ISCC2019线上赛杂项Misc Write up

原创

Tunutu127 于 2019-05-31 15:18:15 发布 700 收藏 3

分类专栏： ISCC 文章标签： ISCC Misc 杂项 隐写

本文链接：https://blog.csdn.net/qq_41798754/article/details/90716743

ISCC_2019 杂项misc Write up

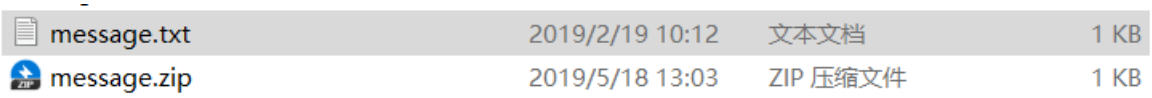
前言

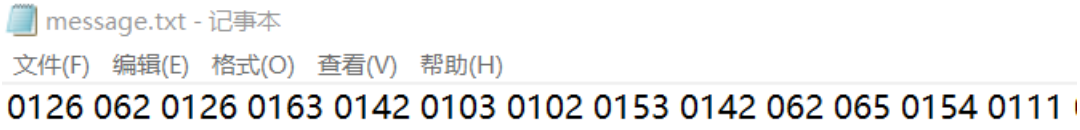
今年第一次参加了ISCC的比赛，觉得很有趣，当把题目解出来得到flag的时候是非常开心和有成就感的，想在这里分享一下杂项misc的解题思路，记录下本次比赛的过程和一些经验！当然第一次作为菜鸟参加很多时候在当经验宝宝，只有一些杂项题做了出来，如果有更好的解题思路（方法），请多多指教！好了，话不多说，请看题！（题目不按照放题顺序）

（对了，本次misc用到的工具和题目，放在文章末尾的链接里，如有需要请自行下载）

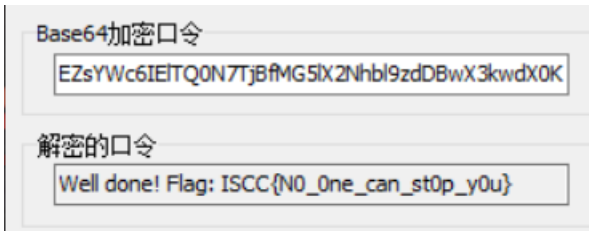
1： 隐藏的信息（这是一个被混淆的文件，但是我忘记了这个文件的密码。你能够帮助我还原明文吗？50分）

下载附件是个message.zip文件，解压得到message.txt，打开后发现是很多4位在一块的数字，仔细看完后发现没有超过8的数字，是八进制。





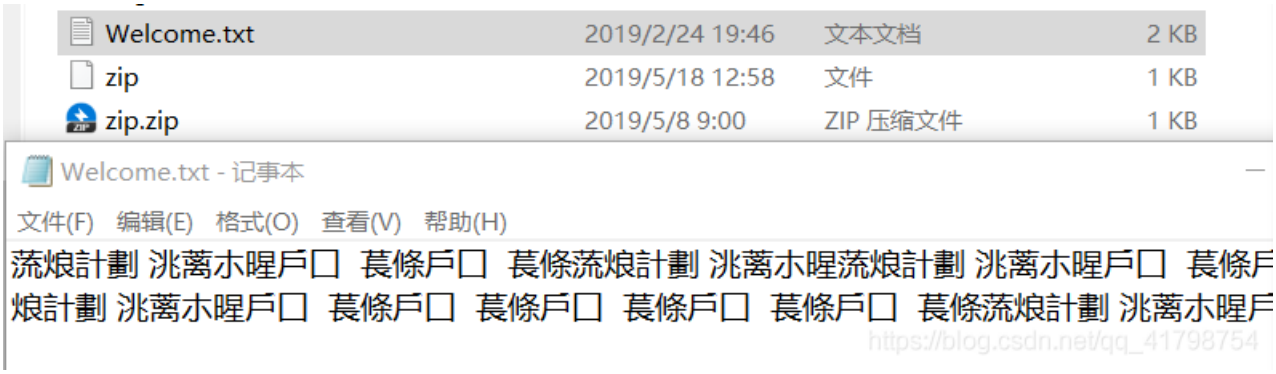
八进制转十进制，再转Ascll码，发现一串数字+字母很像base64，于是进行base64解密，很幸运真的是



base64，得到Flag:ISCC{N0_0ne_can_st0p_y0u}

2. 流浪地球

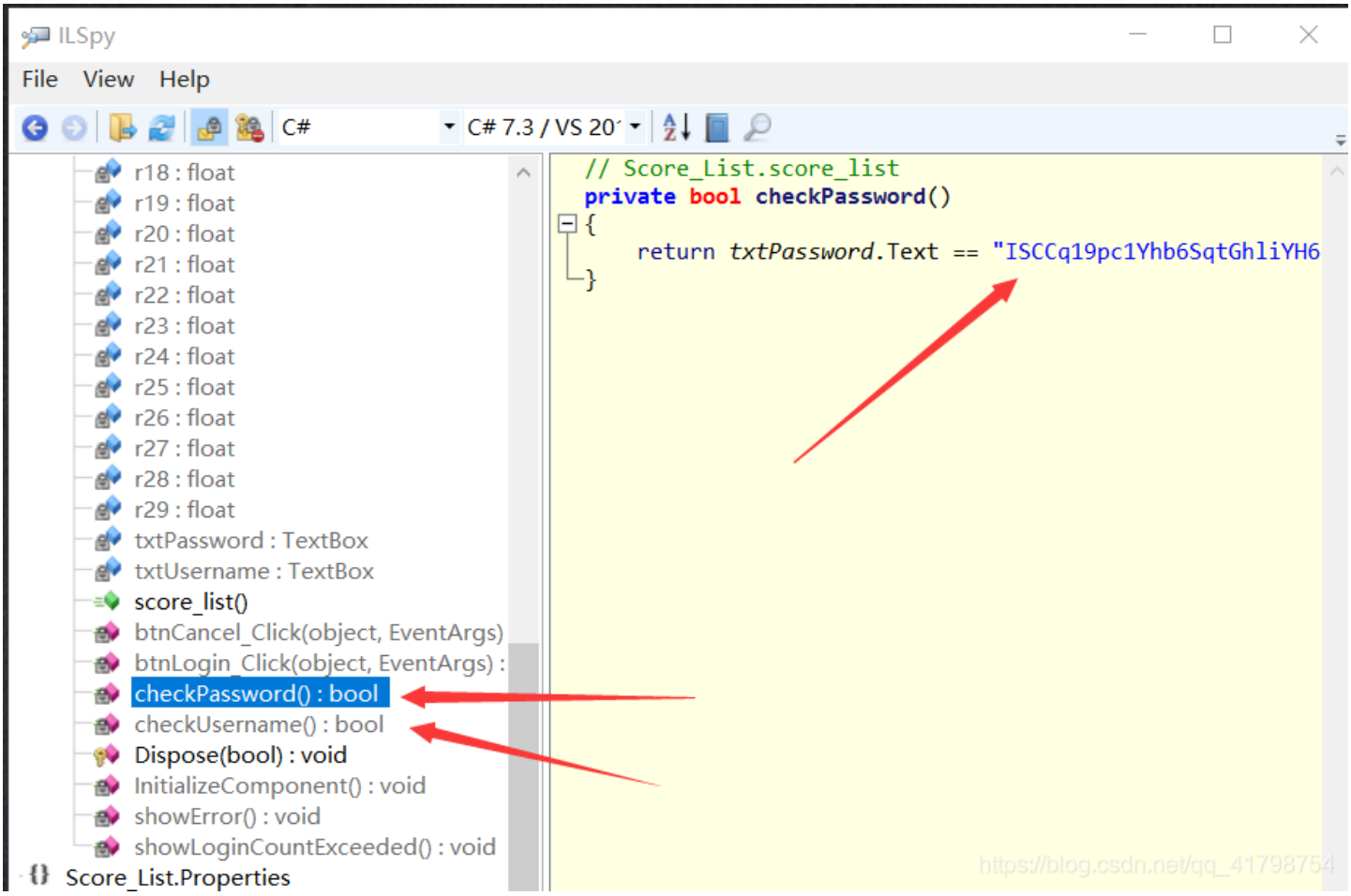
不得不说这道题的脑洞是真的大，下载附件后是个无法打开的文件名字就叫zip，于是想到改拓展名为zip.zip，解压后得到welcome.txt，打开后发现是火星文，可以转为中文简体，原件打开如下：

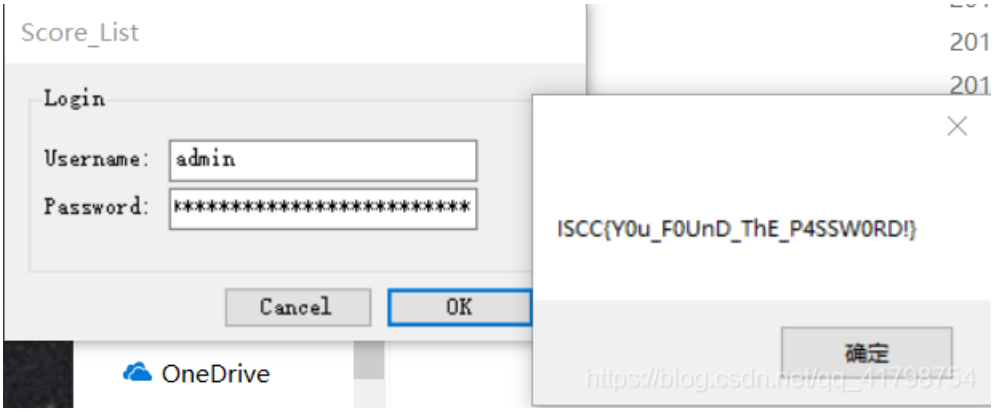


看着是不是感觉头大，当时第一眼发现很多重复的字，以为是可以切换为摩斯电码 .-然后按照这个思路做下去，真的是流浪了一下午也没流浪出来，后来发现文字之间空格间距不一样，有的是一个空格有的是两个空格，于是猜测一个空格为0，两个空格为1，转换后为二进制，直接二进制转text，得到flag!

3. 揭秘成绩单

下载附件是Score_List.zip，解压后得到Score_List.exe，双击打开，发现让填Username和Password，直接把Score_List.exe扔进反编译软件ILspy，翻了一翻找到了checkusername和checkpassword，打开后看到用户名和密码，随后双击打开.exe文件，将其输入之后得到flag!





4. 最危险的地方就是最安全的地方

下载附件打开后是Misc-01.zip，解压后得到.jpg文件，发现打不开，丢到winhex里面查看一下，发现还包含有png文件

Misc-01.jpg

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
000082D0	68	4F	28	0F	5B	4E	90	47	B3	09	17	DB	3A	C3	15	9F	hO(.[N.G³..Û:Ã.▌
000082E0	E4	D0	5D	43	B9	BF	05	1B	3F	20	48	79	30	9F	70	B1	äÐ]C¹¿..? Hy0▌p±
000082F0	DC	0C	1B	6E	64	9E	43	BB	41	1F	6B	8D	DA	F3	5A	66	Ü..nd▌C»A.k.ÚóZf
00008300	26	16	57	F1	DE	E7	63	40	A6	7F	EF	F9	B8	FC	3F	93	&.WñÞçc@¦.ïù¸ü?▌
00008310	39	E4	90	43	0E	39	E4	90	43	00	7F	00	6A	A4	82	6D	9ä.C.9ä.C...j¤▌m
00008320	72	1D	AA	AA	00	00	00	00	49	45	4E	44	AE	42	60	82	r.ªª....IEND®B`▌
00008330	50	4B	03	04	14	00	00	00	08	00	A3	A2	59	4E	1D	B1	PK........£¢YN.±
00008340	50	7D	58	03	00	00	53	03	00	00	0D	00	00	00	51	52	P}X...S.......QR
00008350	63	6F	64	65	2F	32	35	2E	70	6E	67	01	53	03	AC	FC	code/25.png.S.¬ü
00008360	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	▌PNG........IHDR
00008370	00	00	01	9A	00	00	01	9A	01	00	00	00	00	1E	7D	B8	...▌...▌......}¸
00008380	CE	00	00	03	1A	49	44	41	54	78	9C	ED	9C	CB	8D	DB	Î....IDATx▌í▌Ë.Û
00008390	30	10	86	BF	09	05	F8	48	01	5B	C0	96	42	75	B0	25	0.▌¿..øH.[À▌Bu°%
000083A0	05	29	29	1D	88	A5	A4	03	F1	18	80	C2	9F	83	29	3F	.)).▌¥¤.ñ.▌Â▌.)?
000083B0	16	01	82	24	1B	D9	B1	86	07	03	B6	F8	C1	43	78	30	..▌$.Ù±▌..¶øÁCx0
000083C0	6F	DA	C4	6F	AF	FC	E9	F7	19	70	C8	21	87	1C	72	C8	oÚÄo¯üé÷.pÈ!▌.rÈ
000083D0	21	87	9E	13	B2	BE	06	C8	E3	6A	C0	6A	36	01	36	95	!▌▌.²¾.ÈãjÀj6.6▌
000083E0	01	28	DB	86	E9	2E	E2	39	B4	23	84	24	89	24	49	5A	.(Û▌é.â9´#▌$▌$IZ
000083F0	82	48	4B	90	66	40	73	AC	48	0B	48	4B	D0	D5	BE	F9	▌HK.f@s¬H.HKÐÕ¾ù
00008400	C1	CF	E4	D0	47	40	E5	6C	00	00	88	92	4D	E5	24	9B	ÁÏäÐG@ål..▌'Må$▌
00008410	A2	64	13	D0	2C	C8	BD	C4	73	68	37	68	78	FF	41	1E	¢d.Ð,È½Äsh7hxÿA.

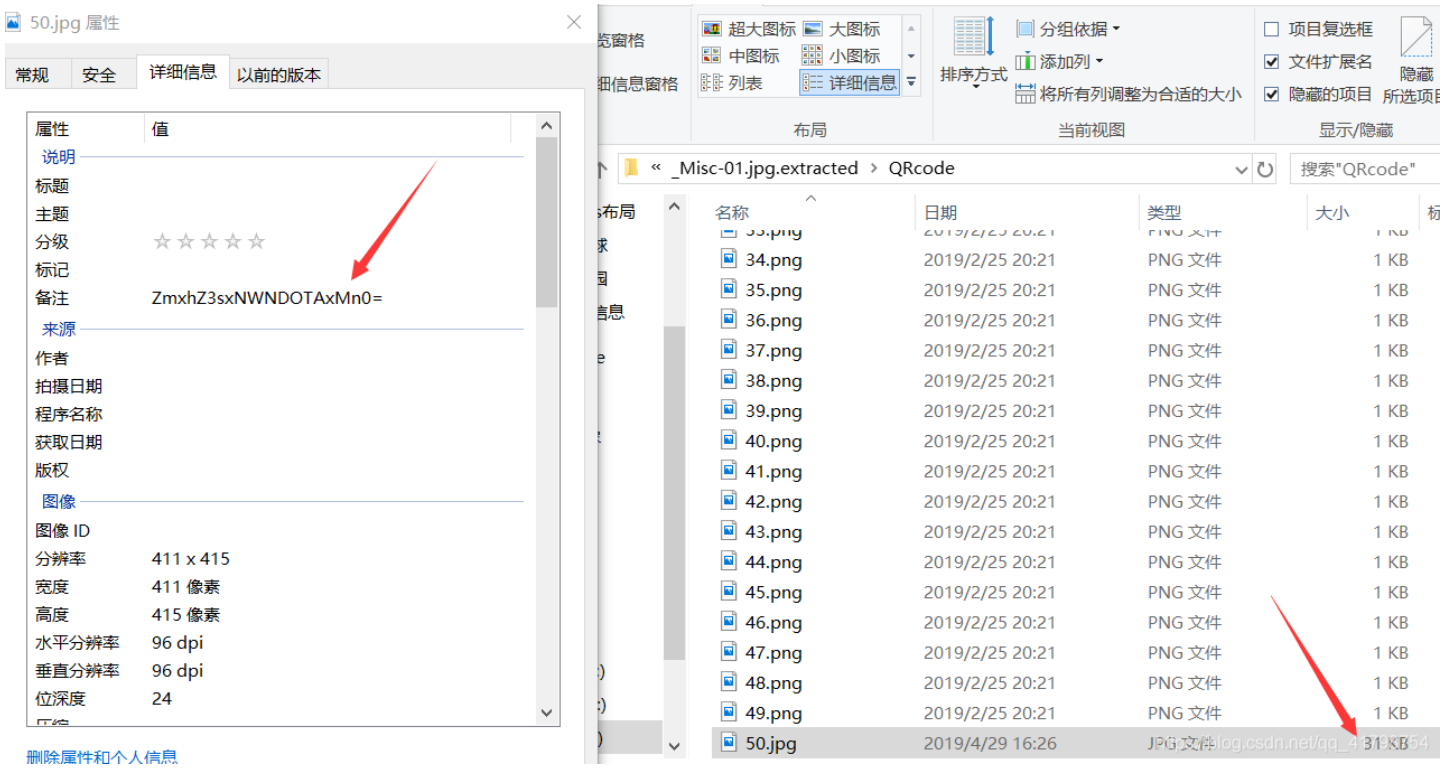
直接丢到binwalk里面

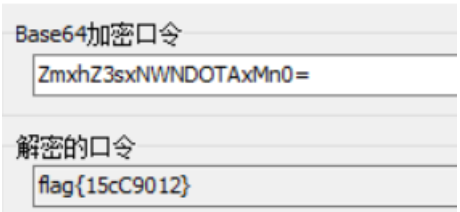
```
root@kali:~/桌面# binwalk -e Misc-01.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
18527         0x485F          Zip archive data, at least v1.0 to extract, name:
QRcode/
18564         0x4884          Zip archive data, at least v2.0 to extract, compre
ssed size: 838, uncompressed size: 833, name: QRcode/1.png
19444         0x4BF4          Zip archive data, at least v2.0 to extract, compre
ssed size: 878, uncompressed size: 873, name: QRcode/10.png
20365         0x4F8D          Zip archive data, at least v2.0 to extract, compre
ssed size: 816, uncompressed size: 811, name: QRcode/11.png
21224         0x52E8          Zip archive data, at least v2.0 to extract, compre
ssed size: 839, uncompressed size: 834, name: QRcode/12.png
22106         0x565A          Zip archive data, at least v2.0 to extract, compre
ssed size: 799, uncompressed size: 794, name: QRcode/13.png
22948         0x59A4          Zip archive data, at least v2.0 to extract, compre
ssed size: 863, uncompressed size: 858, name: QRcode/14.png
23854         0x5D2E          Zip archive data, at least v2.0 to extract, compre
ssed size: 819, uncompressed size: 814, name: QRcode/15.png
24716         0x608C          Zip archive data, at least v2.0 to extract, compre
ssed size: 877, uncompressed size: 872, name: QRcode/16.png
25636         0x6424          Zip archive data, at least v2.0 to extract, compre
```

分离出来很多图片，都是二维码，扫码之后解码数据为：remake:最危险的地方就是最安全的地方+1，并没

有得到有用的信息

再次查看图片，查看详细信息，发现有个图片比较大，于是右击属性查看详细信息，发现了一串base64编码

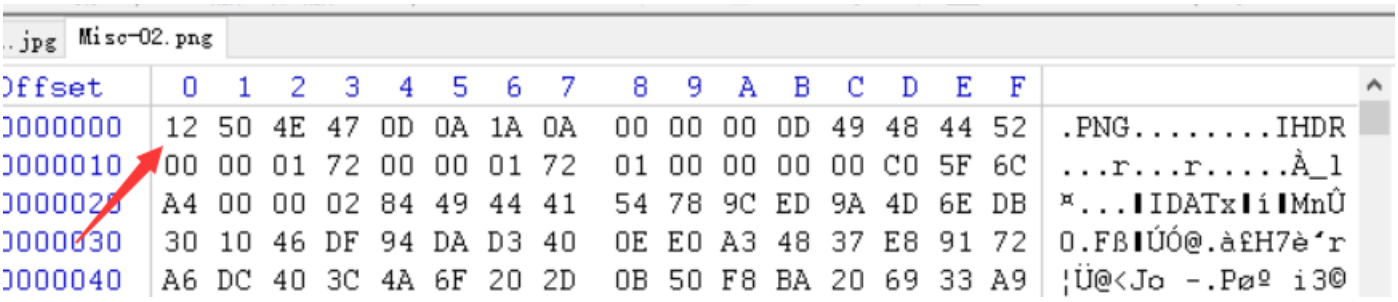




经过base64解密得flag！

5. High起来

附件下载后是个zip文件，解压后是png图片，发现打不开，扔进winhex里面看一下，发现png头不对，把12改成89（png文件头标志是89504E47）然后保存，打开图片发现是个二维码，扫一下得到密文：中口由羊口中中大中中中井！



密文发现是当铺密码，在线揭秘一下，得到一串数字：201902252228，目前还不知道有什么用

当铺密码

中口由羊口中中大中中中井

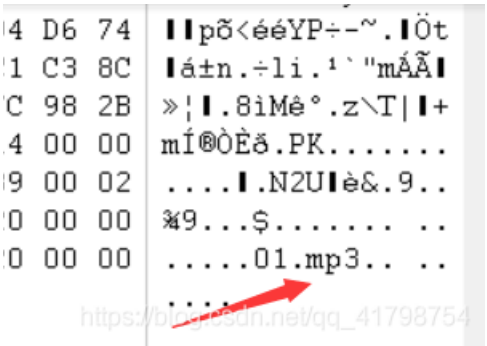
转换密码↓

201902252228

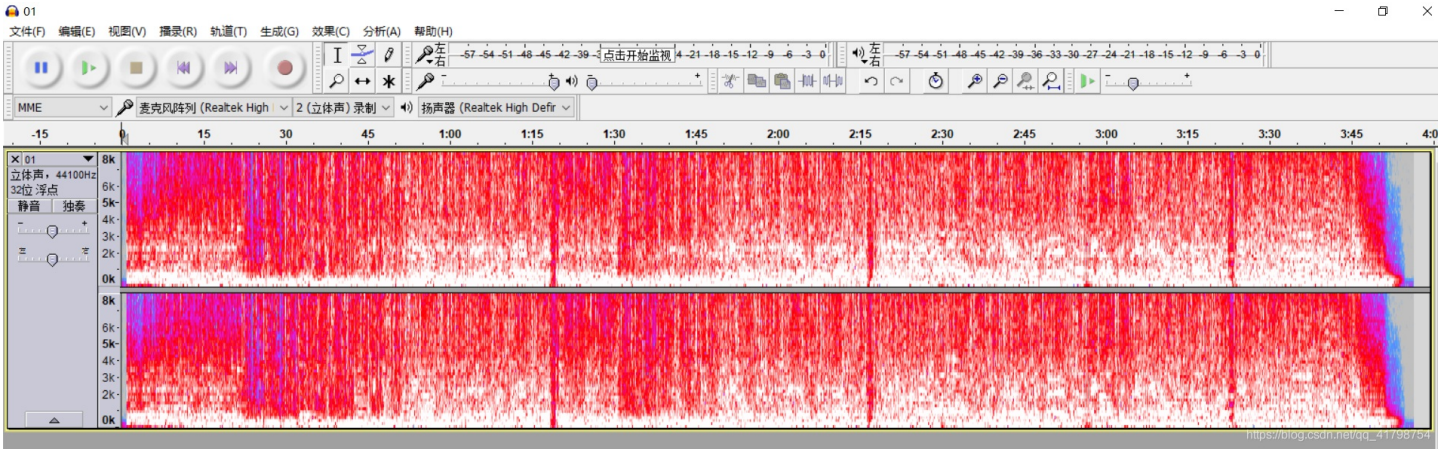
简介：当前汉字有多少笔画出头，就是转化成数字几。
(例：王夫井工夫口 = 678470)

返回

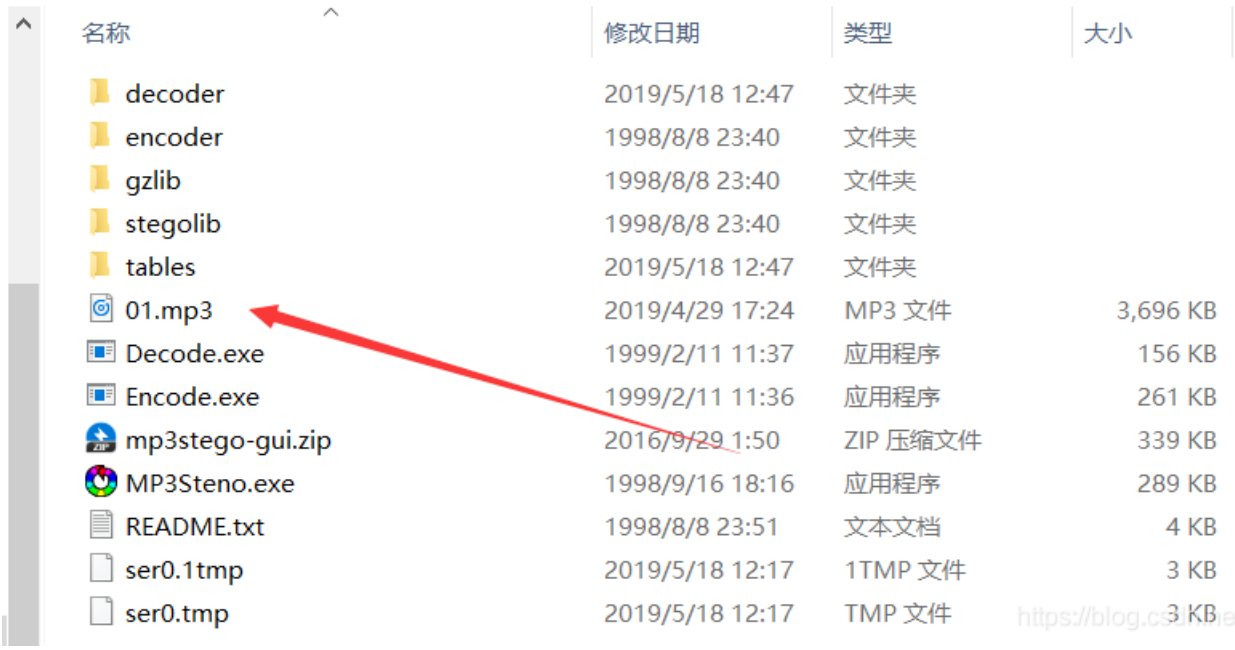
目前没有发现这串数字有什么用，再次回到图片，在winhex里面拉到最下面发现里面蕴含01.mp3，可以用binwalk分离一下，也可以改.png为.zip,解压一下得到01.zip，此次选择改拓展名



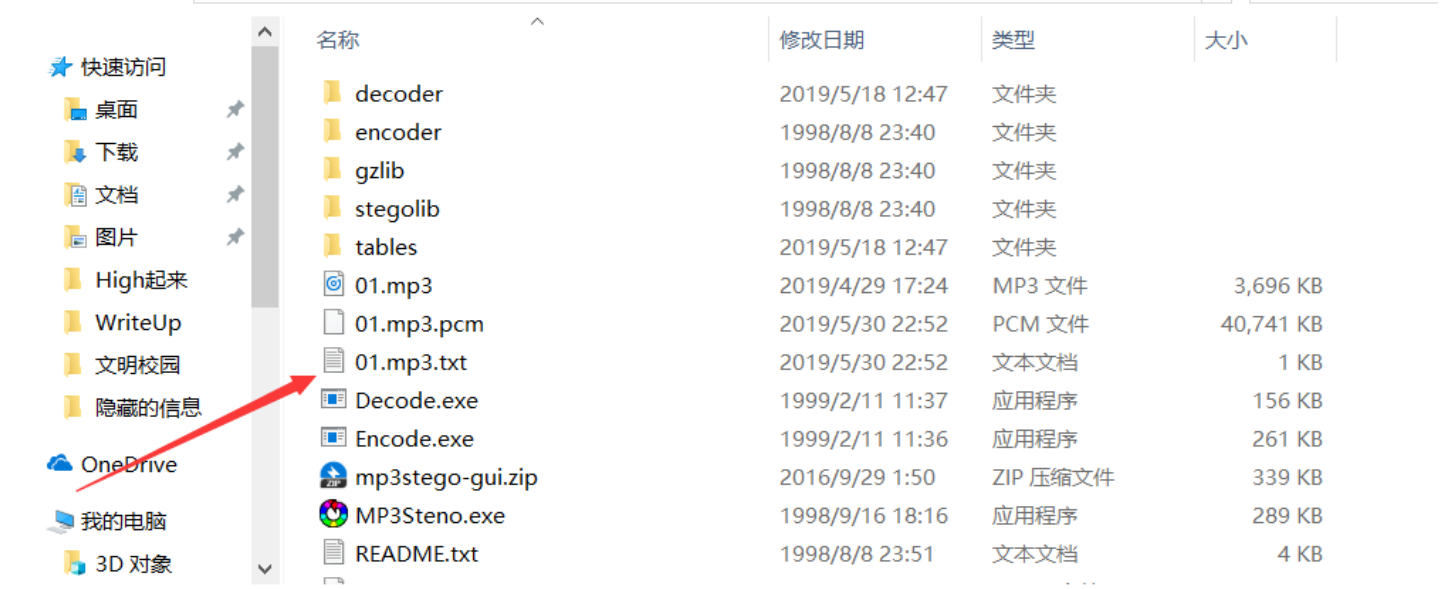
看到mp3，第一时间想到拖进Audacity里查看一下频谱图，很显然，并没有什么收获。



这个时候 想起了Mp3stego，首先将文件复制到MP3stego这个目录下，



在cmd下用decode来提取，这个需要密码，这个时候想起来前面解出来的数字201902252228，在cmd下输入Decode.exe -X -P 201902252228 01.mp3!




```
E:\2019ISCC\工具\隐写工具\音频mp3隐写\音频隐写>Decode.exe -X -P 201902252228 01.mp3
MP3StegoEncoder 1.1.15
See README file for copyright info
Input file = '01.mp3'  output file = '01.mp3.pcm'
Will attempt to extract hidden information. Output: 01.mp3.txt
the bit stream file 01.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=stereo, sblim=32, jsbd=32, ch=2
[Frame 9053]Avg slots/frame = 417.913; b/smp = 2.90; br = 127.986 kbps
Decoding of "01.mp3" is finished
The decoded PCM output file name is "01.mp3.pcm"
```


解密完成，生成了一个01.txt文件，打开发现是一串Unicode编码，解码得flag！

6.它们能在一起吗？

他们能在一起吗?

200

857 solves

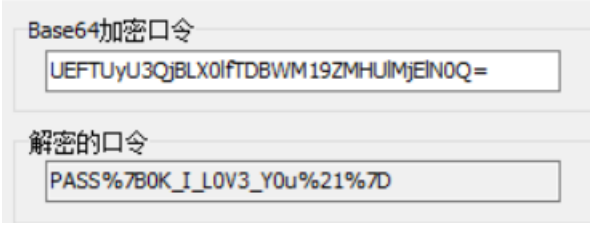
小明在网上向暗恋已久的女生表白了，对方只给小明发来了一个二维码作为回复，面对小明的求助，你会告诉他这名女生想表达的意思吗?

附件下载

Flag

提交

下载后发现是个png图片，打开是个二维码，扫码得到一串编码，很明显是base64，解码得

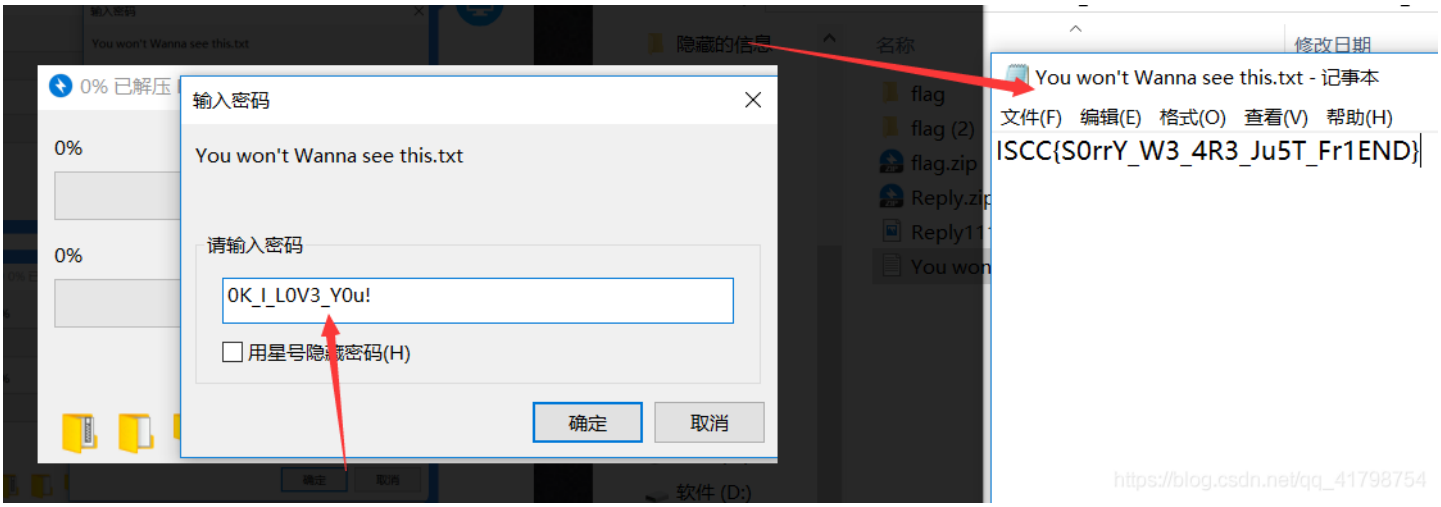


用软件Converter中的Unescape再次解码得到

看起来很像flag，试着去提交一下，发现不对，改了各种格式发现还是不对，再次把目标放在图片上，放到winhex里面查看一下，拉到最下面，发现里面隐藏了一个.txt文件

```
0A 54 81 06   56 3D 50 05 AA C0 65 14   ÌªJ´.T..V=P.ªÀe.
55 25 5A 05   AA 40 03 AB 1E A8 02 55   h`]fU%Z.ª@.«.¨.U
0B 4D 64 1D   30 9F 3D 47 18 00 00 00   à2.ü.Md.0▮=G....
44 AE 42 60   82 50 4B 03 04 0A 00 01   .IEND®B`▮PK.....
78 53 4E DD   AE E9 B6 2A 00 00 00 1E   ....xSNÝ®é¶*....
00 00 00 59   6F 75 20 77 6F 6E 27 74   .......You won't
6E 61 20 73   65 65 20 74 68 69 73 2E    Wanna see this.
6A A0 34 F2   94 42 06 F1 C8 02 E2 B9   txtqj 4ò▮B.ñÈ.â¹
75 63 E2 45   41 44 3B 45 48 22 4E FB   ▮§vIucâEAD;EH"Nû
45 99 84 66   BC 6C DF AF 20 50 4B 01   ▮1ÛQE▮▮f¼lß¯ PK.
00 01 08 00   00 15 78 53 4E DD AE E9   .?........xSNÝ®é
00 1E 00 00   00 1C 00 24 00 00 00 00   ¶*.........$....
00 00 00 00   00 00 00 59 6F 75 20 77   ... .......You w
20 57 61 6E   6E 61 20 73 65 65 20 74   on't Wanna see t
74 78 74 0A   00 20 00 00 00 00 00 01   his.txt.. ......
0A 1E D3 20   C8 D4 01 C3 6F B2 1B 95   . ..Ó ÈÔ.Ão².▮
6F B2 1B 95   C7 D4 01 50 4B 05 06 00   ÇÔ.Ão².▮ÇÔ.PK...
00 01 00 6E   00 00 00 64 00 00 00 00   .......n...d....
                                        .
```


接着用binwalk分离 or 改成.zip再解压，解压发现需要密码，这个时候联想到前面解出来得PASS，把{}里面的输进去，发现解压出来了个.txt，打开后得到Flag！！可惜，小明他们不能在一起，ha！



7.无法运行的exe

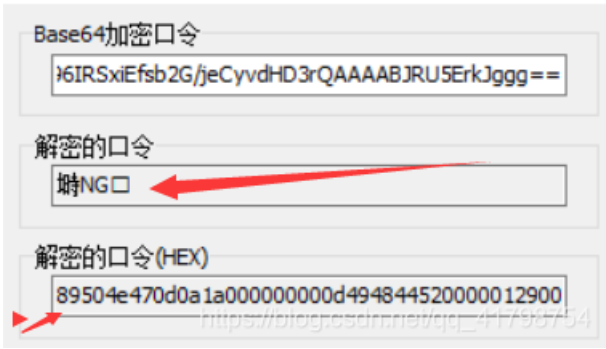
附件下载后是个runable.zip文件，首先解压一下，得到runable.exe，双击运行，发现无法运行

这个时候首先想到放进winhex里面，看看有没有什么隐藏的信息，看右边发现是编码，拉到最下面看到==，疑似base64编码

runnable.exe

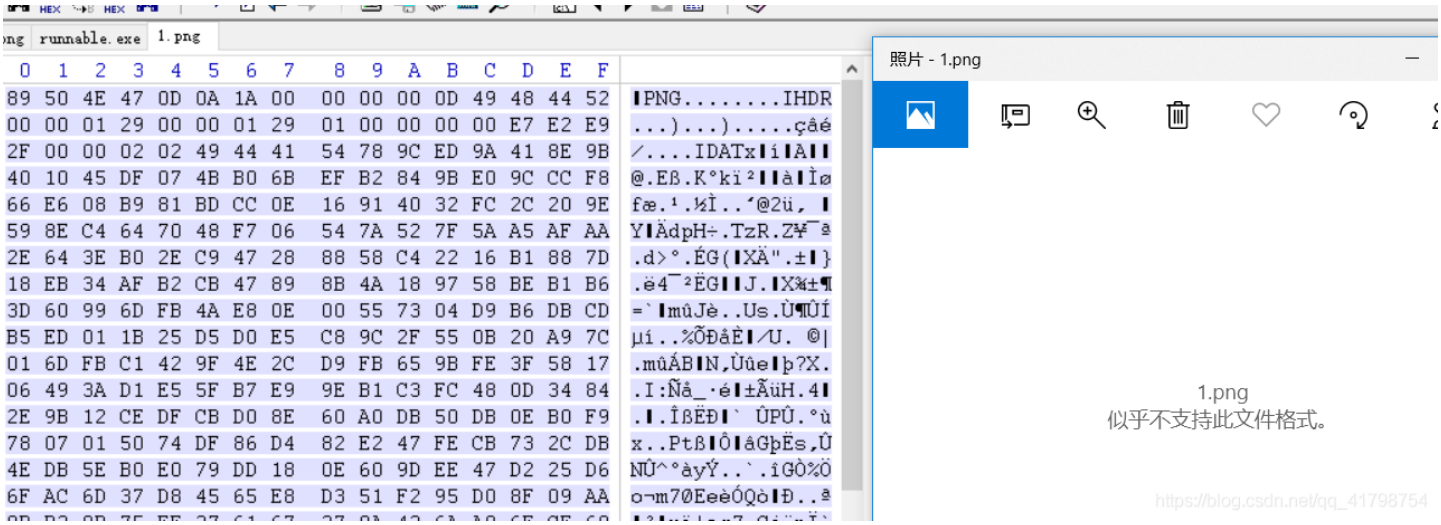
1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
65	56	55	74	41	43	4F	33	72	73	57	57	37	4A	33	xeVUtAC03rsWW7J3
51	54	33	73	79	63	55	62	66	62	51	57	78	72	48	8QT3sycUbfbQWxrH
46	32	48	5A	5A	36	41	52	67	6F	50	57	54	57	45	7F2HZZ6ARgoPWTWE
6D	76	4A	35	34	32	31	2F	64	50	59	30	72	58	68	HmvJ5421/dPY0rXh
48	41	76	42	32	6B	79	7A	66	33	34	4D	39	65	6B	xHAvB2kyzf34M9ek
62	58	74	42	78	74	54	53	36	70	61	30	67	6E	56	jbXtBxtTS6pa0gnV
50	63	63	69	33	4E	73	4B	31	5A	69	2B	50	31	71	FPcci3NsK1Zi+P1q
30	2B	38	71	78	77	6F	32	75	69	39	71	37	48	6E	M0+8qxwo2ui9q7Hn
43	4A	30	53	6C	69	6D	46	51	6D	63	66	64	74	63	tCJ0SlimFQmcfdtc
78	36	77	50	39	4F	4B	4C	6A	77	30	4A	79	33	70	2x6wP9OKLjw0Jy3p
48	41	2F	62	71	35	74	44	39	67	79	72	56	69	47	BHA/bq5tD9gyrViG
64	79	50	67	79	52	6F	71	75	69	39	6E	34	6C	6C	QdyPgyRoqui9n4ll
30	75	2B	51	76	59	41	31	78	44	62	69	73	2F	45	D0u+QvYA1xDbis/E
6F	50	73	47	6B	4A	33	6B	4C	6D	63	76	6D	54	54	hoPsGkJ3kLmcvmTT
57	4D	73	42	59	4D	39	58	2B	6E	4D	6C	77	39	32	HWMsBYM9X+nMlw92
7A	35	72	69	56	67	35	72	4D	55	47	7A	53	4D	32	nz5riVg5rMUGzSM2
69	46	42	76	67	4A	59	71	6C	39	42	32	7A	2B	4E	siFBvgJYql9B2z+N
51	44	43	32	33	39	38	36	66	4B	61	50	54	44	45	HQDC23986fKaPTDE
39	36	49	52	53	78	69	45	66	73	62	32	47	2F	6A	+96IRSxiEfsb2G/j
43	79	76	64	48	44	33	72	51	41	41	41	41	42	4A	eCyvdHD3rQAAAABJ
55	35	45	72	6B	4A	67	67	67	3D	3D					RU5ErkJggg==

解码一下，发现了有意思的东西，解密的口令是**xxxNG**，而下面的**HEX**值是**89504e47**开头，哈

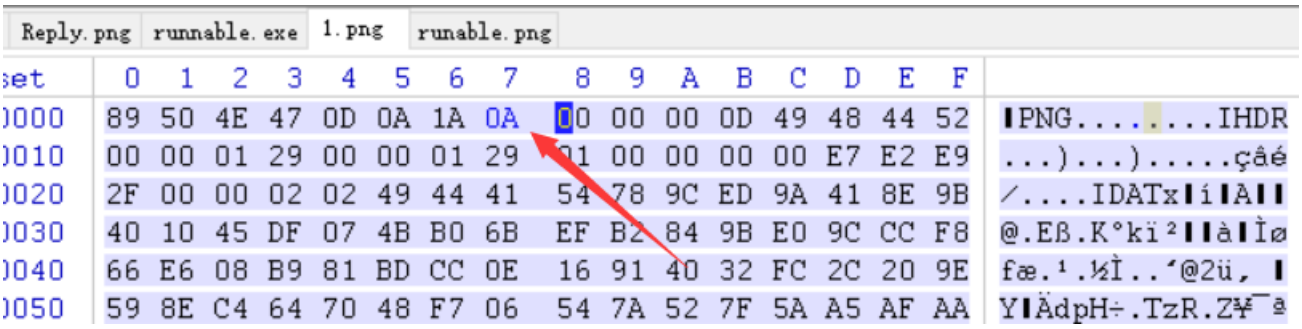


哈，想到了什么，**bingo**！就是**png**图片

然后复制**hex**值，打开**winhex**，构造一个文件，将值复制进去，保存得到一个**png**图片，然后打开文件，发现文件打不开



再次回到winhex，对比了一下其他png文件，发现文件头第七位00有问题,将其改为png正确的头



再次保存文件，发现能打开了，打开后是个二维码，扫码得到Flag!

8。倒立屋

倒立屋

100

1166 solves

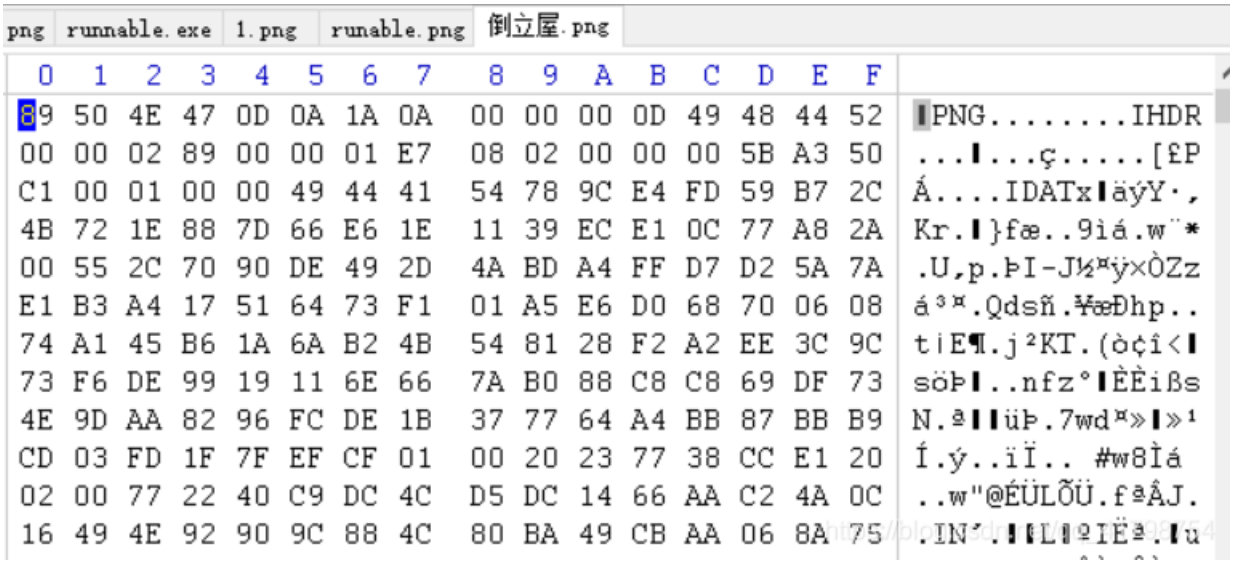
房屋为什么会倒立！是重力反转了吗？

附件下载

Flag

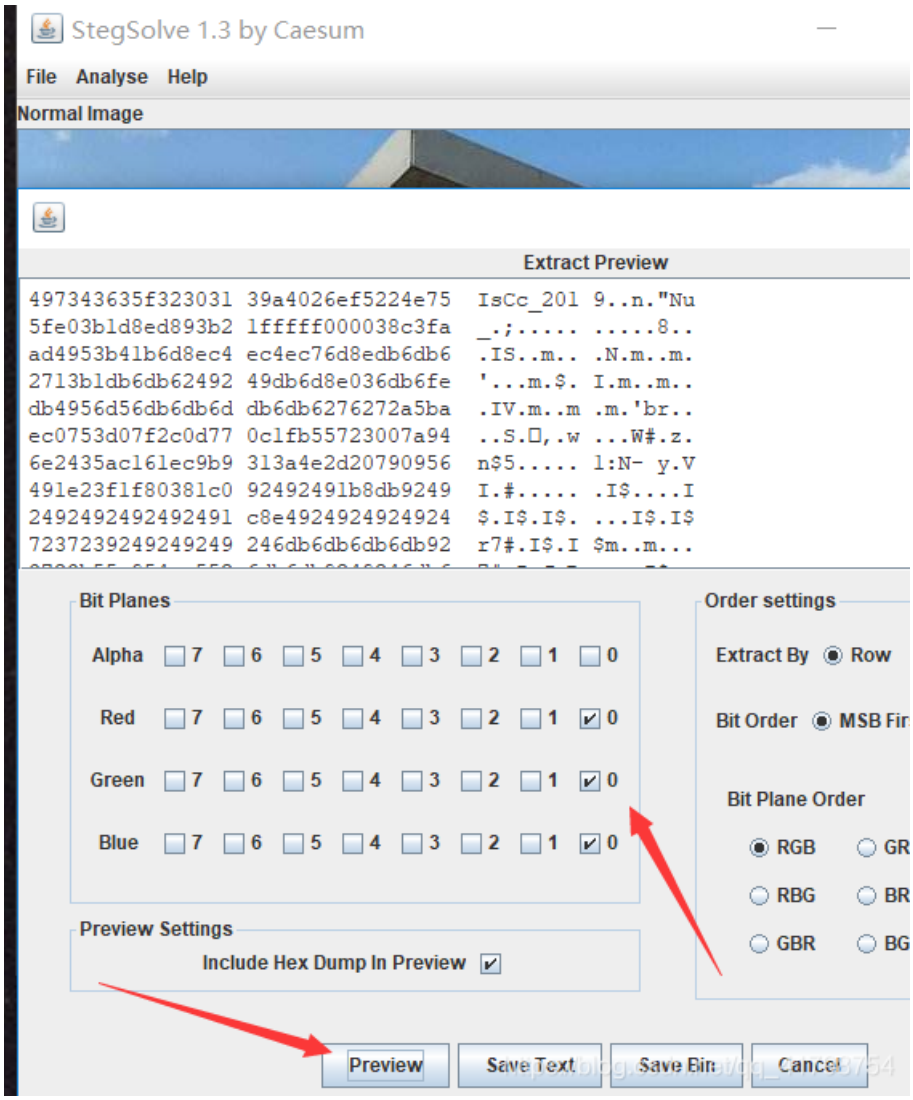
提交

下载附件，额...不出意外还是zip文件，解压后是个png图片，首先放进winhex里面看一下，没有



发现什么端倪

打开Stegsolve看看，点Analyse—Date Extract，然后最低位0逐个试一下，点Preview提交，发现了有字母，拉到最上面看一下，发现了第一行疑似Flag，去提交试一试，发现不对，刚开始认为

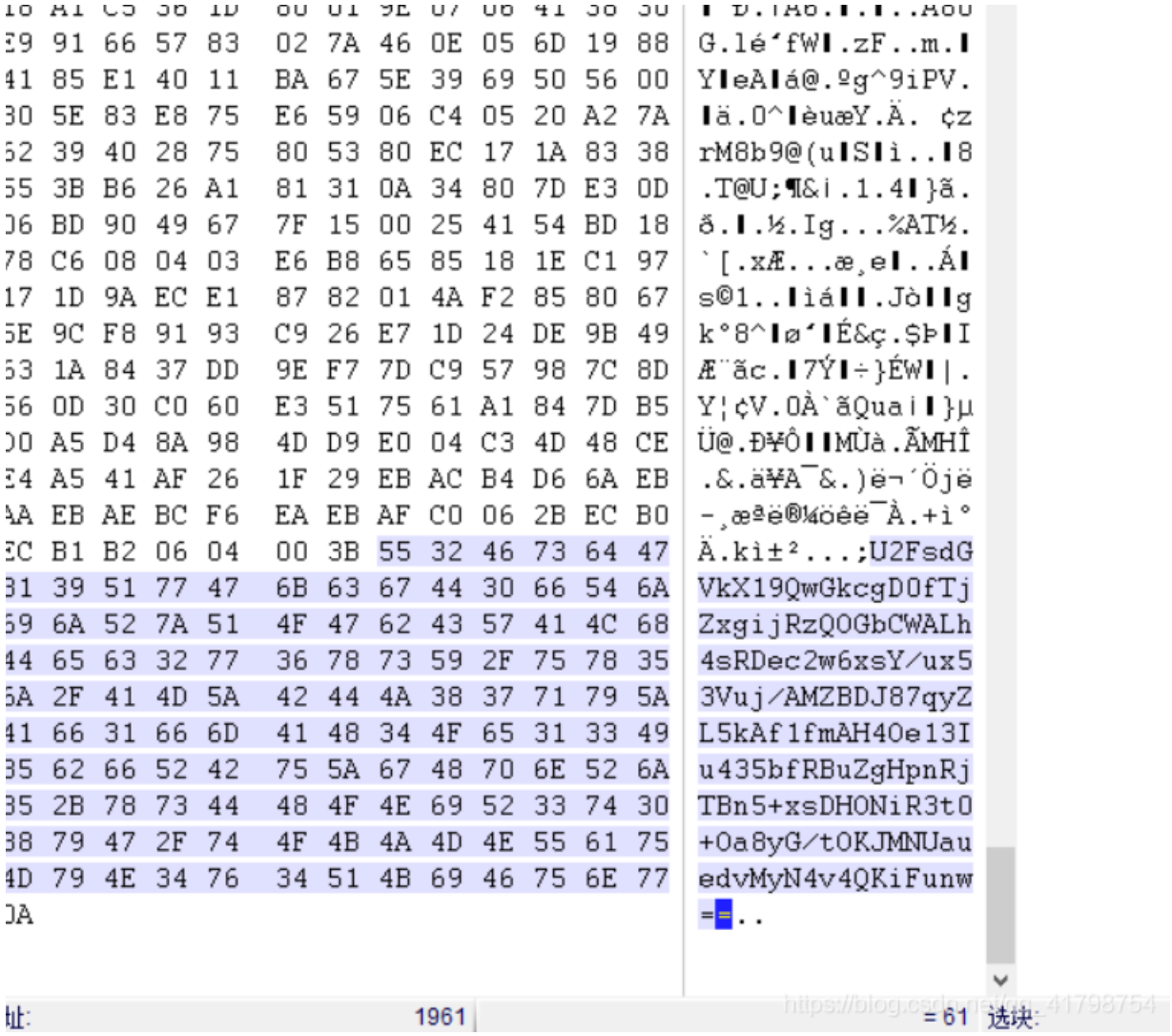


是格式不对，换了很多还是不对

这时候得到学长提示说再看一看题目，题目是倒立屋，倒立”，“反转”，于是重新构造flag倒过来写：9102_cCsl，提交之后发现成功！（本题考了LSB隐写）

9.Aesop’s secret

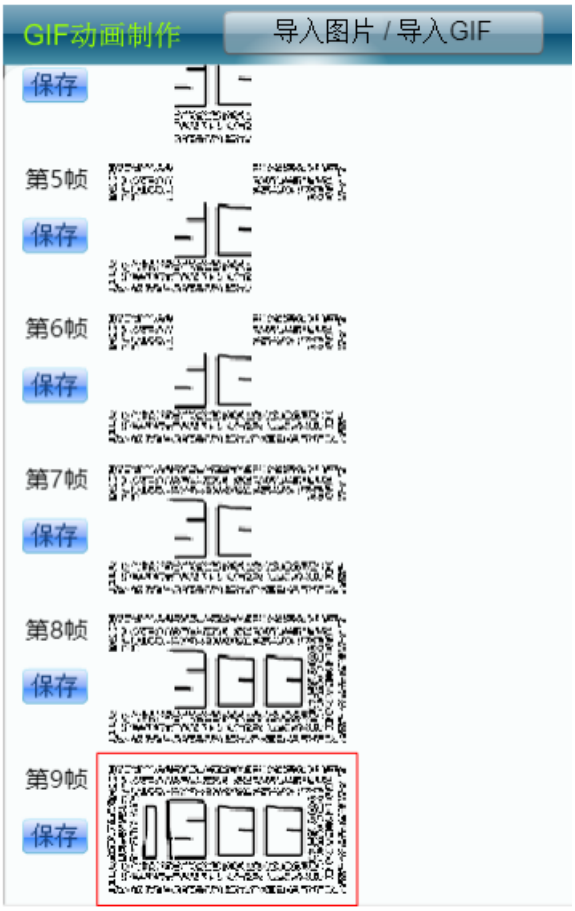
附件下载后，是个gif图片，跳得很快，看不清什么东西，拖进winhex里面看一看，发现有个



base64编码

解一下码，得到一串乱码，Salted_P开头，查了一下发现是AES加密，但是解密需要密码

再次回到前面，分解一下gif动图，在第九张图发现了ISCC字样，试试iscc当作密码



注：动画的帧速是按秒算，默认是0.2

解密了一下，发现还是编码，再次解密，得到Flag！！

在线加密解密(采用Crypto-JS实现)

Feedback

加密/解密 | 散列/哈希 | BASE64 | 图片/BASE64转换

明文:

U2FsdGVkX18OvTUlZubDnmvk2lSAkb8Jt4Zv6UWpE7Xb43f8uzeFRUKGMo6QaaNFHZriDDV0EQ/qt38Tw73tbQ==

加密算法:

- AES
- DES
- RC4
- Rabbit
- TripleDes

密码:

ISCC

加密 >

< 解密

密文:

U2FsdGVkX19QwGkcgD0fTjZxgijRzQOGbCWALh4sRDec2w6xsY/ux53Vuj/AMZBDJ87qyZL5kAf1fmAH4Oe13lu435bfRBuZgHpnRjTBn5+xsDHONiR3t0+Oa8yG/tOKJMNUauedvMyN4v4QKiFunw==

在线加密解密(采用Crypto-JS实现)

Feedback

加密/解密 | 散列/哈希 | BASE64 | 图片/BASE64转换

明文:

flag{DugUpADiamondADeepDarkMine}

加密算法:

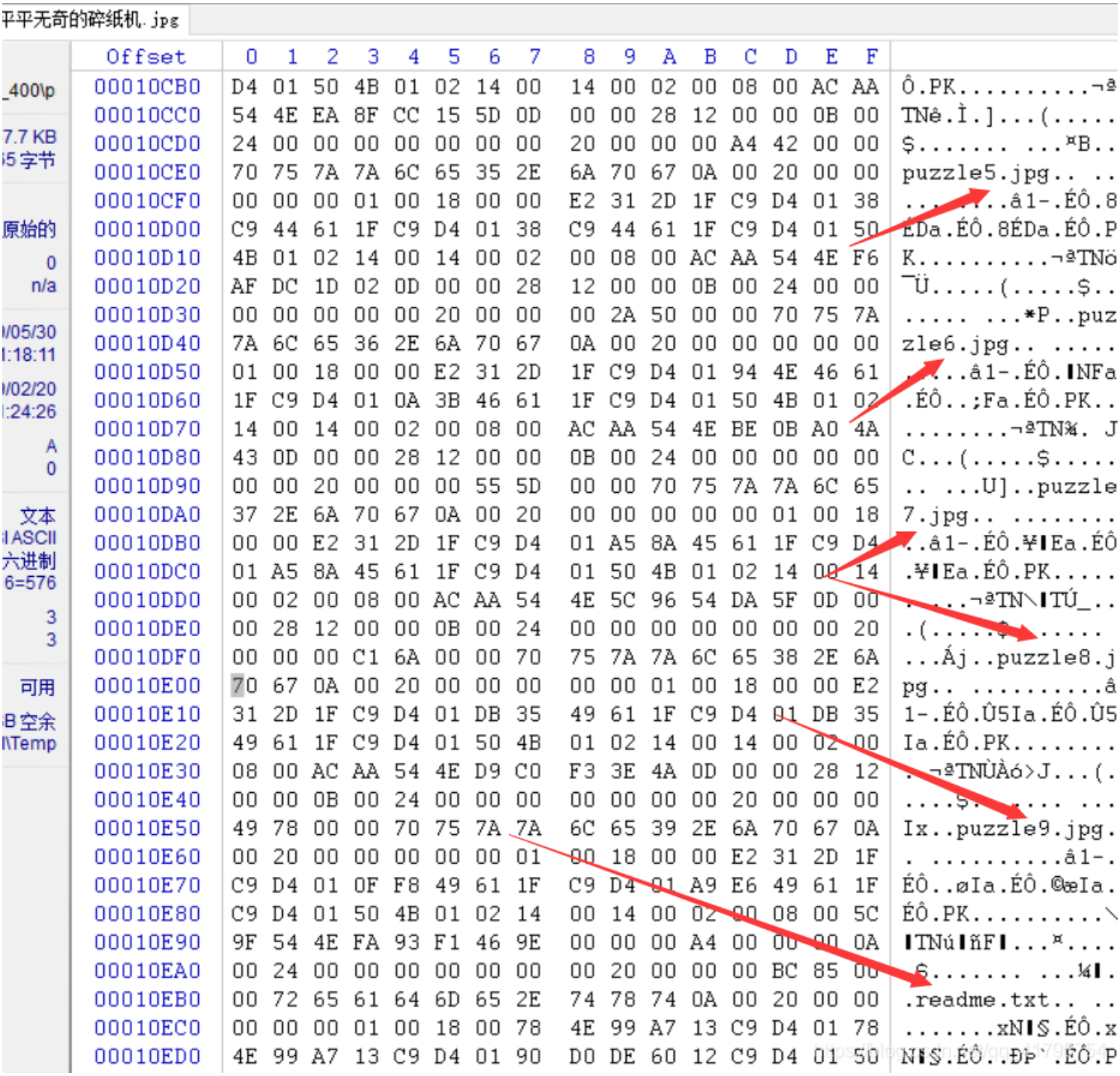
- AES
- DES
- RC4

密文:

U2FsdGVkX18OvTUlZubDnmvk2lSAkb8Jt4Zv6UWpE7Xb43f8uzeFRUKGMo6QaaNFHZriDDV0EQ/qt38Tw73tbQ==

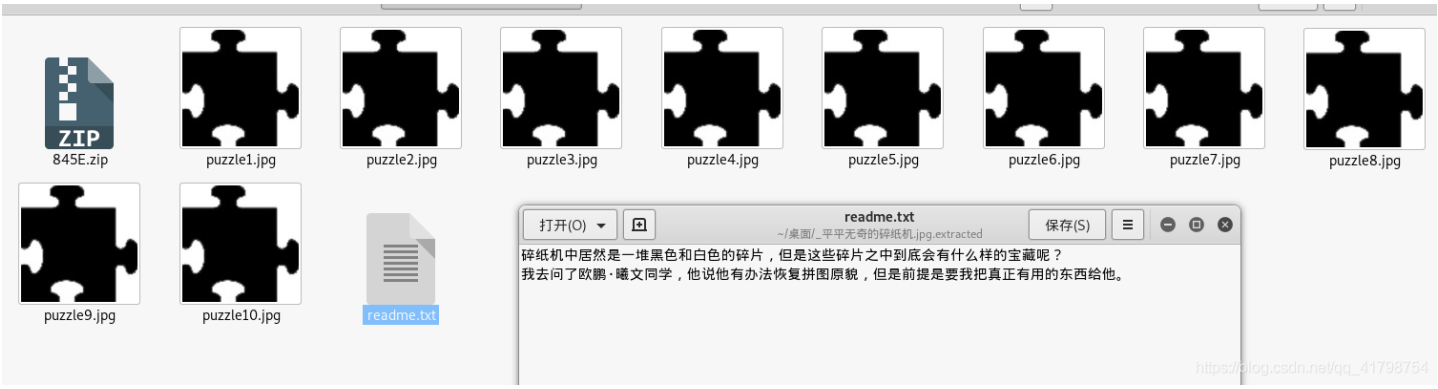
10.碎纸机

下载附件解压打开后是个图片，放进winhex里面看一下，发现里面含有其他文件



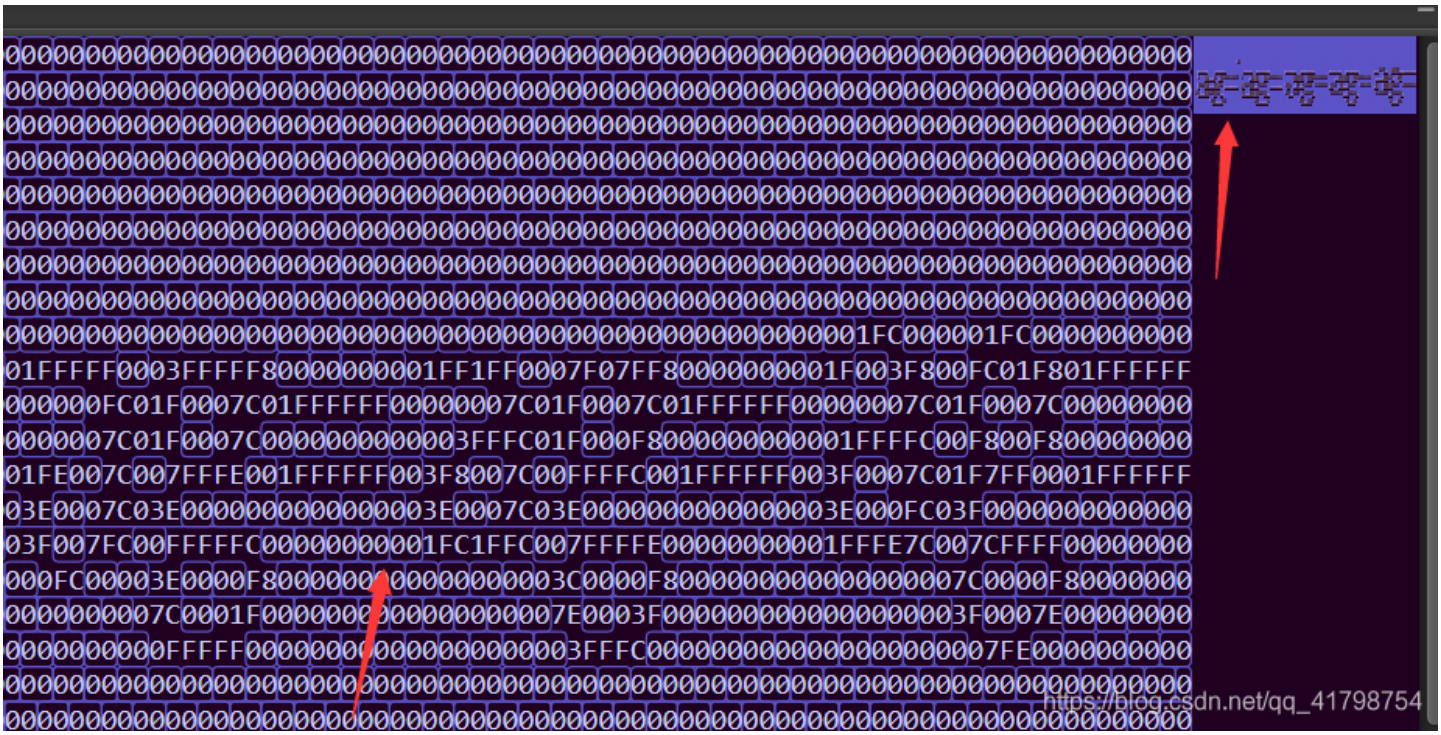
在binwalk里分离一下，得到很多图片和一个.txt文件，打开txt文件，，如题，让找欧朋曦文同学，呃呃呃，谁知道这位同学在哪

```
文件(F)  编辑(E)  查看(V)  搜索(S)  终端(T)  帮助(H)
root@kali:~/桌面# binwalk -e 平平无奇的碎纸机.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
33886         0x845E          Zip archive data, at least v2.0 to extract, compre
ssed size: 3227, uncompressed size: 4648, name: puzzle1.jpg
37154         0x9122          Zip archive data, at least v2.0 to extract, compre
ssed size: 3300, uncompressed size: 4648, name: puzzle10.jpg
40496         0x9E30          Zip archive data, at least v2.0 to extract, compre
ssed size: 3443, uncompressed size: 4648, name: puzzle2.jpg
43980         0xABCC          Zip archive data, at least v2.0 to extract, compre
ssed size: 3511, uncompressed size: 4648, name: puzzle3.jpg
47532         0xB9AC          Zip archive data, at least v2.0 to extract, compre
ssed size: 3373, uncompressed size: 4648, name: puzzle4.jpg
50946         0xC702          Zip archive data, at least v2.0 to extract, compre
ssed size: 3421, uncompressed size: 4648, name: puzzle5.jpg
54408         0xD488          Zip archive data, at least v2.0 to extract, compre
ssed size: 3330, uncompressed size: 4648, name: puzzle6.jpg
57779         0xE1B3          Zip archive data, at least v2.0 to extract, compre
ssed size: 3395, uncompressed size: 4648, name: puzzle7.jpg
61215         0xEF1F          Zip archive data, at least v2.0 to extract, compre
ssed size: 3423, uncompressed size: 4648, name: puzzle8.jpg
64679         0xFCA7          Zip archive data, at least v2.0 to extract, compre
```

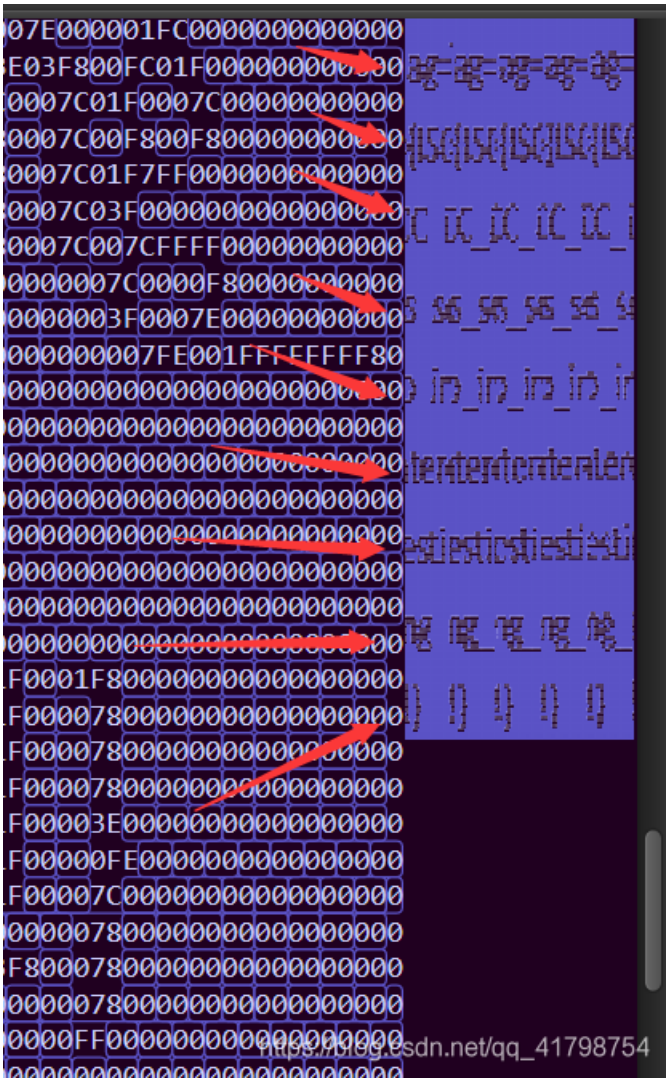


继续回到图片，将拼图放进winhex里面，拉到最下面，发现最下面有东西，把十六进制复制下来，放到sublime中，搜索00打开高亮，看到有形状，接着不断调整大小，可以看到字母FI

继续看下一副图，得到ag=，请注意图中有重复部分，要注意观察



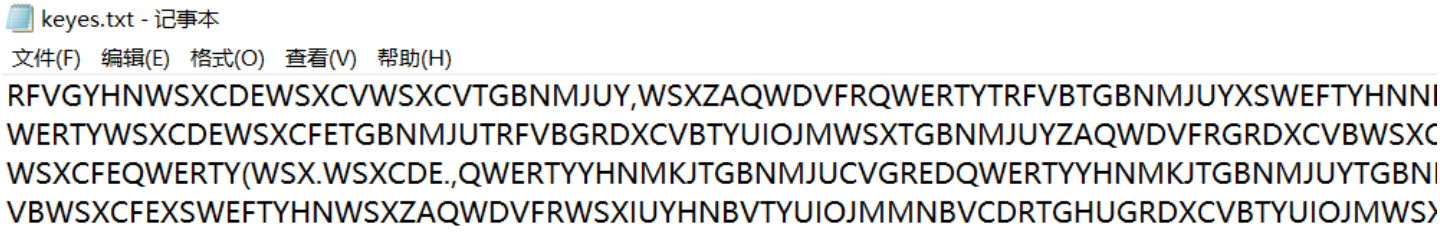
依次打开每个图，最后拼出来Flag={ISCC_is_so_interesting_!}，真的是看的头大，连蒙带猜的。



11.Keyes' secret

下载附件解压后是一个txt文件，打开后是很多大写字母，看题目发现是键盘密码，这题可以一个一个画啊，不过非常非常麻烦，另一种就是写个python脚本了，也需要画出字母代表的意义，比

如：‘MNBVCDRTGHU’: ‘r’, ‘NBVCXSWERF’: ‘p’, ‘EFVGYWDCFT’: ‘w’



反正我是没写出来，哈哈哈，第一次见这种题目，又看到其他人解题方法，网上有键盘密码的字典！

重点来咯！！2019—ISCC题目的下载地址
https://download.csdn.net/download/qq_41798754/11218568

CTF隐写工具包下载地址：https://download.csdn.net/download/qq_41798754/11218577