐp-#
00033840 0B 87 01 04 C2 01 20 C2 04 30 1C 80 03 00 07 36 + Å Å 0 e 6
00033856 36 36 2E 74 78 74 0A 03 02 17 1B 89 15 E5 98 D4 66.txt % ä"Ö
00033872 01 C5 1B 84 26 54 74 23 F6 70 34 BE 04 E2 6D 2E Å „&Tt#øp4% am.
00033888 C7 78 D4 25 OD 32 53 39 5E D3 22 35 22 A6 82 82 Çxô% 2S9^ó"5"!,,
00033904 2B A0 86 A0 BA 2A 2A 3C OD E0 2D 6B 46 FE 7F 90 + t °**< à-kFp
00033920 51 E3 59 47 8C CC F7 2C F8 FA FC A3 D9 EC CE 31 QäYg@i-,øúúšÜiîl
00033936 55 D4 3C 5C 17 F2 3F 5B 47 0C EE 53 32 7C 6C BE Uô<\ ò?[G iS2|1%
00033952 B4 52 89 E2 85 0F 94 B8 54 C4 B6 F7 EC 4F C2 50 'R%á... ",TÄq-ìOÄP
00033968 64 FF B8 OD 45 52 6B 4A C0 F1 97 80 E1 24 57 9E dÿ. ERkJÄf-éášWž
00033984 EA F4 A1 96 4A 2C D0 81 73 C3 00 D2 46 DF BF AB êô;-J,Đ sÄ òFßç«
00034000 FC 3C 87 6B 51 35 A4 80 1D 77 56 51 03 05 04 00 ü<+kQ5#€ wVQ
```

https://blog.csdn.net/qq_41995976

一开始是用foremost跑了一边发现没出来 然后就自己粘贴复制把rar提出来了

```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
在一个a[5][5]的二维数组中有下列几个元素
(2,5)
(5,1)
(2,4)
(2,5)
(3,5)
(3,2)
(1,4)
(5,1)
(2,2)
(2,5)
(4,5)
(2,1)
(1,2)
(4,5)
(5,5)
那么flag是什么呢?
```

https://blog.csdn.net/qq_41995976

得到一个txt
看到是一个5x5的数组就想到了波利比奥斯方阵密码
但是试了一下发现并不对

最后最后的最后看了别人的WP才发现应该是这样的

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	j
3	k	l	m	m	o
4	p	q	r	s	t
5	u	v	w	x	y

得到

juijoldugjfbty

凯撒遍历解密得到

ithinkctfiseasy

这题给的提示是真的少

安慰的话语

先把科加斯的图片拉去binwalk跑一边 得到一个压缩包

压缩包的txt里有段佛曰.....

佛曰：能那栗俱曰幡大夜呐漫侄依佛梵遮等諳顛老訶老諳者耨梵婆真輪故般豆輸俱明幡涅諳得鉢跋無俱提至朋鉢上實遮侄遮幡心菩呐老幡夷梵諦燦南咒怯心究呐明鉢神罰故諳輸勝俱蘇一哆摩恐哆喝哆切切諳阿死哆若有摩鉢真若夢姪侄離蒙哆倒是侄薩曰怯耶豆般利幡都若夜俱耨逝訶諳無侄悉涅幡波諳耶諳婆罰彌倒諳摩鉢智梵闍怯波罰遠地若侄迦梵闍實殿侄依喝梵寫槃醞特三除竟呐滅諳究漫諳一等冥耶侄世地鉢提吉羅幡除罰遮咒薩薩梵盡

像是前几年很流行的佛曰加密来着（那时候好多论坛和群里都玩这个来着？）

<http://www.keyfc.net/bbs/tools/tudoucode.aspx> 解密地址

得到一串

```
e58e8be7bca9e58c85e5af86e7a081e4b8ba7061737331323321212121
```

一开始没啥思路 试了很久

最后发现 把他们加上%然后urldecode解码就好了

```
%e5%8e%8b%e7%bc%a9%e5%8c%85%e5%af%86%e7%a0%81%e4%b8%ba%70%61%73%73%31%32%33%21%21%21%21
```

得到压缩包密码为 **pass123!!!!**

然后另外一个压缩包输入密码进去之后 会有一堆压缩包

最后到一个虚空.zip的压缩包 是一个伪加密

里边有个txt是base64

转码后得到一个urldecode

再转得到

```
公正公正友善公正公正屏蔽的关键字公正法治法治诚信屏蔽的关键字自由友善公正公正敬业公正法治公正爱国法治自由平等友善敬业公正友善敬业公正公正平等友善敬业公正爱国公正友善敬业法治富强公正平等法治友善法治
```

有两个屏蔽的关键字

去试了一下flag{

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{
```

编 码

公正公正公正诚信文明公正民主公正法治法治诚信民主

https://blog.csdn.net/qq_41995976

发现前面内容和解码得到的一样 所以猜测这两个被屏蔽的就是民主了

填进去再转码就得到flag了

[画图](#)

首先把flag.bmp放在winhex

发现下边有好多类似于 0 0 255 255 255这样的数值

猜测是 坐标和RGB的值

我们把这个数值复制一下放到一个txt里



The screenshot shows a Notepad window titled '画图.txt - 记事本'. The text inside the window consists of 46 lines, each containing a coordinate pair followed by three 255 values, representing RGB values. The lines are: 0 0 255 255 255, 0 1 255 255 255, 0 2 255 255 255, 0 3 255 255 255, 0 4 255 255 255, 0 5 255 255 255, 0 6 255 255 255, 0 7 255 255 255, 0 8 255 255 255, 0 9 255 255 255, 0 10 255 255 255, 0 11 255 255 255, 0 12 255 255 255, 0 13 255 255 255, 0 14 255 255 255, 0 15 255 255 255, 0 16 255 255 255, 0 17 255 255 255, 0 18 255 255 255, 0 19 255 255 255, 0 20 255 255 255, 0 21 255 255 255, 0 22 255 255 255, 0 23 255 255 255, 0 24 255 255 255, 0 25 255 255 255, 0 26 255 255 255, 0 27 255 255 255, 0 28 255 255 255, 0 29 255 255 255, 0 30 255 255 255, 0 31 255 255 255, 0 32 255 255 255, 0 33 255 255 255, 0 34 255 255 255, 0 35 255 255 255, 0 36 255 255 255, 0 37 255 255 255, 0 38 255 255 255, 0 39 255 255 255, 0 40 255 255 255, 0 41 255 255 255, 0 42 255 255 255, 0 43 255 255 255, 0 44 255 255 255, 0 45 255 255 255. A URL 'https://blog.csdn.net/gg_419959' is visible in the bottom right corner of the window.

然后可以利用python来画图

代码:

```
from PIL import Image
x = 173 #x坐标 通过对txt里的行数进行整数分解
y = 173 #y坐标 x*y = 行数

im = Image.new("RGB", (x,y))#创建图片
file = open('画图.txt') #打开rgb值文件

#通过一个个rgb点生成图片
for i in range(0,30000):
    line = file.readline()#获取一行
    rgb = line.split(" ")#分离rgb
    try:
        im.putpixel((int(rgb[0]),int(rgb[1])),(int(rgb[2]),int(rgb[3]),int(rgb[4])))#rgb转化为像素
    except:
        im.show()
        break
```

代码是直接拿这个博主的代码改的

<https://www.cnblogs.com/webFuckeeer/p/4536776.html>

```
flag  
{painterY0ur}
```

得到flag

flag不在这里

首先一个rar的压缩包 暴力跑一边就发现了密码



压缩包里的图片 看crc32值 发现就一个不一样

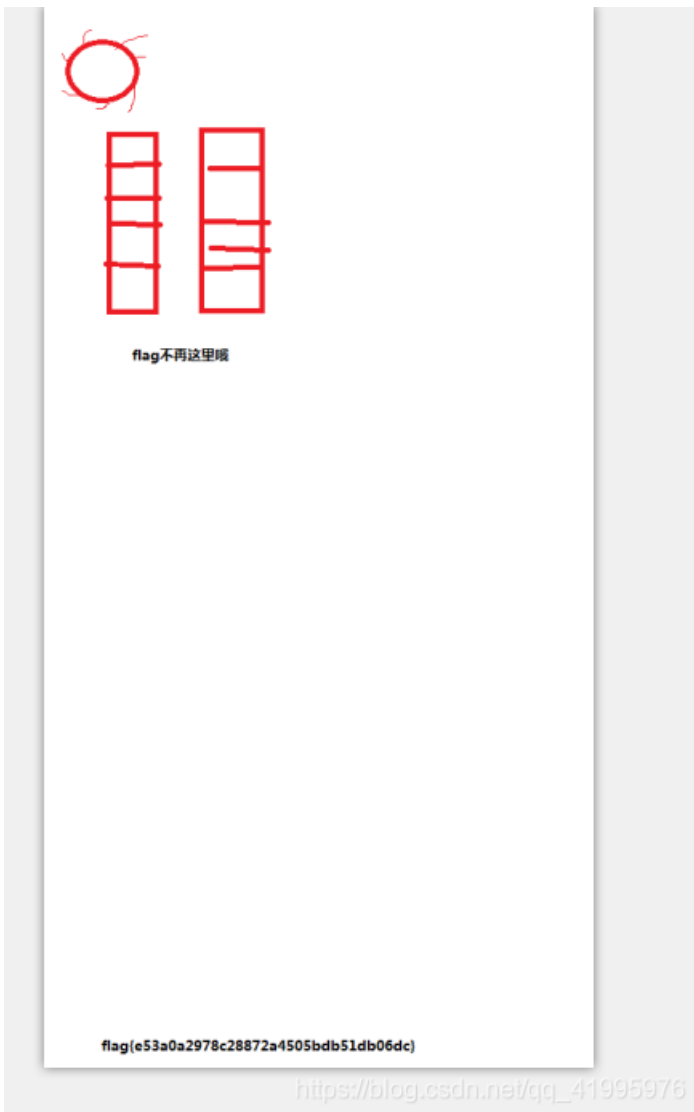
2.png *	5.32 KB	2.85 KB	看图王 PNG 图片文件	2018-12-06 09:30:15	40226FBC	m3:17
4.png *	5.32 KB	2.85 KB	看图王 PNG 图片文件	2018-12-06 09:30:15	40226FBC	m3:17
6.png *	5.32 KB	2.85 KB	看图王 PNG 图片文件	2018-12-06 09:30:15	40226FBC	m3:17
8.png *	5.32 KB	2.85 KB	看图王 PNG 图片文件	2018-12-06 09:30:15	40226FBC	m3:17
10.png *	5.32 KB	2.85 KB	看图王 PNG 图片文件	2018-12-06 09:30:15	40226FBC	m3:17
11.png *	6.92 KB	4.40 KB	看图王 PNG 图片文件	2018-12-06 09:29:07	8226A734	m3:17

所以就在这里边找

最后找着找着 发现改一下高度就行了

struct PNG_CHUNK_IHDR ihdr	518 x 1000 (x8)	10
uint32 width	518	10
uint32 height	1000	14
ubyte bits	8	18
enum PNG_COLOR_SPAC...	TrueColor (2)	19

(一开始改的比较小还没看到来着 之后想着下边没有出现黑色 就又试着改大了一点)



Blind

下过来图片里边有个压缩包 分离之后发现两张图片一样

题目是Blind猜测是盲水印加密

于是用脚本decode即可

```
python2 decode.py --original blind.png --image blind_blind.png --result result.png
```



结果

github地址:

<https://github.com/linyacool/blind-watermark>

<https://github.com/chishaxie/BlindWaterMark>

两种加密方式不同 解不出来用另外一个试试

火眼金睛

拿到的题目到手是一个压缩包

题干中给的提示有tips: five-digit

于是猜测是5位数字

字符类型: 固定字符集		起始密码	
<input checked="" type="checkbox"/> 数字 (0 - 9)	<input type="checkbox"/> 特殊符号 (!@...)	最小密码长度 =	5
<input type="checkbox"/> 小写字母 (a - z)	<input type="checkbox"/> 空格	最大密码长度 =	5
<input type="checkbox"/> 大写字母 (A - Z)	<input type="checkbox"/> 所有印刷字符		

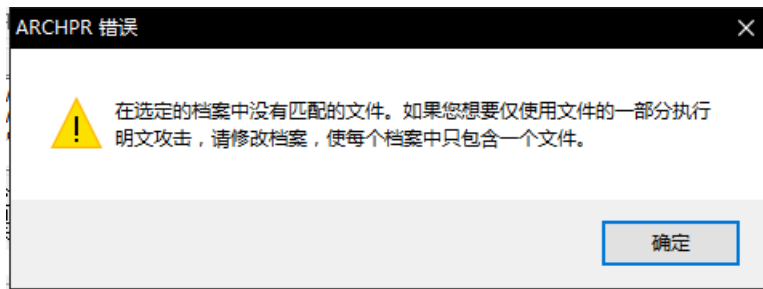


暴力破解后得到密码



下一个压缩包内有和已经破解出来的压缩包一样的文件 于是又用到明文破解了

但是这里可能会出个问题 把之前的Readme.txt压缩之后开始明文攻击的时候可能会出现这里的提示



这里尝试了好久也 找了许多资料 发现是压缩算法的问题 我这个压缩的算法和作者压缩的算法不一样



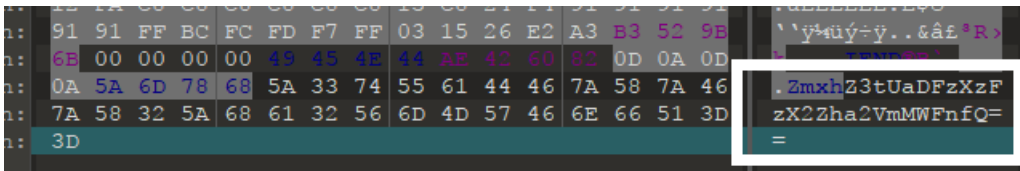
所以没办法破解 于是换了个算法 再次尝试



破解成功
得到张图片



首先在winHex查看 最后有组base64



解出来是flag{Th1s_1s_fakef1ag} 这是个假flag 先尝试一下能不能提交.....



于是又试了其他的方法 发现改了高度之后就OK了

struct PNG_CHUNK chunk[0]	IHDR (Critical, Pu...	8h	19h	Fg:	Bg:
uint32 length	13	8h	4h	Fg:	Bg:
union CTYPE type	IHDR	Ch	4h	Fg:	Bg:
struct PNG_CHUNK_IHDR ihdr	500 x 800 (x8)	10h	Dh	Fg:	Bg:
uint32 width	500	10h	4h	Fg:	Bg:
uint32 height	800	14h	4h	Fg:	Bg:
ubyte bits	8	18h	1h	Fg:	Bg:
enum PNG_COLOR_SPAC...	AlphaTrueColor (6)	19h	1h	Fg:	Bg:



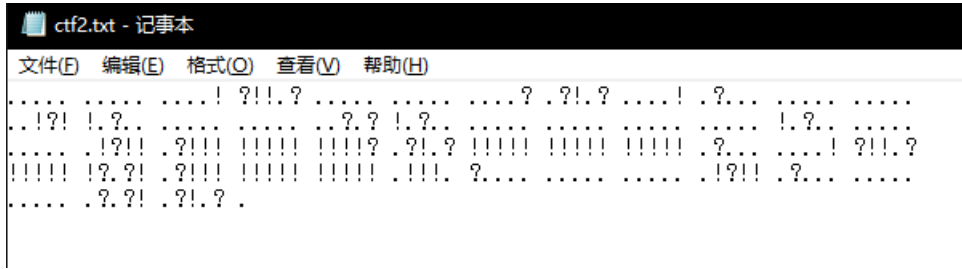
flag{40[redacted]493d}1995976

得到flag~

被截获的电报

第二题跑一边foremost

发现有个zip



先跑一边 short ook!

<https://www.splitbrain.org/services/ook>

得到 3oD54e

再跑一边base58（这谁想得到??）

<http://ctf.ssleye.com/base58w.html>

得到 misc

第三题不能直接用手机扫出来

这里用这个网站扫 可以扫出来

<https://online-barcode-reader.inliteresearch.com/>

得到12580}

三个一起提交就行了

500txt

一开始没什么思路 还以为是要转码什么的

想了半天没啥思路 就想着是不是里边藏了什么关键字

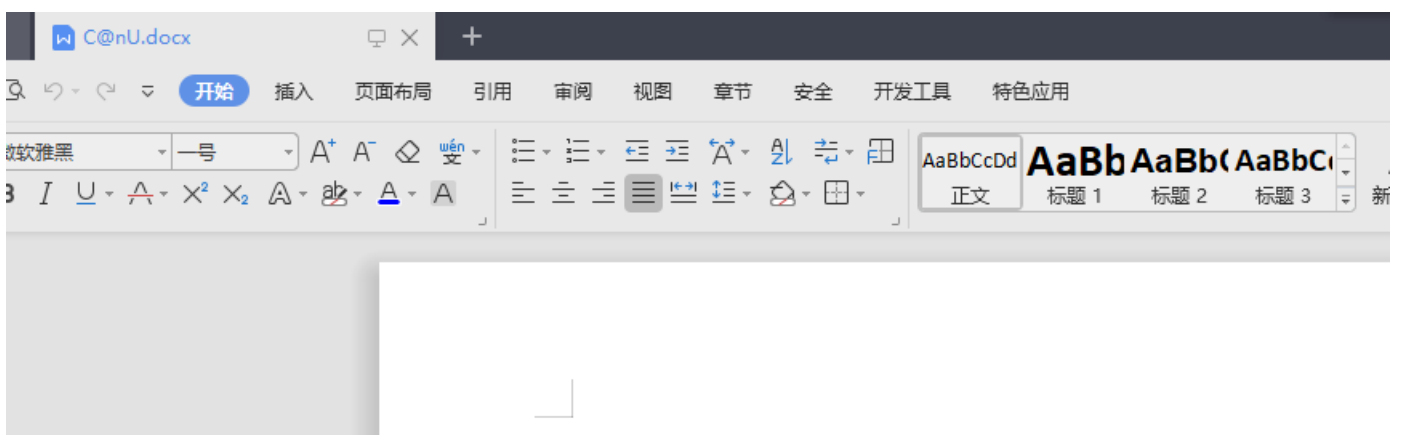
就自己写了个脚本查

```
for i in range(1,501):
    with open(str(i)+'.txt',"r") as f:
        str1 = f.read()
        if 'key{' in str1:
            print(i)
```

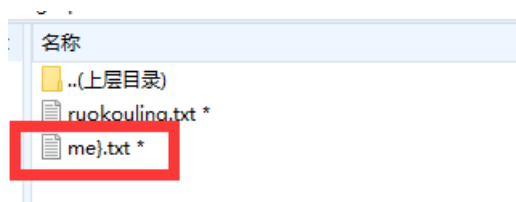
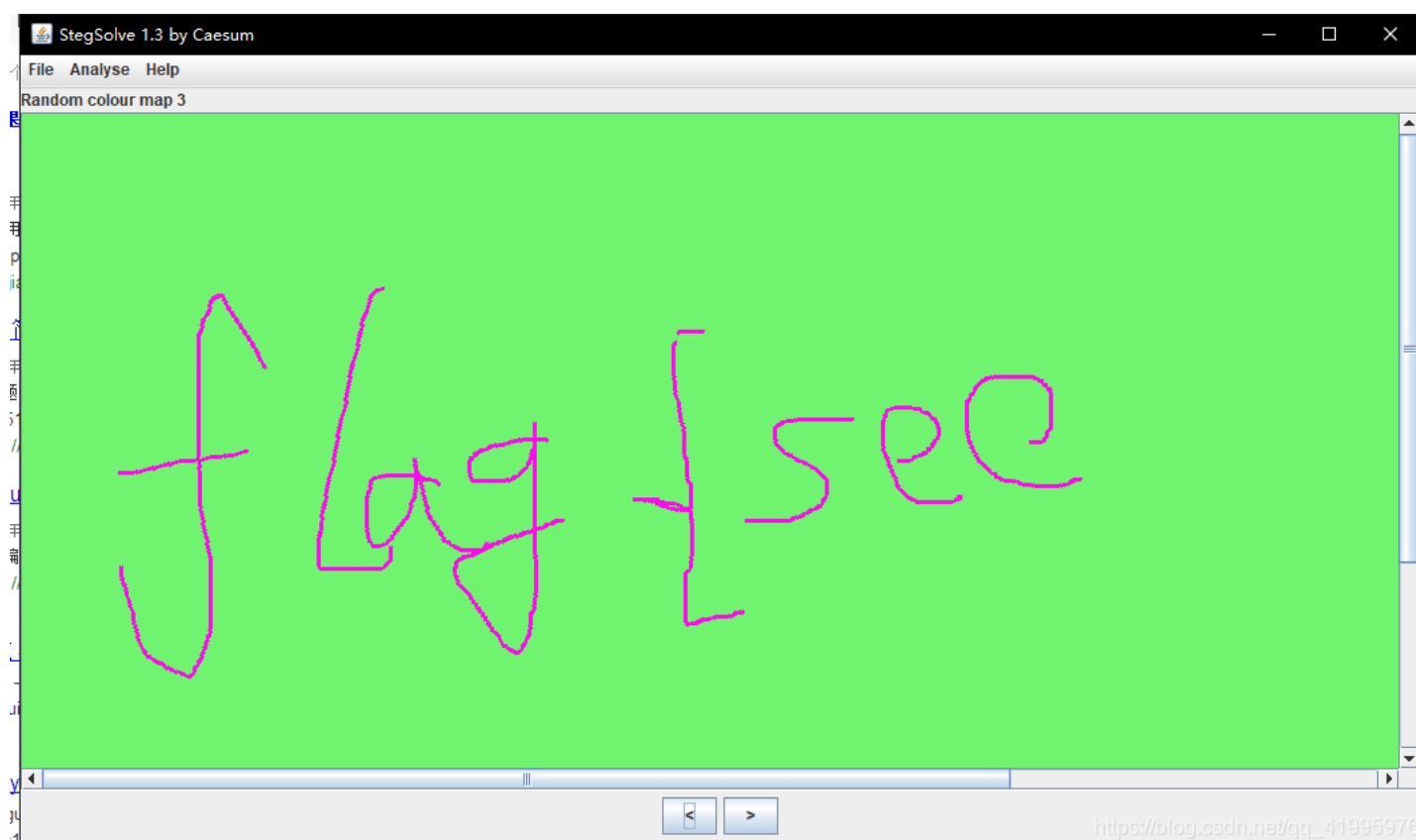
试了flag、ctf、key之后 再到txt里看了一下 就找到flag了

c2un

下载过来是一个doc文件 打开出现这样的页面



打开图片 发现是一片空白 试了好久 发现放到stegsolve里有反应



结合 之前压缩包里的文件名
猜测flag 可能为flag{seeme}
提交之后成功了.....

easyzip

```
#!/usr/bin/perl
$key= time();
print "$key\n";
`zip -P $key flag.zip flag`;
```

https://blog.csdn.net/qq_41995976

打开encrypt文件 发现zip的压缩包是用时间戳加密的

```
>>> time.time()
1558434301.323551
>>> len(1558434301)
```

查一下 现在的时间戳大概是155xxxxxxx



爆破一下 就可以出来了

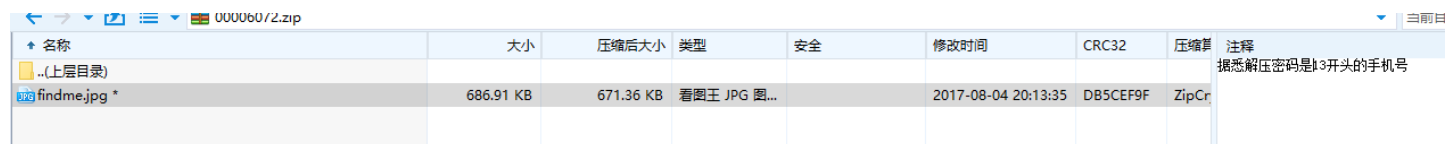


findme

压缩包里有 flag.vmdk 文件

去搜了一下好像要用虚拟机安装虚拟盘什么的

感觉太麻烦了 就用winhex看了一下 看到里面有zip文件头
就去用foremost-master跑了一下
还真跑出来一个压缩包

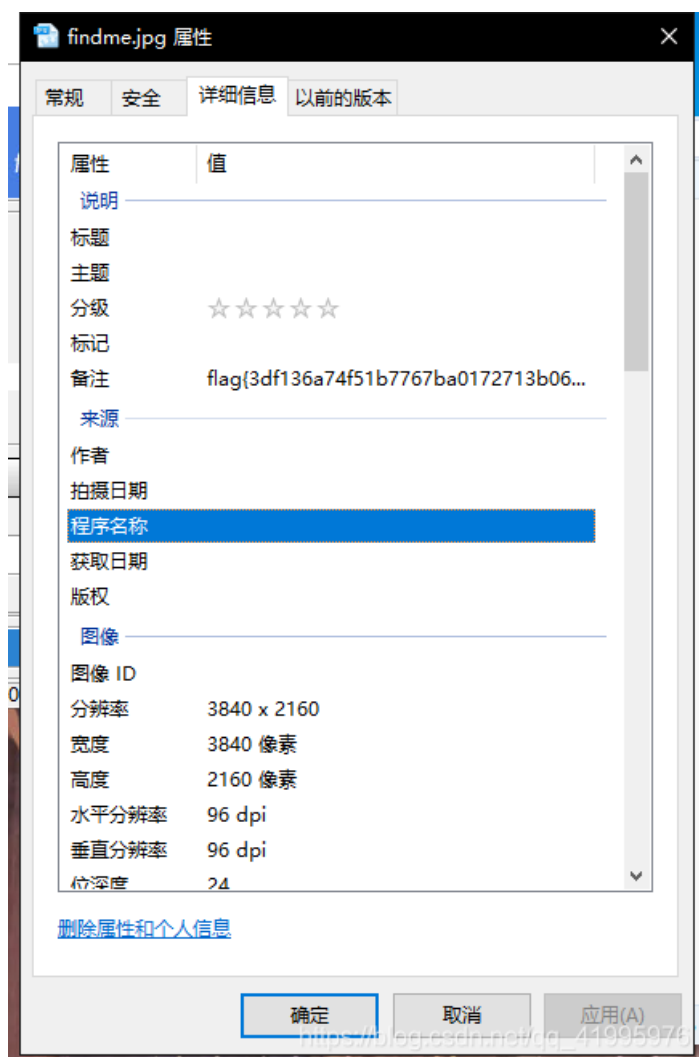


名称	大小	压缩后大小	类型	安全	修改时间	CRC32	压缩	注释
..(上层目录)								
findme.jpg *	686.91 KB	671.36 KB	看国王 JPG 图...		2017-08-04 20:13:35	DB5CEF9F	ZipCr	据悉解压密码是13开头的手机号

旁边有提示是13位开头的手机号

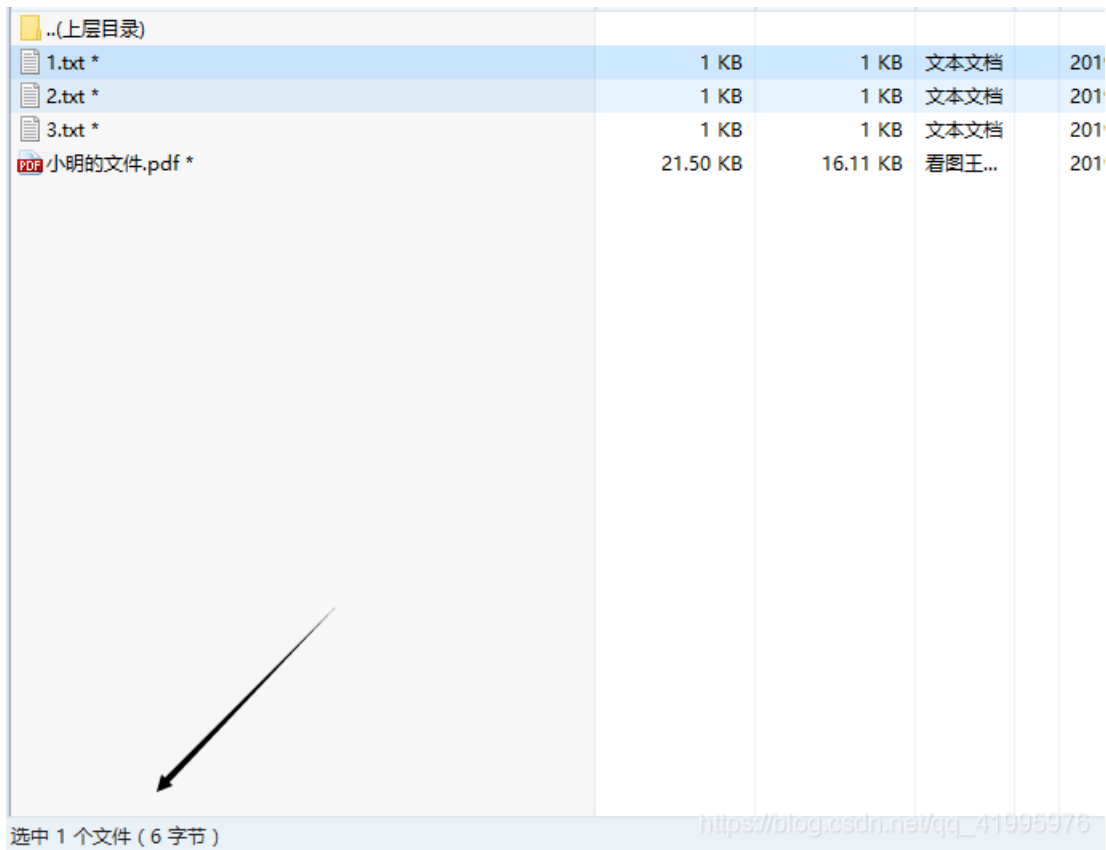


拿软件爆破一下是一张图片



属性里边可以看到flag

小明的文件



File Name	Size	Compressed Size	Type	Count
1.txt *	1 KB	1 KB	文本文档	201
2.txt *	1 KB	1 KB	文本文档	201
3.txt *	1 KB	1 KB	文本文档	201
小明的文件.pdf *	21.50 KB	16.11 KB	看图王...	201

选中 1 个文件 (6 字节)

https://blog.csdn.net/qq_41995976

下载过来的压缩包有四个文件

其中三个txt 只有六个字节

跑了一遍弱口令 和伪加密 发现都不能

那应该就是要crc32碰撞了

```
选择C:\Windows\System32\cmd.exe
alternative: 4Dimre (OK)
alternative: 65ANFp (OK)
alternative: 6Y2cB4 (OK)
alternative: D55UOm (OK)
alternative: E5tdTt (OK)
alternative: NRDIvD (OK)
alternative: P10kVQ (OK)
alternative: Q1qZMH (OK)
alternative: Vi98fw (OK)
alternative: Vuvdgc (OK)
alternative: X7Di6e (OK)
alternative: Y4d1F (OK)
alternative: crc32_ (OK)
alternative: V4d1F (OK)
alternative: iDpNgj (OK)
alternative: qcBcvM (OK)
alternative: wfKOFk (OK)
alternative: zI_s9u (OK)

G:\学校需要的文件\ctf\ctf工具\CRC32碰撞\crc32-master>python3 crc32.py reverse 0x6A037F6B
4 bytes: {0x97, 0xf7, 0x0a, 0x34}
verification checksum: 0x6a037f6b (OK)
alternative: 170708 (OK)
alternative: 6bits_ (OK)
alternative: 9m7uTH (OK)
alternative: RJ0rWk (OK)
alternative: SJqCLr (OK)
alternative: _4FPDi (OK)
alternative: bthYpu (OK)
alternative: chf4jx (OK)
alternative: kbpWfP (OK)
alternative: 1a2F1a (OK)
```

```
alternative: 1g65mD (OK)
alternative: ofmVg3 (OK)
alternative: q4jYCb (OK)
alternative: sEBzww (OK)
alternative: xo_j80 (OK)
alternative: zSZtaR (OK)

G:\学校需要的文件\ctf\ctf工具\CRC32碰撞\crc32-master> https://blog.csdn.net/qq\_41995976
```

都跑一边 找出有规律的字符串 得到

easy_crc32_6bits

成功解压文件

打开pdf

发现一个二维码



扫描后发现是个假的flag

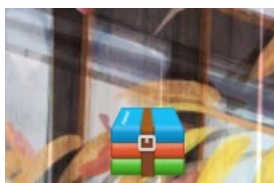
放进winhex、010editor、一系列操作 都没结果后

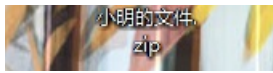
于是 我就开始了一波神奇的操作了！



首先 我先

把他转成了DOCX

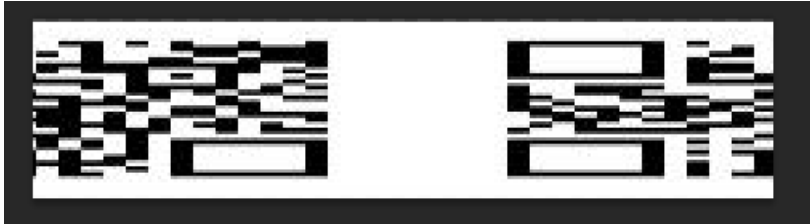




然后改成ZIP

名称	大小	压缩后大小	类型	安...	修改
..(上层目录)					
image1.png	11.40 KB	11.17 KB	看图王...		2019
image2.jpeg	16.84 KB	13.94 KB	看图王...		2019

打开居然找到了两张图片 其中一张是PDF本来就有了 另外一张是这个



用PS修复了一番加了三个点点之后就得到了这个二维码 扫出来就是答案了



注意!!! 上边的转成doc做法是在扯蛋!! 后边我发现直接把PDF拉去foremost-master跑一边分离就好了!!

新加卷 (G:) > 学校需要的文件 > ctf > ctf工具 > 图片隐写分离 > foremost-master > outfile > jpg

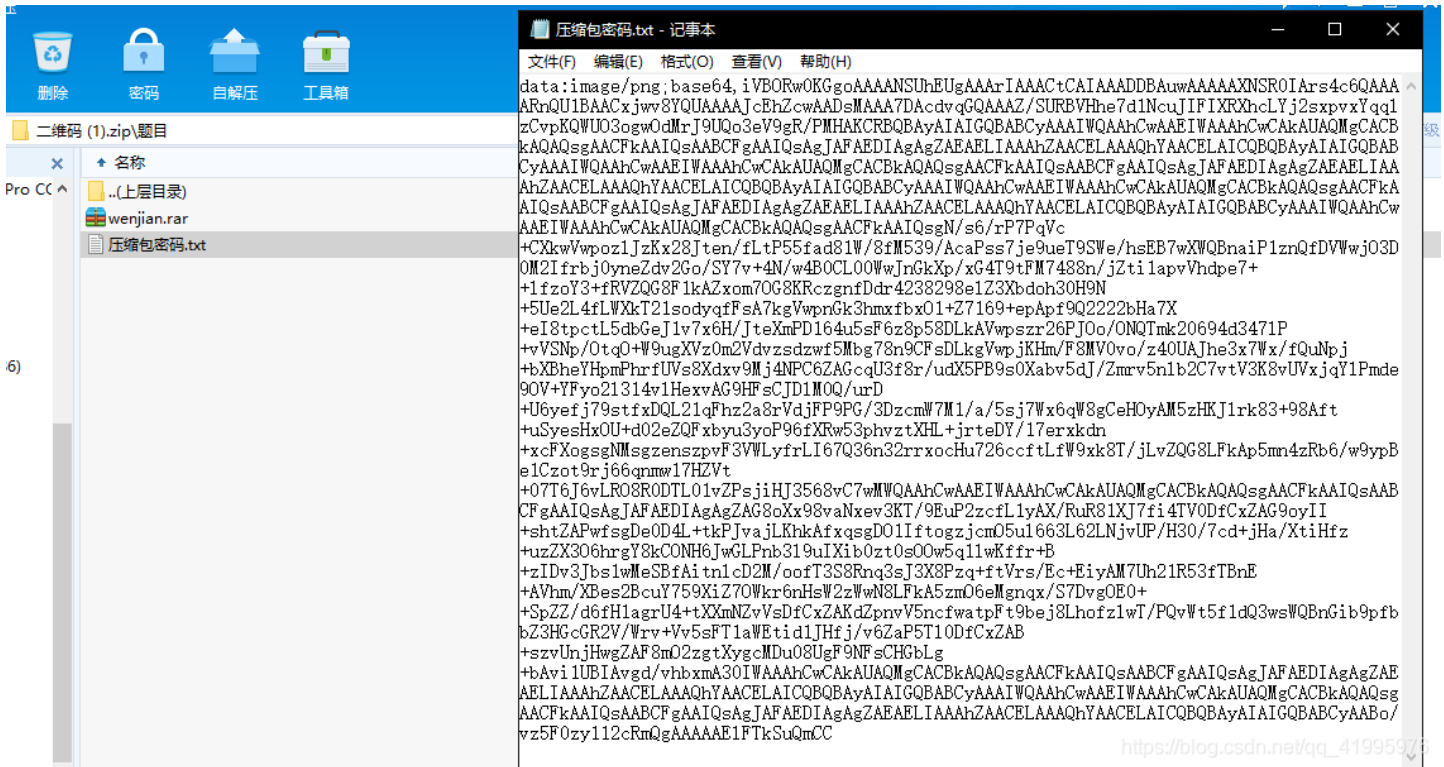


00000001.jpg



00000015.jpg

二维码



打开密码 发现是个图片的base64的值 随便找个地方转换一下就好了

<http://www.vgot.net/test/image2base64.php>

我用的是这个 注意要把前边的 data:xxx去掉

得到密码是asdfghjkl



然后获得一堆二维码

扫了几个发现 只有数值 0 和 1

应该组成起来是个二进制字符串

当然不可能一个个扫 之后利用两种二维码的图片大小不一样 来区分是0还是1

python脚本:

```
import os
for i in range(160):
    a = os.path.getsize(str(i) + '.png')
    if a == 443:
        print(0,end='')
    else:
        print(1,end='')
```

得到结果:

```
01100110011011000110000101100111011110110101000101010010011000110110111101100100011001010011000101110011010
10101011100110110010101100110011101010110110001111101
```

然后转成十六进制后再转成字符串就好了



得到flag

春节三重礼

这是我做过最tmZZ的隐写题目了

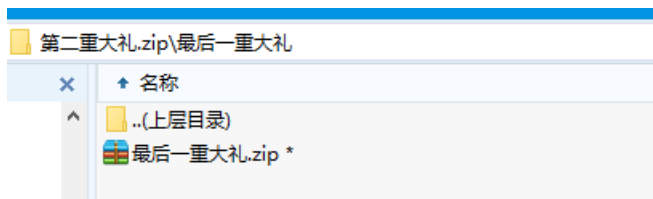
名称	大小	压缩后大小	类型	安...
春节三重礼.zip				
..(上层目录)				
pwd.zip *	54.66 KB	30.35 KB	好压 ZIP 压缩文件	
第二重大礼.zip *	107.35 KB	107.28 KB	好压 ZIP 压缩文件	

首先 一个压缩包 里边两个有密码的压缩包 没有其他提示 所以先字典跑了一边 然后又去改了一下zip伪加密 发现是伪加密

pwd.zip里是22个txt

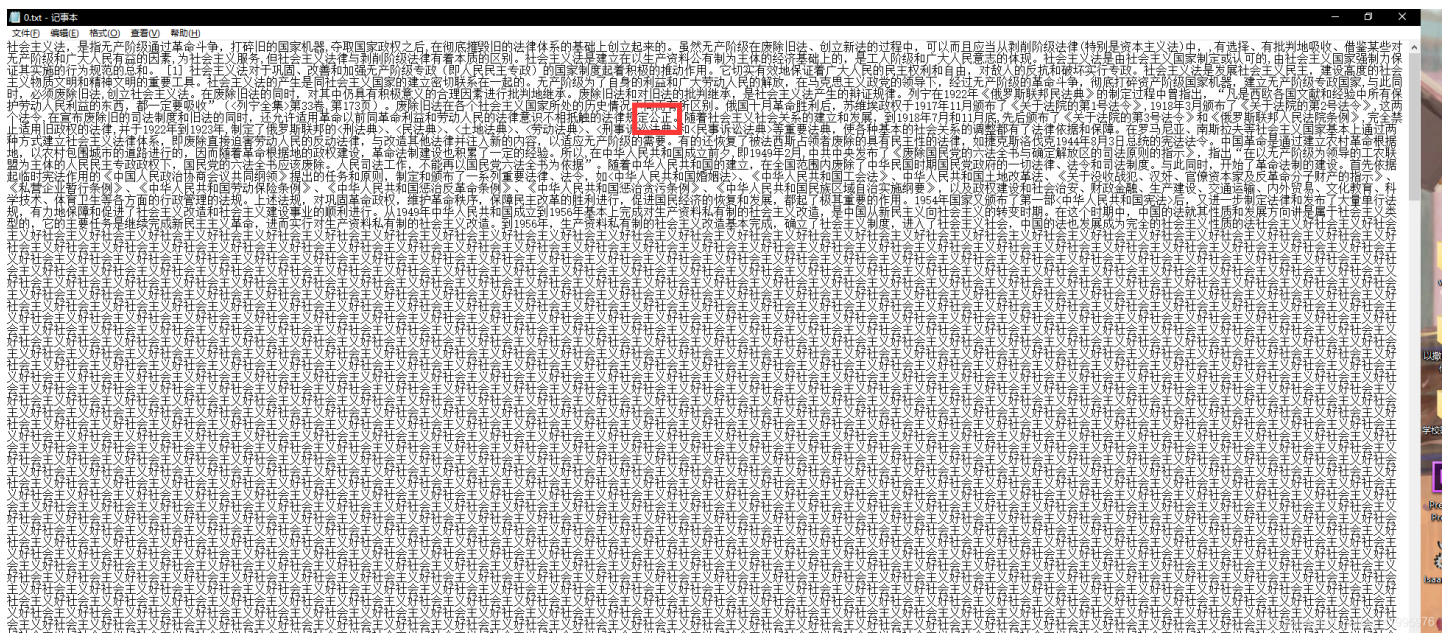
名称	大小	压缩后大小	类型	安...	修改时间	CRC32
..(上层目录)						
0.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	64FC3E81
1.txt	68.76 KB	2.40 KB	文本文档		2019-02-08 21:14:06	AE7CFE66
2.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	11B9F482
3.txt	68.76 KB	2.40 KB	文本文档		2019-02-08 21:14:06	F5A405FC
4.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	18653CB7
5.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	99923CD2
6.txt	68.76 KB	2.40 KB	文本文档		2019-02-08 21:14:06	DA7EAE1A
7.txt	68.76 KB	2.40 KB	文本文档		2019-02-08 21:14:06	82106E97
8.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	8BF7CDFC
9.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	DB2901B1
10.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	3AAAC194
11.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	B91EAFDD
12.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	C30DCC49
13.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	19C58668
14.txt	68.76 KB	2.40 KB	文本文档		2019-02-08 21:14:06	F6DC6A3C
15.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	A718F247
16.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	3B8D8D7B
17.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	15EB15C5
18.txt	68.76 KB	2.40 KB	文本文档		2019-02-08 21:14:06	0EE1A367
19.txt	68.76 KB	2.40 KB	文本文档		2019-02-08 21:14:06	F6EC1783
20.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	807ACCE7
21.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	738BD0B0

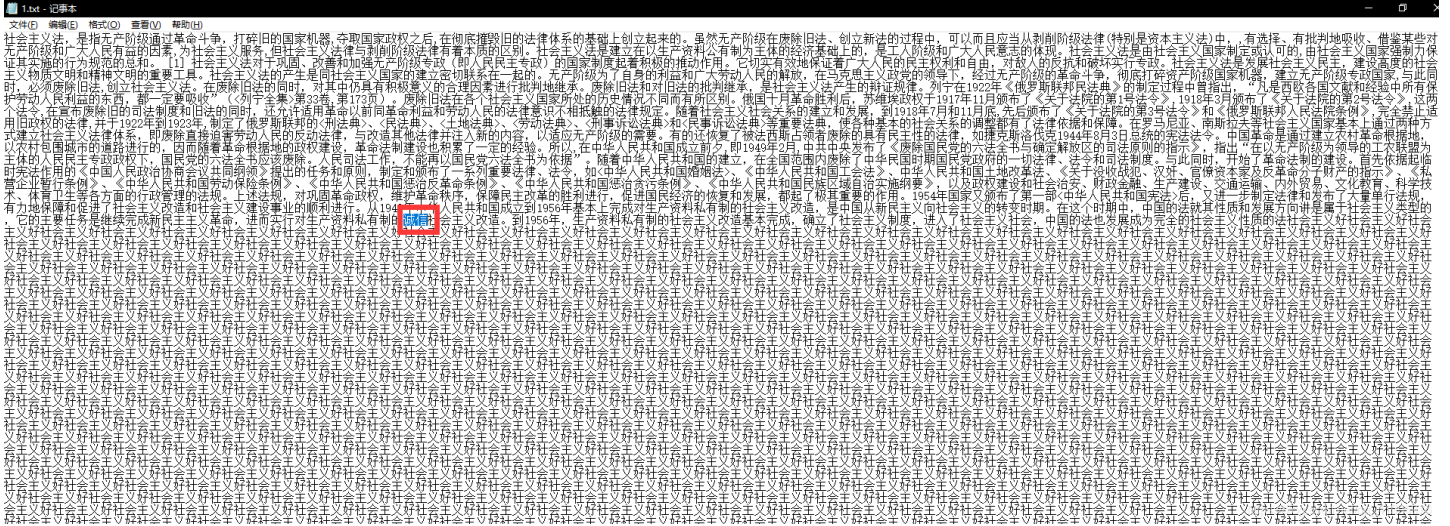
第二重大礼.zip里是一个加密的压缩包



大概就是pwd解密出来就是 第二个压缩包的密码了

然后来看txt的内容了





对比了一下前面两个txt发现 第一个txt有公正 第二个没有 第二个有诚信 第一个却没有

大概可以猜到了是核心价值观编码<http://ctf.ssleye.com/cvencode.html>

找到每个txt与其他不同的部分 然后解码就行了

开始写脚本~

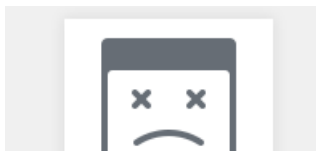
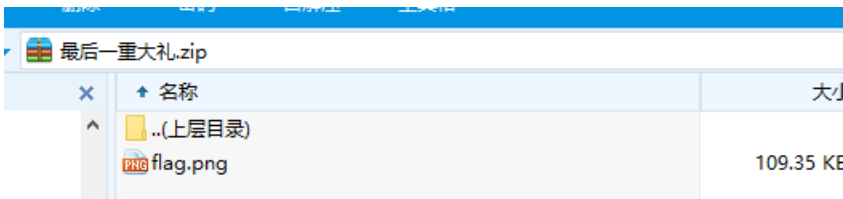
```
list1 = ['富强','民主','文明','和谐','自由','平等','公正','法治','爱国','敬业','诚信','友善']
for i in range(22):
    with open(str(i) + '.txt','r') as f: #设置文件对象
        temp = f.read()
        temp=temp.replace('民主',' ',8)
        temp=temp.replace('文明',' ',2)
        temp=temp.replace('自由',' ',1)
        for j in list1:
            if j in temp:
                print(j,end='')
```

这里要注意一下 原文本里边本来就带有8个民主 2个 文明 1个自由 所以判断的时候 要先用replace去掉 得到内容为:

```
>>>
RESTART: C:/Users/Administrator/AppData/Local/Programs/Python/Python37-32/春节三重礼.py
公正诚信民主公正平等法治敬业和谐文明和谐友善自由平等诚信平等文明民主法治和谐平等诚信平等
>>>
```

得到明文: **key2:!s**

然后就可以打开另外一个压缩包了

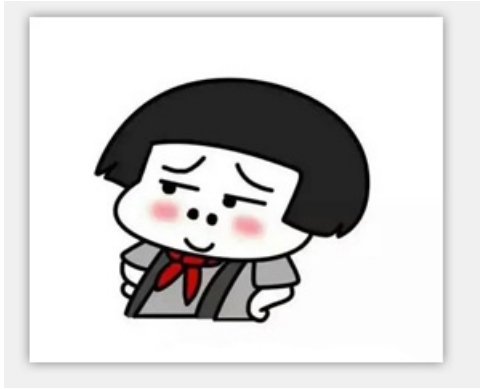


图片错误

最后一个压缩包里边有个打不开的图片

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	89	50	4E	47	D	0A	0A	1A	00	00	00	0D	49	48	44	52	%PNG
00000016	00	00	02	58	0	00	01	54	0	02	00	00	00	31	04	0F	X
00000032	8B	00	00	00	09	70	48	59	73	00	00	0B	13	00	00	0B	< p
00000048	13	01	00	92	9C	18	00	00	00	20	63	48	52	4D	00	00	~

改了文件头之后在打开



然后听题干说有ntfs隐写！！我还特地去试了半天！发现和NTFS没有屁点关系 祝出题人买菜超级加倍

春节三重礼.zip hint:ntfs, 在最后一个压缩包里面的文件流里面flag{md5(key1+key2+key3)}

最后发现这个图片要改高度 改完高度之后发现key3



key3:c0o1

注意！！！！最后一位是1不是l

我转MD5的时候还试了半天！！！！

最后的最后！！还有key1没有找到！！！！

于是我又又又！！！！找了好久好久！！！！

最后又在随便翻的时候 在最开始的压缩包里找到了! ! ? ? ?

```
00141120 48 4E 79 5E 6F 07 25 AD 01 00 6C AD 01 00 0E 00 HNy^o %- 1-
00141136 1C 00 00 00 00 00 00 00 20 00 00 00 90 79 00 00 y
00141152 B5 DA B6 FE D6 D8 B4 F3 C0 F1 2E 7A 69 70 75 70 μÚq̄p̄ōō'óÅñ.zipup
00141168 18 00 01 E4 6F 93 CD E7 AC AC E4 BA 8C E9 87 8D äo"İç¬ā°œé#
00141184 E5 A4 A7 E7 A4 BC 2E 7A 69 70 50 4B 05 06 00 00 ä#šç#4.zipPK
00141200 00 00 02 00 02 00 8D 00 00 00 FD 26 02 00 00 00 ý&
00141216 61 32 56 35 4D 54 70 49 51 47 4E 72 4D 33 49 3D a2V5MTpIQGNrM3I
00141232 40 23 24 5E 26 25 21 24 23 20 85 85 2A 26 25 00 @#$^&#!$# .....*%#
00141248 26 40 33 34 25 23 21 40 23 24 5E 26 25 21 24 23 &@34%#!@#$^&#!$#
00141264 20 85 85 2A 26 25 00 26 40 33 34 25 23 21 40 23 .....*%# &@34%#!@#
00141280 24 5E 26 25 21 24 23 20 85 85 2A 26 25 00 26 40 $^&#!$# .....*%# &@
00141296 33 34 25 23 21 64 34%#!d
```

https://blog.csdn.net/qq_41995976

base64转一下就好了 得到的是key1

如果把三个key的值加一起 转成md5就是flag了

之后的再做了之后更新