

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](#)

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_41798754/article/details/90716743

版权



[ISCC 专栏收录该内容](#)

1 篇文章 1 订阅

订阅专栏

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。你能够帮助我还原文明吗? 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。

message.txt	2019/2/19 10:12	文本文档	1 KB
message.zip	2019/5/18 13:03	ZIP 压缩文件	1 KB

message.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
0126 062 0126 0163 0142 0103 0102 0153 0142 062 065 0154 0111
```

八进制转十进制, 再转Ascii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

解密成绩单

100

722 solves

老师为了保密将某门课程的成绩单进行了加密处理，但在查成绩时忘记了自己原来是怎样进行了加密，你能帮同学们顺利查到成绩吗？

附件下载

Flag

Submit

https://blog.csdn.net/qq_41798754

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！

ILSpy

File View Help

C# C# 7.3 / VS 20...

r18 : float
r19 : float
r20 : float
r21 : float
r22 : float
r23 : float
r24 : float
r25 : float
r26 : float
r27 : float
r28 : float
r29 : float
txtPassword : TextBox
txtUsername : TextBox
score_list()
btnCancel_Click(object, EventArgs)
btnLogin_Click(object, EventArgs) :
checkPassword() : bool
checkUsername() : bool
Dispose(bool) : void
InitializeComponent() : void
showError() : void
showLoginCountExceeded() : void

```
// Score_List.score_list  
private bool checkPassword()  
{  
    return txtPassword.Text == "ISCCq19pc1Yhb6SqtGhliYH6"  
}
```

Score_List.Properties

https://blog.csdn.net/qq_41798754



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	
方 节 的 0 /a 16 50 29 41 A 0 本 制 76 3 3		000082D0	68	4F	28	0F	5B	4E	90	47	B3	09	17	DB	3A	C3	15	9F	h0([N.G³..Û:Ã.!
		000082E0	E4	D0	5D	43	B9	BF	05	1B	3F	20	48	79	30	9F	70	B1	äD]C¹¿...? Hy0 p±
		000082F0	DC	0C	1B	6E	64	9E	43	BB	41	1F	6B	8D	DA	F3	5A	66	Û..nd C»A.k.ÚóZf
		00008300	26	16	57	F1	DE	E7	63	40	A6	7F	EF	F9	B8	FC	3F	93	&.Wñpçc@! .iù,ü?!
		00008310	39	E4	90	43	0E	39	E4	90	43	00	7F	00	6A	A4	82	6D	9ä.C.9ä.C...jª 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.....éçYN.±
		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	í...IDATx i É.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	B3	29	3F	.) ¥ª.ñ. Á .)?
		000083B0	16	01	82	24	1B	D9	B1	86	07	03	B6	F8	C1	43	78	30	..!\$..Û± ...ªÁCx0
		000083C0	6F	DA	C4	6F	AF	FC	E9	F7	19	70	C8	21	87	1C	72	C8	oÚÀo~üé+.pÈ! .rÈ
	000083D0	21	87	9E	13	B2	BE	06	C8	E3	6A	C0	6A	36	01	36	95	! !.²ª.ÈäJÀj6.6	
	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	Á äÐG@äl...!Mâ\$	
	00008410	A2	64	13	D0	2C	C8	BD	C4	73	68	37	68	78	FF	41	1E	çd.Ð.ÈkÄsh7hxyÄ.54	
	00008420	02	2A	0E	0A	2B	01	2D	E4	F1	FF	2E	0E	42	77	07	24	ÿ.../T04% C... 4	

直接丢到binwalk里面

```

root@kali:~/桌面# binwalk -e Misc-01.jpg
BMP
png 22.jpg 123456cry.jpg bad bestwing1234567
-----
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
runnable.txt
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
https://blog.csdn.net/qq_41798754

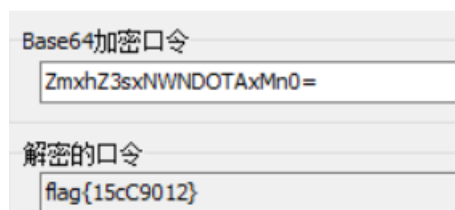
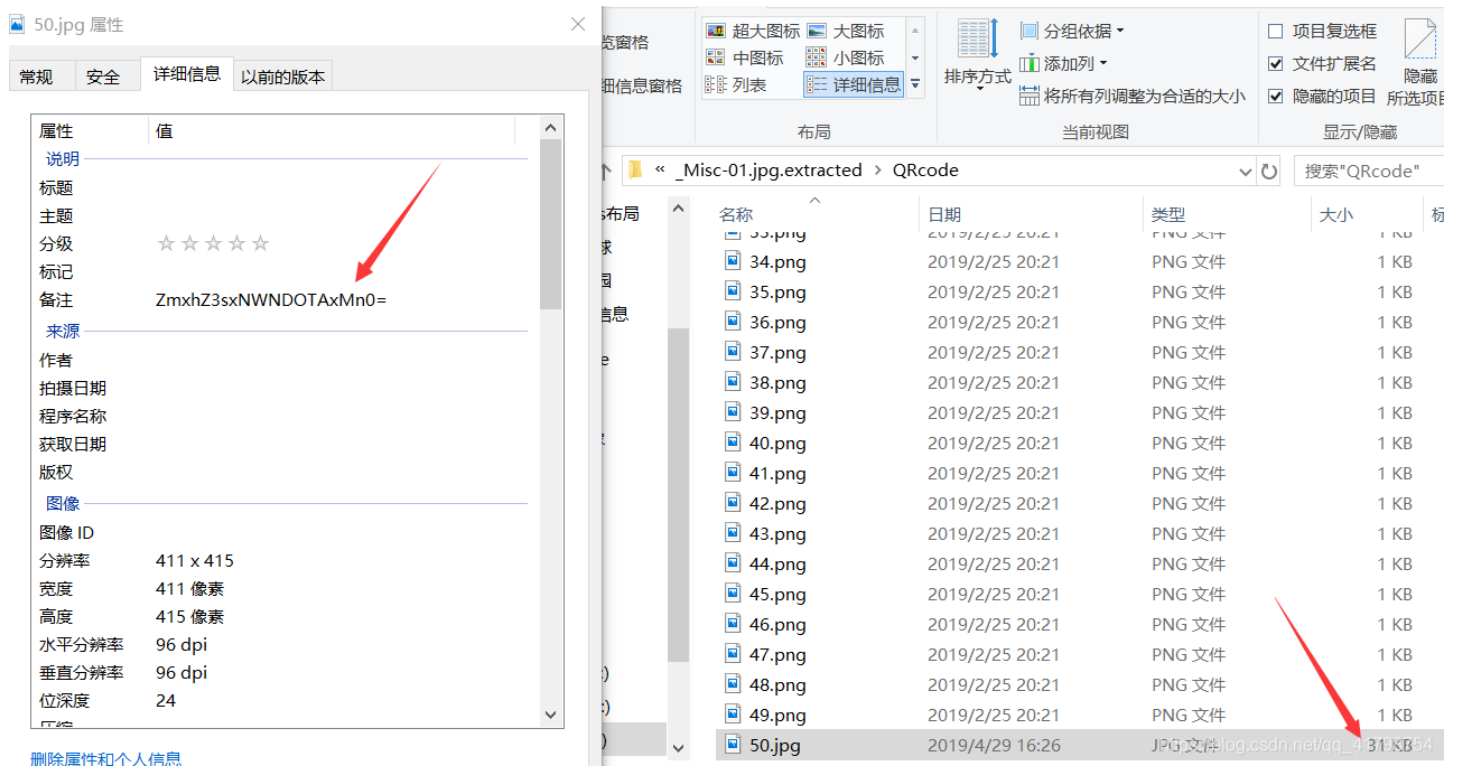
```

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

High起来!

200

676 solves

酷爱音乐的你，在听歌的过程中突然收到音乐发烧友发来的一封神秘的邮件，邮件里什么都没有说，只有一个被损坏的图片。这名歌友到底要向你传达什么信息呢？答案或许就隐藏在这个损坏的文件中...

附件下载

Flag

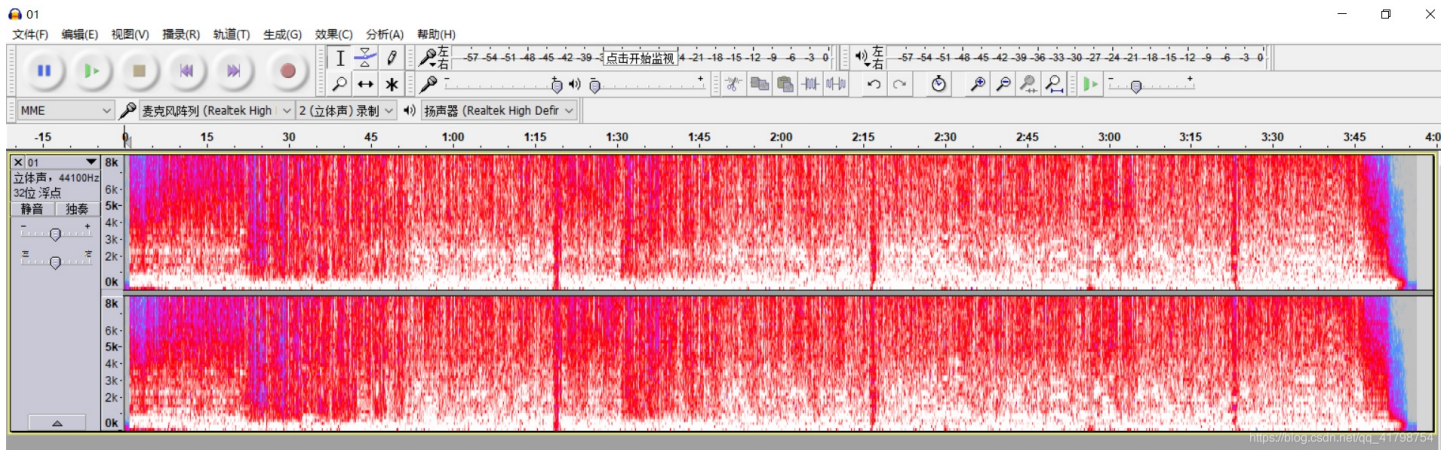
Submit

https://blog.csdn.net/qq_41798754

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！

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
000000	12	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	.PNG.....IHDR
000010	00	00	01	72	00	00	01	72	01	00	00	00	00	C0	5F	6C	...r...r.....À_1
000020	A4	00	00	02	84	49	44	41	54	78	9C	ED	9A	4D	6E	DB	¸... IDATx i MnÛ
000030	30	10	46	DF	94	DA	D3	40	0E	E0	A3	48	37	E8	91	72	0.FB ÚÓ@.à£H7è'r
000040	A6	DC	40	3C	4A	6F	20	2D	0B	50	F8	BA	20	69	33	A9	!Û@<Jo -.Pøº i3@

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



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

名称	修改日期	类型	大小
decoder	2019/5/18 12:47	文件夹	
encoder	1998/8/8 23:40	文件夹	
gzip	1998/8/8 23:40	文件夹	
stegolib	1998/8/8 23:40	文件夹	
tables	2019/5/18 12:47	文件夹	
01.mp3	2019/4/29 17:24	MP3 文件	3,696 KB
Decode.exe	1999/2/11 11:37	应用程序	156 KB
Encode.exe	1999/2/11 11:36	应用程序	261 KB
mp3stego-gui.zip	2016/9/29 1:50	ZIP 压缩文件	339 KB
MP3Steno.exe	1998/9/16 18:16	应用程序	289 KB
README.txt	1998/8/8 23:51	文本文档	4 KB
ser0.1tmp	2019/5/18 12:17	1TMP 文件	3 KB
ser0.tmp	2019/5/18 12:17	TMP 文件	3 KB

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!

名称	修改日期	类型	大小
decoder	2019/5/18 12:47	文件夹	
encoder	1998/8/8 23:40	文件夹	
gzlib	1998/8/8 23:40	文件夹	
stegolib	1998/8/8 23:40	文件夹	
tables	2019/5/18 12:47	文件夹	
01.mp3	2019/4/29 17:24	MP3 文件	3,696 KB
01.mp3.pcm	2019/5/30 22:52	PCM 文件	40,741 KB
01.mp3.txt	2019/5/30 22:52	文本文档	1 KB
Decode.exe	1999/2/11 11:37	应用程序	156 KB
Encode.exe	1999/2/11 11:36	应用程序	261 KB
mp3stego-gui.zip	2016/9/29 1:50	ZIP 压缩文件	339 KB
MP3Steno.exe	1998/9/16 18:16	应用程序	289 KB
README.txt	1998/8/8 23:51	文本文档	4 KB

```

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"
https://blog.csdn.net/qq_41798754

```

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!

Unicode编码 UTF-8编码 URL编码/解码 Unix时间戳 Ascii/Native编码互转

```

&#102;&#108;&#97;&#103;&#123;&#80;&#114;&#69;&#116;&#84;&#121;&#95;&#49;&#83;&#99;&#67;&#57;&#48;&#49;&#50;&#95;&#103;&#79;&#48;&#100;&#125

```

flag{PrEtTy_1ScC9012_gO0d}

https://blog.csdn.net/qq_41798754

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

https://blog.csdn.net/mg_42773804
https://blog.csdn.net/mg_42773804

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

Base64加密口令

UEFTUyJ3QjBLX0lftDBWM19ZMHUIMjEIN0Q=

解密的口令

PASS%7B0K_I_L0V3_Y0u%21%7D



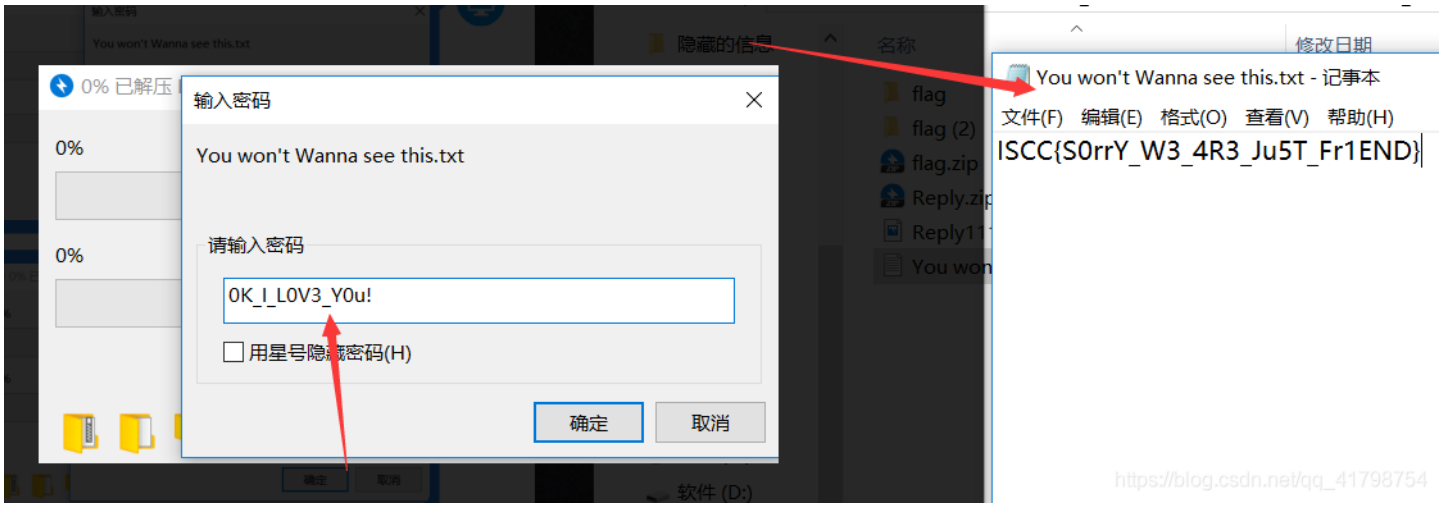
用软件Converter中的Unescape再次解码得到

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	ï	â	J	'	.	T	.	V	=	P	.	â	À	e	.	
55	25	5A	05	AA	40	03	AB	1E	A8	02	55	h	`]	f	U	%	Z	.	â	@	.	«	.	"	.	U
0B	4D	64	1D	30	9F	3D	47	18	00	00	00	à	2	.	ü	.	M	d	.	0	!	=	G
44	AE	42	60	82	50	4B	03	04	0A	00	01	.	I	E	N	D	@	B	`	!	P	K
78	53	4E	DD	AE	E9	B6	2A	00	00	00	1E
00	00	00	59	6F	75	20	77	6F	6E	27	74
6E	61	20	73	65	65	20	74	68	69	73	2E
6A	A0	34	F2	94	42	06	F1	C8	02	E2	B9	t	x	t	q	j		4	ò	!	B	.	ñ	È	.	â	¹
75	63	E2	45	41	44	3B	45	48	22	4E	FB	!	\$	v	I	u	c	â	E	A	D	;	E	H	"	N	ù
45	99	84	66	BC	6C	DF	AF	20	50	4B	01	!	!	!	!	!	!	!	!	!	!	!	!	!	!	!	!
00	01	08	00	00	15	78	53	4E	DD	AE	E9	.	?
00	1E	00	00	00	1C	00	24	00	00	00	00	!	!	!	!	!	!	!	!	!	!	!	!	!	!	!	!
00	00	00	00	00	00	00	59	6F	75	20	77
20	57	61	6E	6E	61	20	73	65	65	20	74
74	78	74	0A	00	20	00	00	00	00	00	01
0A	1E	D3	20	C8	D4	01	C3	6F	B2	1B	95
6F	B2	1B	95	C7	D4	01	50	4B	05	06	00	Ç	Ô	.	Ã	o	²	.	!	Ç	Ô	.	Ã	o	²	.	!
00	01	00	6E	00	00	00	64	00	00	00	00

https://blog.csdn.net/qq_41798754

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

无法运行的exe

150

850 solves

可执行文件无法运行，你是否能修复它？

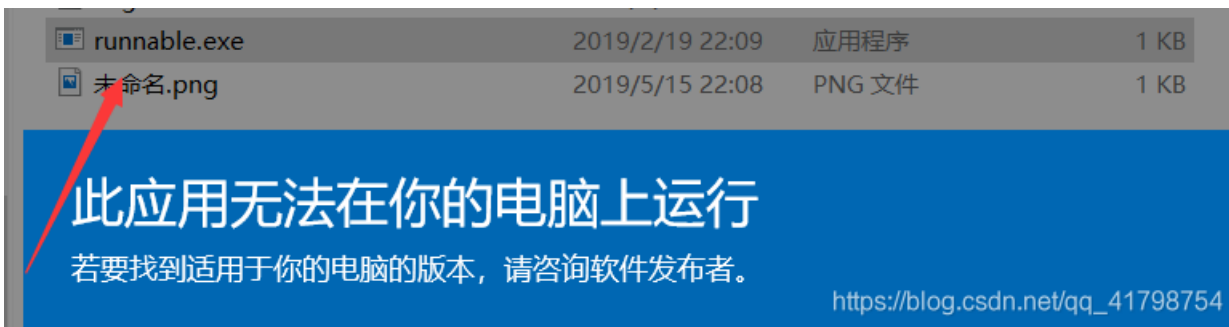
附件下载

Flag

提交

https://blog.csdn.net/qq_41798754

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

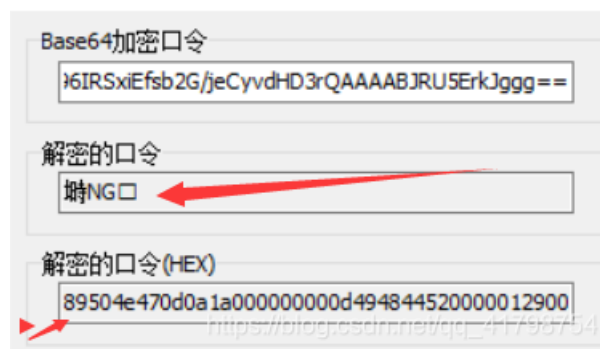


这个时候首先想到放进winhex里面，看看有没有什么隐藏的信息，看右边发现是编码，拉到最下面看到==，疑似base64编码

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	8QT3syncUbfbQWxrH
46	32	48	5A	5A	36	41	52	67	6F	50	57	54	57	45	7F2HZZ6ARgoPWlWE
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+Plq
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	tCJOSlimFQmcfdtc
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	QdyPgyRoqui9n4l1
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==

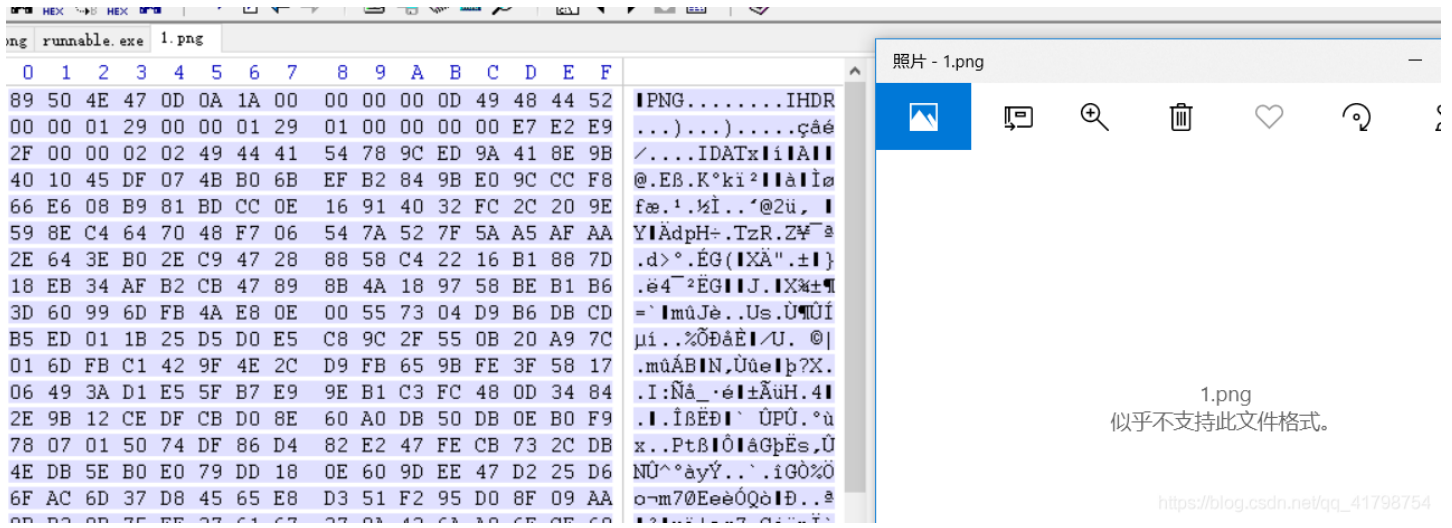
https://blog.csdn.net/qq_41798754

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

set	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
1000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	!PNG....IHDR
1010	00	00	01	29	00	00	01	29	01	00	00	00	00	E7	E2	E9	...)...)....çâé
1020	2F	00	00	02	02	49	44	41	54	78	9C	ED	9A	41	8E	9B	/....IDATx i A
1030	40	10	45	DF	07	4B	B0	6B	EF	B2	84	9B	E0	9C	CC	F8	@.EB.K°ki² à Iø
1040	66	E6	08	B9	81	BD	CC	0E	16	91	40	32	FC	2C	20	9E	fæ.¹.¼Ï..'@2ü,
1050	59	8E	C4	64	70	48	F7	06	54	7A	52	7F	5A	A5	AF	AA	Y ÄdpH+.TzR.Z¥~ª

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

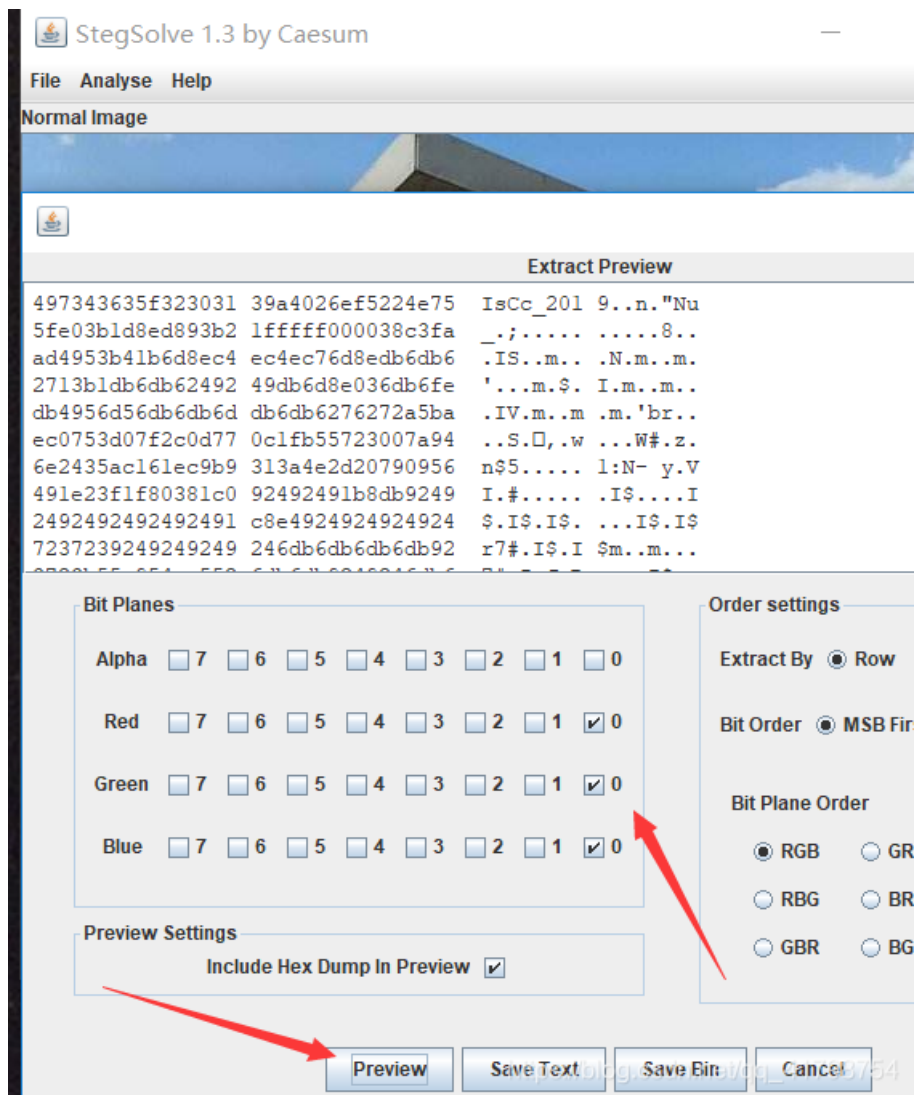
https://blog.csdn.net/qq_41798754

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

png	runnable.exe	1.png	runable.png	倒立屋.png												
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	PN
00	00	02	89	00	00	01	E7	08	02	00	00	00	5B	A3	50	...
C1	00	01	00	00	49	44	41	54	78	9C	E4	FD	59	B7	2C	Á...
4B	72	1E	88	7D	66	E6	1E	11	39	EC	E1	0C	77	A8	2A	Kr.}
00	55	2C	70	90	DE	49	2D	4A	BD	A4	FF	D7	D2	5A	7A	.U,p.
E1	B3	A4	17	51	64	73	F1	01	A5	E6	D0	68	70	06	08	á³
74	A1	45	B6	1A	6A	B2	4B	54	81	28	F2	A2	EE	3C	9C	tiE
73	F6	DE	99	19	11	6E	66	7A	B0	88	C8	C8	69	DF	73	söb
4E	9D	AA	82	96	FC	DE	1B	37	77	64	A4	BB	87	BB	B9	N.ä
CD	03	FD	1F	7F	EF	CF	01	00	20	23	77	38	CC	E1	20	í.y.
02	00	77	22	40	C9	DC	4C	D5	DC	14	66	AA	C2	4A	0C	..w"
16	49	4E	92	90	9C	88	4C	80	BA	49	CB	AA	06	8A	75	.IN

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

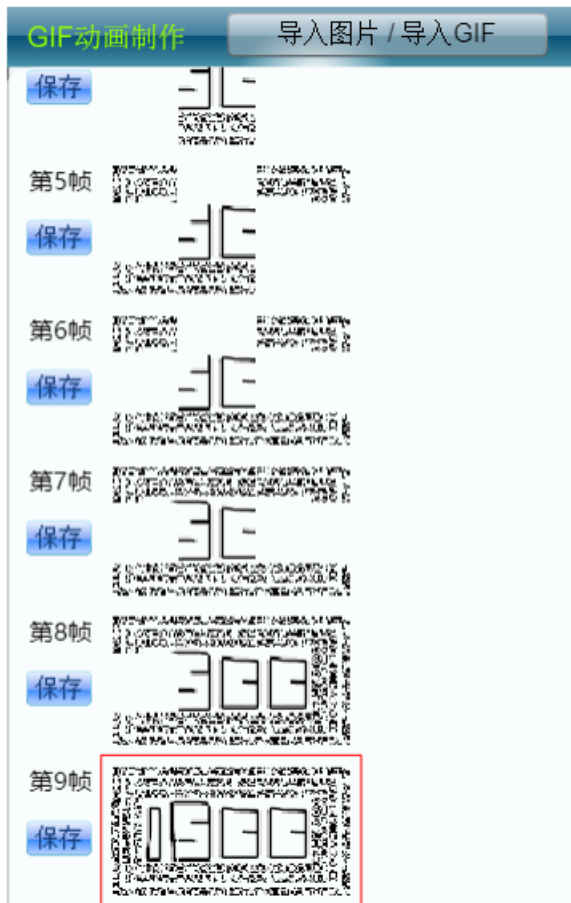
10	A1	C3	30	1D	00	01	9E	07	00	41	30	30	■	D..IAB..I..MOU
19	91	66	57	83	02	7A	46	0E	05	6D	19	88	G.lé'fWl.zF..m.■	
41	85	E1	40	11	BA	67	5E	39	69	50	56	00	YleAlá@.9g^9iPV.	
30	5E	83	E8	75	E6	59	06	C4	05	20	A2	7A	lä.0^lèuæY.Ä. çz	
52	39	40	28	75	80	53	80	EC	17	1A	83	38	rM8b9@(u S i..l8	
55	3B	B6	26	A1	81	31	0A	34	80	7D	E3	0D	.T@U;¶&i.1.4l}ä.	
06	BD	90	49	67	7F	15	00	25	41	54	BD	18	ä..l.¼.Ig...%AT¼.	
78	C6	08	04	03	E6	B8	65	85	18	1E	C1	97	`[.xÆ...æ,eI..ÁI	
17	1D	9A	EC	E1	87	82	01	4A	F2	85	80	67	s@1...liálll.Jòllg	
5E	9C	F8	91	93	C9	26	E7	1D	24	DE	9B	49	k°8^lè'IE&ç.\$P I	
53	1A	84	37	DD	9E	F7	7D	C9	57	98	7C	8D	Æ"äc.l7Y ÷}ÉW l.	
56	0D	30	C0	60	E3	51	75	61	A1	84	7D	B5	Y çV.OÀ`äQuail}µ	
00	A5	D4	8A	98	4D	D9	E0	04	C3	4D	48	CE	Ü@.Ð¥ÔllMÙà.ÄMHÍ	
34	A5	41	AF	26	1F	29	EB	AC	B4	D6	6A	EB	.&.ä¥A`&.)ë~'Öjë	
4A	EB	AE	BC	F6	EA	EB	AF	C0	06	2B	EC	B0	-,ææë@¼öëë`À.+i°	
3C	B1	B2	06	04	00	3B	55	32	46	73	64	47	Ä.kit±²...;U2FsdG	
31	39	51	77	47	6B	63	67	44	30	66	54	6A	VkX19QwGkcgD0fTj	
59	6A	52	7A	51	4F	47	62	43	57	41	4C	68	ZxgijRzQOGbCWALh	
44	65	63	32	77	36	78	73	59	2F	75	78	35	4sRDec2w6xsY/ux5	
5A	2F	41	4D	5A	42	44	4A	38	37	71	79	5A	3Vuj/AMZBDJ87qyZ	
41	66	31	66	6D	41	48	34	4F	65	31	33	49	L5kAf1fmAH40e13I	
35	62	66	52	42	75	5A	67	48	70	6E	52	6A	u435bfrRBuZgHpnRj	
35	2B	78	73	44	48	4F	4E	69	52	33	74	30	TBn5+xsDHONiR3t0	
38	79	47	2F	74	4F	4B	4A	4D	4E	55	61	75	+Oa8yG/tOKJMNUau	
4D	79	4E	34	76	34	51	4B	69	46	75	6E	77	edvMyN4v4QKiFunw	
JA													=■...	

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



https://blog.csdn.net/qn_41798754
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:

U2FsdGVkX18OvTUIZubDnmvk2ISAKb8Jt4Zv6UWpE7Xb43f8uzeFRU
KGMo6QaaNFHZriDDV0EQ/qt38Tw73tbQ==

加密算法:

- AES
- DES
- RC4
- Rabbit
- TripleDes

密码:

ISCC

加密 >

< 解密

密文:

U2FsdGVkX19QwGkcgD0fTjZxgijRzQOGbCWALh4sRDec2w6xsY/ux5
3Vuji/AMZBDJ87qyZL5kAf1fmAH4Oe13lu435bfRBuZgHpnRjTBn5+xs
DHONiR3t0+Oa8yG/tOKJMNUaedvMyN4v4QKIFunw==

https://blog.csdn.net/qq_41798754

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:

U2FsdGVkX18OvTUIZubDnmvk2ISAKb8Jt4Zv6UWpE7Xb43f8uzeFRU
KGMo6QaaNFHZriDDV0EQ/qt38Tw73tbQ==

https://blog.csdn.net/qq_41798754

10.碎纸机

碎纸机

400

1216 solves

“想要我的宝藏吗？如果想要的话，那就到碎纸机中找吧，我全部都放在那里。”

附件下载

Flag

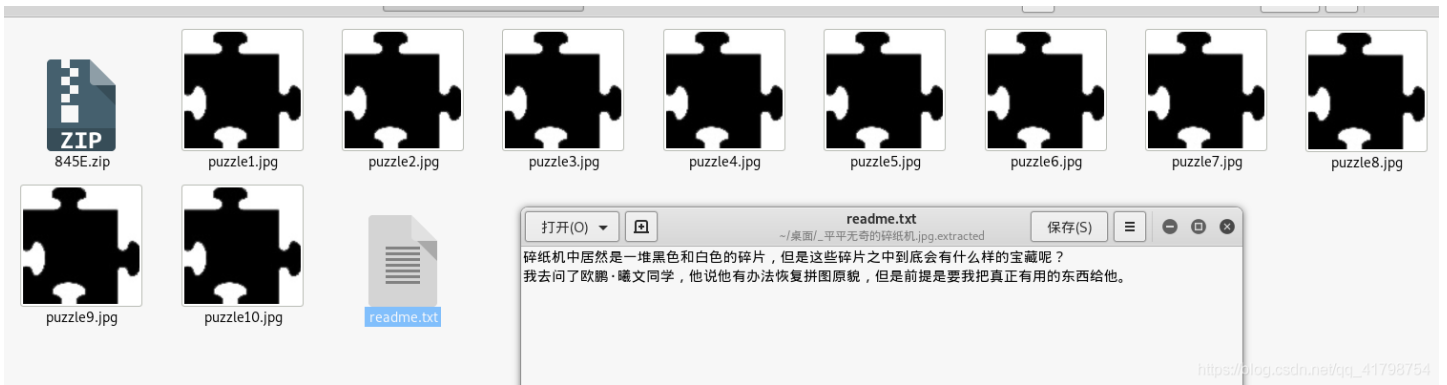
提交

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

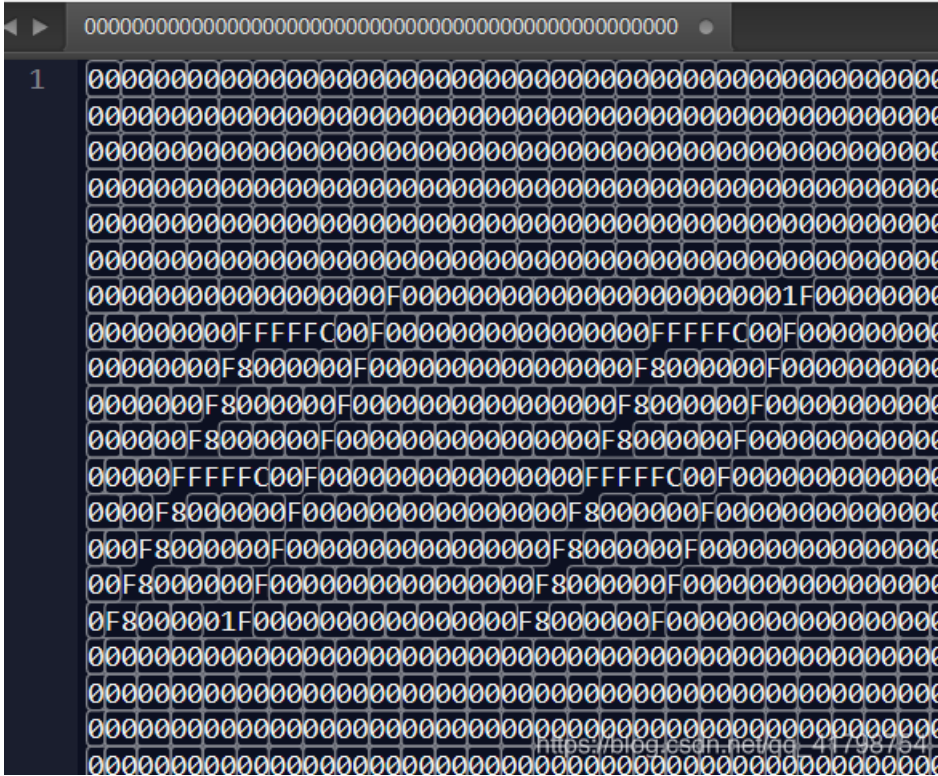
	Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
400ip	00010CB0	D4	01	50	4B	01	02	14	00	14	00	02	00	08	00	AC	AA	Ô.PK.....~ª
	00010CC0	54	4E	EA	8F	CC	15	5D	0D	00	00	28	12	00	00	0B	00	TNè.Ï.]...(.....
7.7 KB 15 字节	00010CD0	24	00	00	00	00	00	00	00	20	00	00	00	A4	42	00	00	\$. ¤B..
	00010CE0	70	75	7A	7A	6C	65	35	2E	6A	70	67	0A	00	20	00	00	puzzle5.jpg.. ..
原始的	00010CF0	00	00	00	01	00	18	00	00	E2	31	2D	1F	C9	D4	01	38	...v...â1-.ÉÔ.8
	00010D00	C9	44	61	1F	C9	D4	01	38	C9	44	61	1F	C9	D4	01	50	ÉDa.ÉÔ.8ÉDa.ÉÔ.P
0 n/a	00010D10	4B	01	02	14	00	14	00	02	00	08	00	AC	AA	54	4E	F6	K.....~ªTNö
	00010D20	AF	DC	1D	02	0D	00	00	28	12	00	00	0B	00	24	00	00	Ü.....(.....\$. .
/05/30 1:18:11	00010D30	00	00	00	00	00	20	00	00	00	2A	50	00	00	70	75	7A*P..puz
	00010D40	7A	6C	65	36	2E	6A	70	67	0A	00	20	00	00	00	00	00	zle6.jpg.. ..
/02/20 1:24:26	00010D50	01	00	18	00	00	E2	31	2D	1F	C9	D4	01	94	4E	46	61	...â1-.ÉÔ.NFa
	00010D60	1F	C9	D4	01	0A	3B	46	61	1F	C9	D4	01	50	4B	01	02	.ÉÔ.;Fa.ÉÔ.PK..
A 0	00010D70	14	00	14	00	02	00	08	00	AC	AA	54	4E	BE	0B	A0	4A~ªTN. J
	00010D80	43	0D	00	00	28	12	00	00	0B	00	24	00	00	00	00	00	C...(.....\$. .
文本 ASCII 十六进制 6=576	00010DA0	37	2E	6A	70	67	0A	00	20	00	00	00	00	00	01	00	18	7.jpg.. ..
	00010DB0	00	00	E2	31	2D	1F	C9	D4	01	A5	8A	45	61	1F	C9	D4	..â1-.ÉÔ.Ea.ÉÔ
3 3	00010DC0	01	A5	8A	45	61	1F	C9	D4	01	50	4B	01	02	14	00	14	.Ea.ÉÔ.PK.....
	00010DD0	00	02	00	08	00	AC	AA	54	4E	5C	96	54	DA	5F	0D	00~ªTN\TÚ_..
可用 B空余 NTemp	00010DE0	00	28	12	00	00	0B	00	24	00	00	00	00	00	00	00	20	.(.....
	00010DF0	00	00	00	C1	6A	00	00	70	75	7A	7A	6C	65	38	2E	6A	...Áj..puzzle8.j
00010E00	00010E00	70	67	0A	00	20	00	00	00	00	00	01	00	18	00	00	E2	pg.. ..â
	00010E10	31	2D	1F	C9	D4	01	DB	35	49	61	1F	C9	D4	01	DB	35	1-.ÉÔ.ÛSa.ÉÔ.ÛS
00010E20	00010E20	49	61	1F	C9	D4	01	50	4B	01	02	14	00	14	00	02	00	Ia.ÉÔ.PK.....
	00010E30	08	00	AC	AA	54	4E	D9	C0	F3	3E	4A	0D	00	00	28	12	..ªTNÙÀó>J...(. .
00010E40	00010E40	00	00	0B	00	24	00	00	00	00	00	00	00	20	00	00	00\$.
	00010E50	49	78	00	00	70	75	7A	7A	6C	65	39	2E	6A	70	67	0A	Ix..puzzle9.jpg.
00010E60	00010E60	00	20	00	00	00	00	00	01	00	18	00	00	E2	31	2D	1Fâ1-. .
	00010E70	C9	D4	01	0F	F8	49	61	1F	C9	D4	01	A9	E6	49	61	1F	ÉÔ..øIa.ÉÔ.æIa.
00010E80	00010E80	C9	D4	01	50	4B	01	02	14	00	14	00	02	00	08	00	5C	ÉÔ.PK.....\
	00010E90	9F	54	4E	FA	93	F1	46	9E	00	00	00	A4	00	00	00	0A	TNúF!...ª....
00010EA0	00010EA0	00	24	00	00	00	00	00	00	00	20	00	00	00	BC	85	00	6.....I.
	00010EB0	00	72	65	61	64	6D	65	2E	74	78	74	0A	00	20	00	00	.readme.txt.. ..
00010EC0	00010EC0	00	00	00	01	00	18	00	78	4E	99	A7	13	C9	D4	01	78xNS.ÉÔ.x
	00010ED0	4E	99	A7	13	C9	D4	01	90	D0	DE	60	12	C9	D4	01	50	NS.ÉÔ..P.ÉÔ.P

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

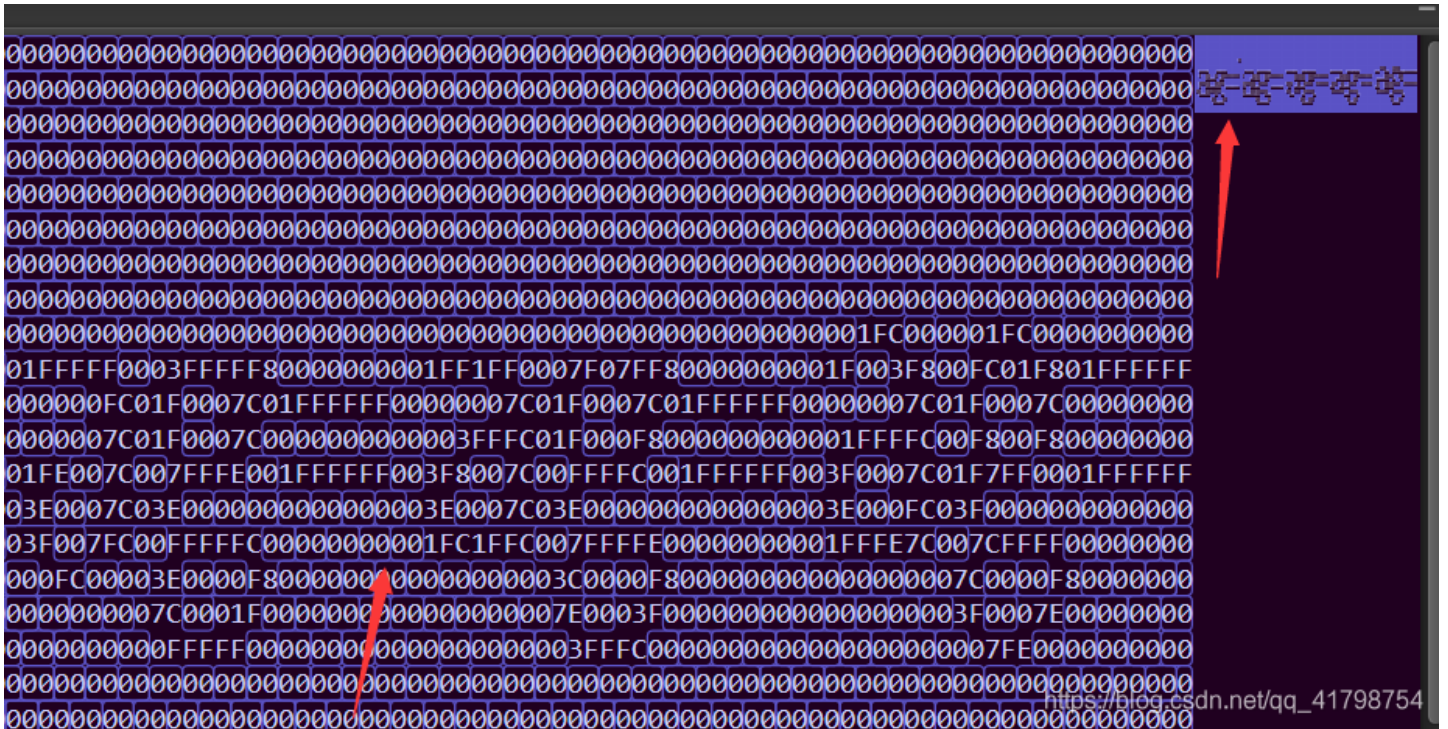
```
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali:~/桌面# binwalk -e 平平无奇的碎纸机.jpg
目录
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         JPEG image data, JFIF standard 1.01
33886       0x845E      Zip archive data, at least v2.0 to extract, compressed size: 3227, uncompressed size: 4648, name: puzzle1.jpg
37154       0x9122      Zip archive data, at least v2.0 to extract, compressed size: 3300, uncompressed size: 4648, name: puzzle10.jpg
40496       0x9E30      Zip archive data, at least v2.0 to extract, compressed size: 3443, uncompressed size: 4648, name: puzzle2.jpg
43980       0xABCC      Zip archive data, at least v2.0 to extract, compressed size: 3511, uncompressed size: 4648, name: puzzle3.jpg
47532       0xB9AC      Zip archive data, at least v2.0 to extract, compressed size: 3373, uncompressed size: 4648, name: puzzle4.jpg
50946       0xC702      Zip archive data, at least v2.0 to extract, compressed size: 3421, uncompressed size: 4648, name: puzzle5.jpg
54408       0xD488      Zip archive data, at least v2.0 to extract, compressed size: 3330, uncompressed size: 4648, name: puzzle6.jpg
57779       0xE1B3      Zip archive data, at least v2.0 to extract, compressed size: 3395, uncompressed size: 4648, name: puzzle7.jpg
61215       0xEF1F      Zip archive data, at least v2.0 to extract, compressed size: 3423, uncompressed size: 4648, name: puzzle8.jpg
64679       0xFCA7      Zip archive data, at least v2.0 to extract, compressed size: 3423, uncompressed size: 4648, name: puzzle8.jpg
```



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。

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

keyes.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
RFVGYHNWSXCDEWSXCVWSXCVTGBNMJUY,WSXZAQWDVFRQWERTYTRFVBTGBNMJUYXSWEFTYHNNI  
WERTYWSXCDEWSXCFETGBNMJUTRFVBGRDXCVBTYUIOJMWSXTGBNMJUYZAQWDVFRGRDXCVBWSXC  
WSXCFEQWERTY(WSX.WSXCDE.,QWERTYYHNMKJTGBNMJUCVGRDQWERTYYHNMKJTGBNMJUYTGBNI  
VBWSXCFEXSWEFTYHNWSXZAQWDVFRWSXIUYHNBVTYUIOJMMNBVCDRTGHUGRDXCVBTYUIOJMWS)
```

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