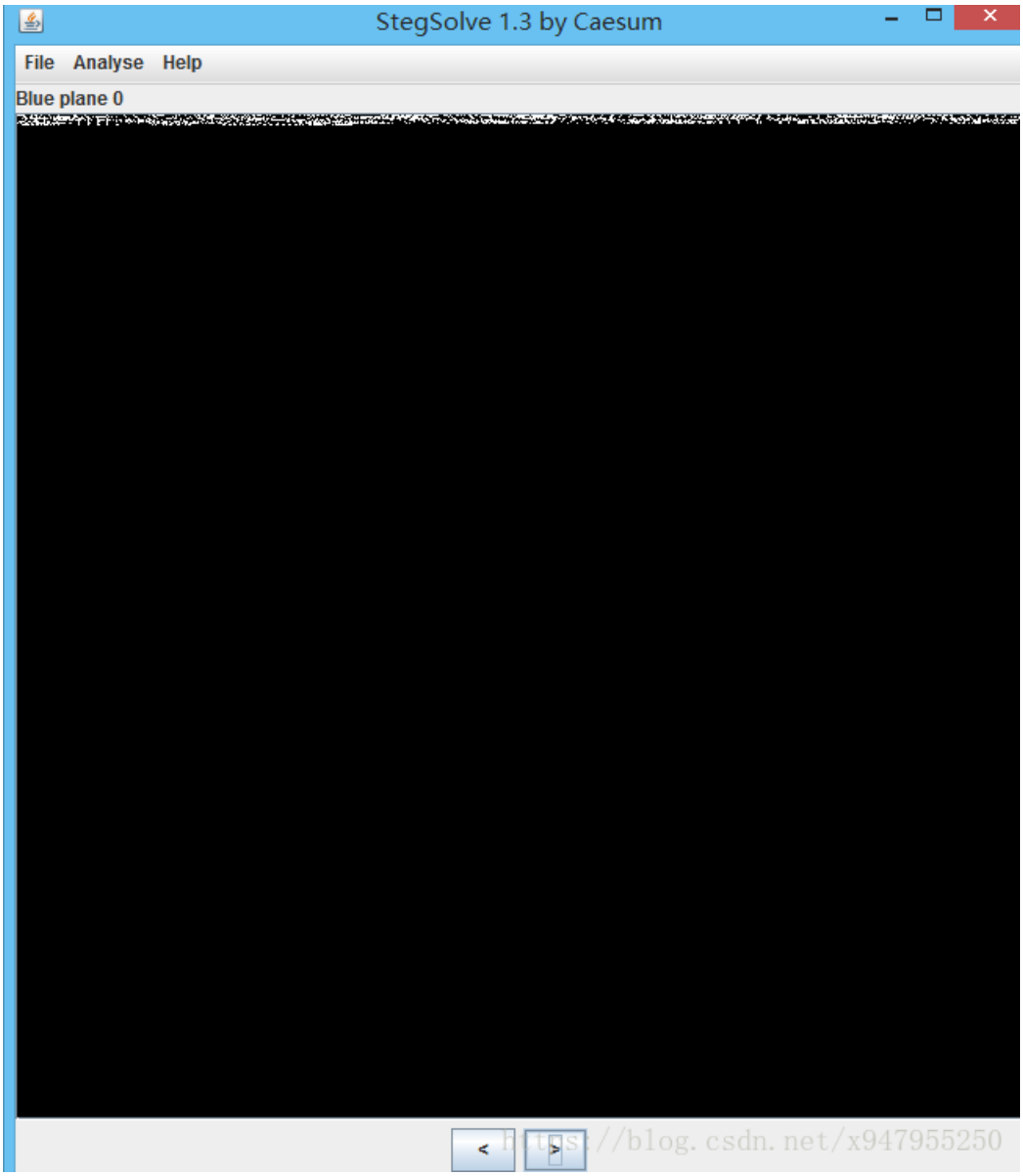
bugkuCTF——猫片(安恒)

原创

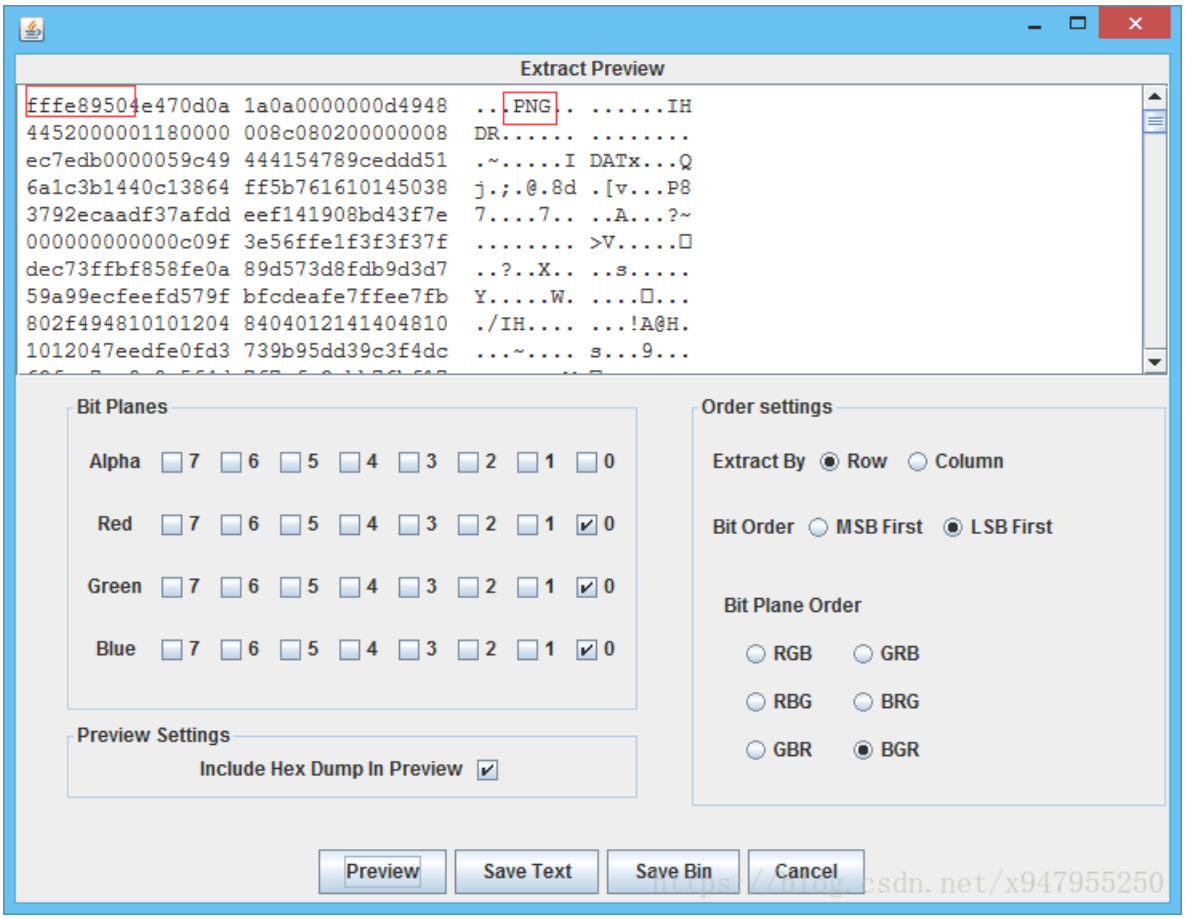
灬彬 于 2018-08-07 16:37:38 发布
分类专栏： ctf 文章标签： bugku ctf 猫片 安恒

bugku昨天才更新的这道题，先将文件下载下来并改后缀png，

通常做图片隐写的题，大概都是先右键查看属性，看下有没有一些特殊的信息，没有就放binwalk看下有没有隐藏什么文件，又或者直接stegsolve分析一波，这题一开始我都试了一遍，无果。但是总不能就这样放弃吧，应该还是漏了点东西。然后折腾了快一个小时，好像有点发现，



在RGB里都发现了这奇怪的一段，然后就试着分析一波，



打算生成一个新的图片，不过要改下文件头

打开winhex将前面的FFFE移除，

1.png

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	FF	FE	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	ÿþ‰PNG IH
00000010	44	52	00	00	01	18	00	00	00	8C	08	02	00	00	00	08	DR ‰
00000020	EC	7E	DB	00	00	05	9C	49	44	41	54	78	9C	ED	DD	51	ì~Û ‰IDATx‰íÝQ
00000030	6A	1C	3B	14	40	C1	38	64	FF	5B	76	16	10	14	50	38	j ; @Á8dÿ[v P8
00000040	37	92	EC	AA	DF	37	AF	DD	EE	F1	41	90	8B	D4	3F	7E	7'ì*ß7¯ÝîñA ‰Ô?~
00000050	00	00	00	00	00	00	C0	9F	3E	56	FF	E1	F3	F3	F3	7F	À‰>Vÿáóóó
00000060	DE	C7	3F	FB	F8	58	FE	0A	89	D5	73	D8	FD	B9	D3	D7	ÞÇ?ûøXþ ‰ÕsØý¹Ó×
00000070	59	A9	9E	CF	EE	FD	57	9F	BF	CD	EA	FE	7F	FE	E7	FB	Y©‰Ïîý‰W‰¿Íêþ þçû
00000080	80	2F	49	48	10	10	12	04	84	04	01	21	41	40	48	10	‰/IH ‰ !A@H
00000090	10	12	04	7E	ED	FE	0F	D3	73	9B	95	DD	39	C3	F4	DC	~íþ Ós‰‰Ý9ÃôÜ
000000A0	63	FA	E7	AE	9C	9A	5F	4D	7F	7E	FA	3A	BB	76	BF	17	cúç®‰‰_M ~ú:»v¿
000000B0	2B	12	04	84	04	01	21	41	40	48	10	10	12	04	84	04	+ ‰ !A@H ‰
000000C0	01	21	41	60	7B	8E	B4	52	ED	27	39	35	37	58	99	9E	!A`{‰´Rí'957X‰‰
000000D0	F3	4C	EF	47	AA	AE	73	6A	7E	B5	7B	FD	5D	D5	FD	58	óLïGª®sj~µ{ý]ÕýX
000000E0	91	20	20	24	08	08	09	02	42	82	80	90	20	20	24	08	‘ $ B‰‰ $
000000F0	08	09	02	D9	1C	E9	75	A7	CE	7F	DB	35	BD	AF	69	75	Ù éu§Î Û5½¯iu
00000100	9D	53	E7	E9	BD	C2	8A	04	01	21	41	40	48	10	10	12	Sçé½Â‰ !A@H
00000110	04	84	04	01	21	41	40	48	10	30	47	8A	9D	7A	5F	D0	‰ !A@H 0G‰ z_Ð
00000120	6D	D7	99	9E	A7	DD	C6	8A	04	01	21	41	40	48	10	10	m×‰‰§ÝÆ‰ !A@H
00000130	12	04	84	04	01	21	41	40	48	10	C8	E6	48	AF	CC	07	‰ !A@H ÈæH¯Ì
00000140	5E	39	CF	AD	DA	2F	34	7D	6E	DE	A9	EF	FD	B6	BF	37	^9Ï-Ú/4}nÞ©ïý¶¿7
00000150	2B	12	04	84	04	01	21	41	40	48	10	10	12	04	84	04	+ ‰ !A@H ‰
00000160	01	21	41	60	7B	8E	54	BD	97	E6	94	53	FB	6D	4E	7D	!A`{‰T½‰æ‰SûmN}
00000170	7E	E5	B6	EB	EF	5E	E7	36	56	24	08	08	09	02	42	82	~å¶ëï^ç6V$ B‰
00000180	80	90	20	20	24	08	08	09	02	42	82	C0	5D	9B	3A	1E	‰ $ B‰À]‰:
00000190	32	3D	27	99	7E	5F	D3	4A	35	47	DA	BD	FE	EB	AC	48	2='‰~_ÓJ5GÚ½þë¬H
000001A0	10	10	12	04	84	04	01	21	41	40	48	10	10	12	04	84	‰ !A@H ‰
000001B0	04	81	EC	5C	BB	EF	B6	FF	A4	DA	47	54	79	E5	3C	BA	ì\»ï¶ÿ¤ÚGTyå<º
000001C0	E9	7D	50	95	DD	E7	63	45	82	80	90	20	20	24	08	08	é}P‰ÝçcE‰‰ $
000001D0	09	02	42	82	80	90	20	20	24	08	8C	0F	13	4E	BD	8F	B‰‰ $ ‰ N½
000001E0	68	D7	EB	FB	7F	6E	9B	D7	9D	DA	D7	34	FD	FC	57	9F	h×ëû n‰× Ú×4ýüW‰
000001F0	B7	22	41	40	48	10	10	12	04	84	04	01	21	41	40	48	·"A@H ‰ !A@H
00000200	10	10	12	04	B2	39	D2	A9	B9	C7	6D	FB	6A	56	4E	ED	²9Ò©¹ÇmûjVNí
00000210	B7	39	B5	0F	EA	D4	5C	6E	65	FA	EF	CD	8A	04	01	21	·9µ êÔ\neúïÍ‰ !
00000220	41	40	48	10	10	12	04	84	04	01	21	41	40	48	10	C8	A@H ‰ !A@H È
00000230	CE	B5	5B	79	7D	5E	B4	72	DB	3E	A2	6A	5F	CD	EB	E7	Îµ[y}^´rÛ>¢j_Íëç
00000240	F2	9D	9A	3B	59	91	20	20	24	08	08	09	02	42	82	80	ò ‰;Y‘ $ B‰‰
00000250	90	20	20	24	08	08	09	02	CB	7F	2C	FF	AA	E7	9E	55	$ Ë ,ÿªç‰U

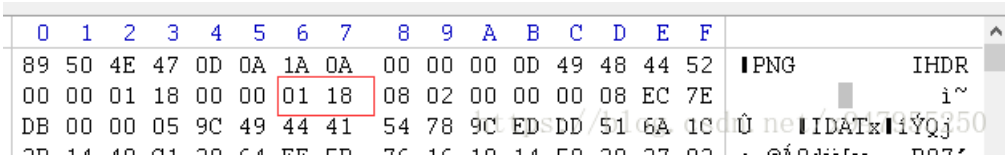
1.png

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	‰PNG IHDR
00000010	00	00	01	18	00	00	00	8C	08	02	00	00	00	08	EC	7E	ì~
00000020	DB	00	00	05	9C	49	44	41	54	78	9C	ED	DD	51	6A	1C	Û IDATxíÝQj
00000030	3B	14	40	C1	38	64	FF	5B	76	16	10	14	50	38	37	92	; @Á8dÿ[v P87’
00000040	EC	AA	DF	37	AF	DD	EE	F1	41	90	8B	D4	3F	7E	00	00	ìªß7¯ÝîñA ‹Ô?~
00000050	00	00	00	00	C0	9F	3E	56	FF	E1	F3	F3	F3	7F	DE	C7	À>Vÿáóóó ÞÇ
00000060	3F	FB	F8	58	FE	0A	89	D5	73	D8	FD	B9	D3	D7	59	A9	?ûøXþ ‰ÕsØý¹Ó×Y©
00000070	9E	CF	EE	FD	57	9F	BF	CD	EA	FE	7F	FE	E7	FB	80	2F	žÏîýW¿Íêþ þçû€/
00000080	49	48	10	10	12	04	84	04	01	21	41	40	48	10	10	12	IH „ !A@H
00000090	04	7E	ED	FE	0F	D3	73	9B	95	DD	39	C3	F4	DC	63	FA	~íþ Ós›•Ý9ÃôÜcú
000000A0	E7	AE	9C	9A	5F	4D	7F	7E	FA	3A	BB	76	BF	17	2B	12	ç®œš_M ~ú:»v¿ +
000000B0	04	84	04	01	21	41	40	48	10	10	12	04	84	04	01	21	„ !A@H „ !
000000C0	41	60	7B	8E	B4	52	ED	27	39	35	37	58	99	9E	F3	4C	A`{Ž´Rí'957X™žóL
000000D0	EF	47	AA	AE	73	6A	7E	B5	7B	FD	5D	D5	FD	58	91	20	ïGª®sj~µ{ý]ÕýX‘
000000E0	20	24	08	08	09	02	42	82	80	90	20	20	24	08	08	09	$ B‚€ $
000000F0	02	D9	1C	E9	75	A7	CE	7F	DB	35	BD	AF	69	75	9D	53	Ù éu§Î Û5½¯iu S
00000100	E7	E9	BD	C2	8A	04	01	21	41	40	48	10	10	12	04	84	çé½Â„ !A@H „
00000110	04	01	21	41	40	48	10	30	47	8A	9D	7A	5F	D0	6D	D7	!A@H 0G„ z_Ðm×
00000120	99	9E	A7	DD	C6	8A	04	01	21	41	40	48	10	10	12	04	™ž§ÝÆ„ !A@H
00000130	84	04	01	21	41	40	48	10	C8	E6	48	AF	CC	07	5E	39	„ !A@H ÈæH¯Ì ^9
00000140	CF	AD	DA	2F	34	7D	6E	DE	A9	EF	FD	B6	BF	37	2B	12	Ï-Ú/4}nÞ©ïý¶¿7+
00000150	04	84	04	01	21	41	40	48	10	10	12	04	84	04	01	21	„ !A@H „ !
00000160	41	60	7B	8E	54	BD	97	E6	94	53	FB	6D	4E	7D	7E	E5	A`{ŽT½—æ”SûmN}~å
00000170	B6	EB	EF	5E	E7	36	56	24	08	08	09	02	42	82	80	90	¶ëï^ç6V$ B‚€
00000180	20	20	24	08	08	09	02	42	82	C0	5D	9B	3A	1E	32	3D	$ B‚À]›: 2=
00000190	27	99	7E	5F	D3	4A	35	47	DA	BD	FE	EB	AC	48	10	10	'™~_ÓJ5GÚ½þë¬H
000001A0	12	04	84	04	01	21	41	40	48	10	10	12	04	84	04	81	„ !A@H „
000001B0	EC	5C	BB	EF	B6	FF	A4	DA	47	54	79	E5	3C	BA	E9	7D	ì\»ï¶ÿ¤ÚGTyå<ºé}
000001C0	50	95	DD	E7	63	45	82	80	90	20	20	24	08	08	09	02	P•Ýçc‚€ $
000001D0	42	82	80	90	20	20	24	08	8C	0F	13	4E	BD	8F	68	D7	B‚€ $ Œ N½ h×
000001E0	EB	FB	7F	6E	9B	D7	9D	DA	D7	34	FD	FC	57	9F	B7	22	ëû n›× Ú×4ýüW·"
000001F0	41	40	48	10	10	12	04	84	04	01	21	41	40	48	10	10	A@H „ !A@H
00000200	12	04	B2	39	D2	A9	B9	C7	6D	FB	6A	56	4E	ED	B7	39	²9Ò©¹ÇmûjVNí·9
00000210	B5	0F	EA	D4	5C	6E	65	FA	EF	CD	8A	04	01	21	41	40	µ êÔ\neúïÍŠ„ !A@
00000220	48	10	10	12	04	84	04	01	21	41	40	48	10	C8	CE	B5	H „ !A@H ÈÎµ
00000230	5B	79	7D	5E	B4	72	DB	3E	A2	6A	5F	CD	EB	E7	F2	9D	[y}^´rÛ>¢j_Íëçò
00000240	9A	3B	59	91	20	20	24	08	08	09	02	42	82	80	90	20	š;Y‘ $ B‚€
00000250	20	24	08	08	09	02	CB	7F	2C	FF	AA	E7	9E	55	6E	7B	$ Ë ,ÿªçžUn{

保存之后出现惊喜，看到半张二维码的图片，接下来就可以考虑改一下图片的高度

这图是280*140的，那就改成280*280的试试，用winhex将高度改为01 18

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	‰PNG IHDR
00	00	01	18	00	00	00	8C	08	02	00	00	00	08	EC	7E	ì~
DB	00	00	05	9C	49	44	41	54	78	9C	ED	DD	51	6A	1C	Û IDATxíÝQj
3B	14	40	C1	38	64	FF	5B	76	16	10	14	50	38	37	92	; @Á8dÿ[v P87’
EC	AA	DF	37	AF	DD	EE	F1	41	90	8B	D4	3F	7E	00	00	ìªß7¯ÝîñA ‹Ô?~
00	00	00	00	C0	9F	3E	56	FF	E1	F3	F3	F3	7F	DE	C7	À>Vÿáóóó ÞÇ



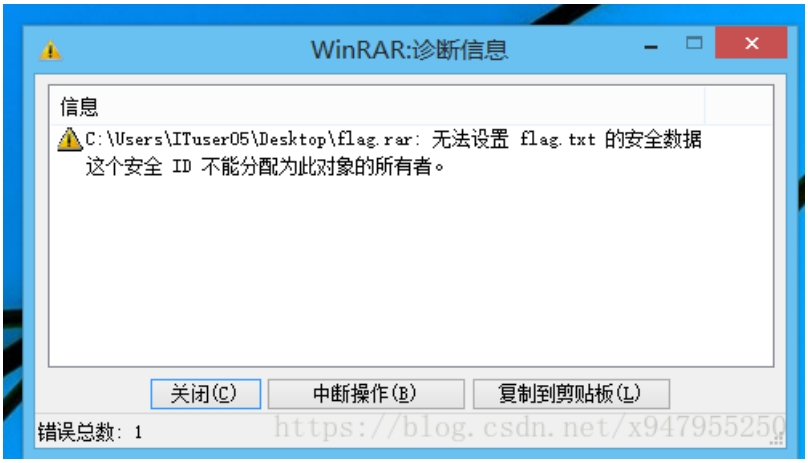
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	‰PNG IHDR
	00	00	01	18	00	00	01	18	08	02	00	00	00	08	EC	7E	ì~
	DB	00	00	05	9C	49	44	41	54	78	9C	ED	DD	51	6A	1C	Û ‰IDATx‰íÝQj

得出一张完整的二维码

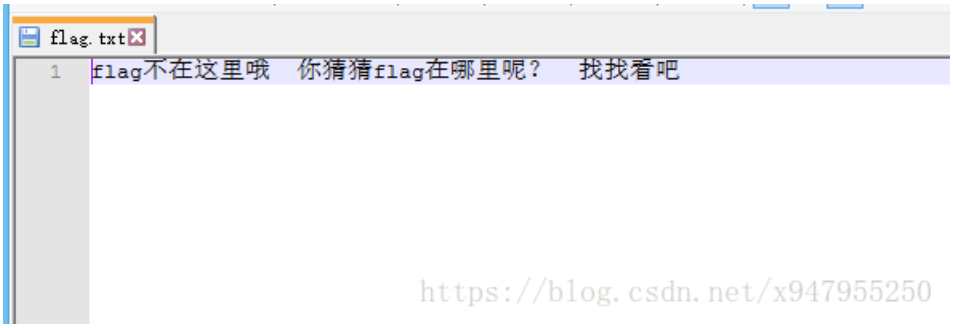
这二维码看着不大对劲，用画图反色(ctrl+shift+i),得出正确的二维码

扫一下，发现有个百度网盘的地址。。。

下载下来是一个压缩包，解压。发现解压出错



更气人的是。。。



真TM。。。无语

后来特意去查了下ctf隐写的各种信息，了解到还有一种ntfs文件流的东西

反正看起来各种高大上，我呢。。肯定就看不懂。。。

只能屁颠屁颠地去找了下某大佬，在被他一顿无情嘲讽之后，他告诉我这是今年安恒杯的赛题，好像还有writeup。。

。。。。。。。。

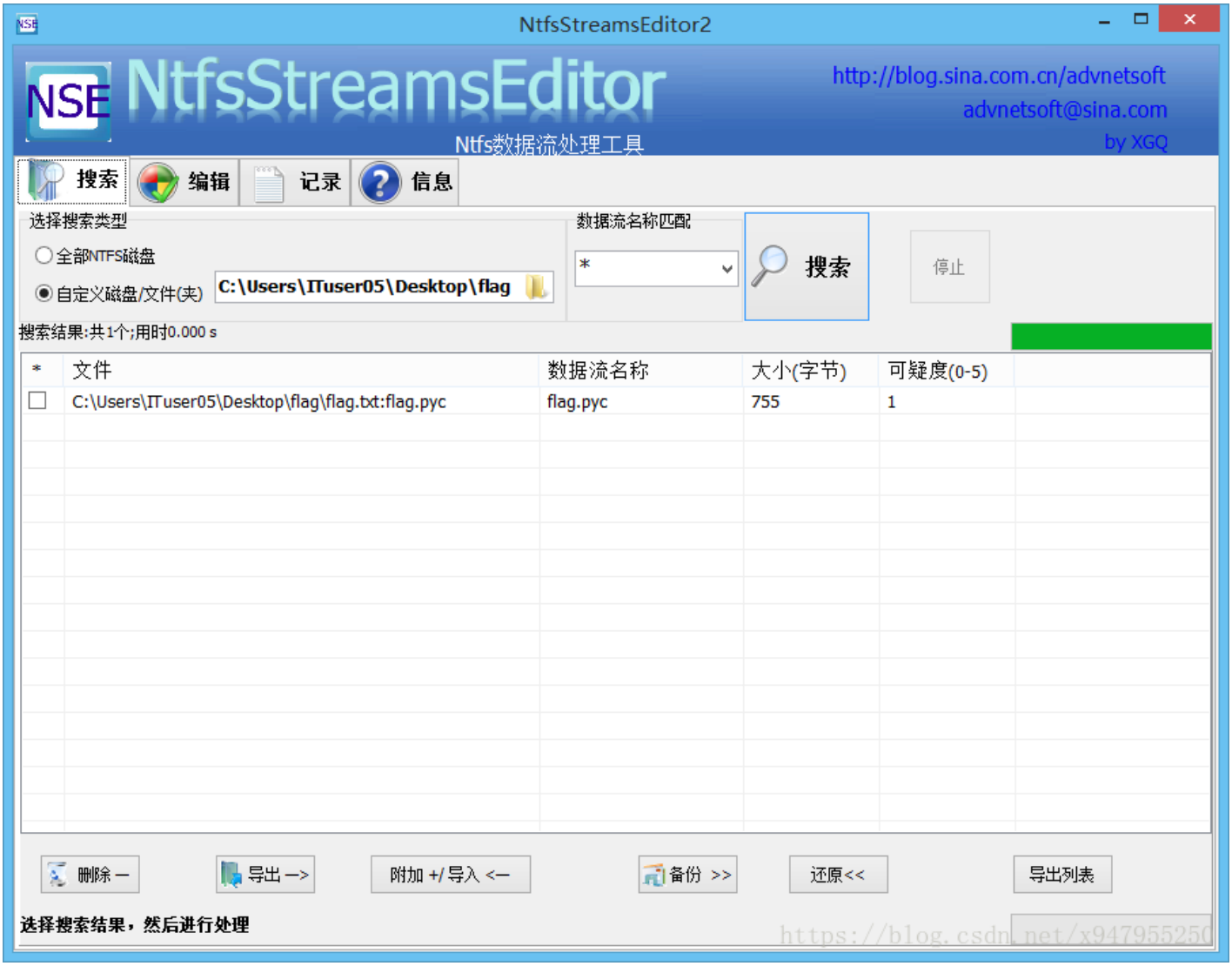
。。。。。。。。

行吧。。百度搜了下，发现另一位老铁写的writeup

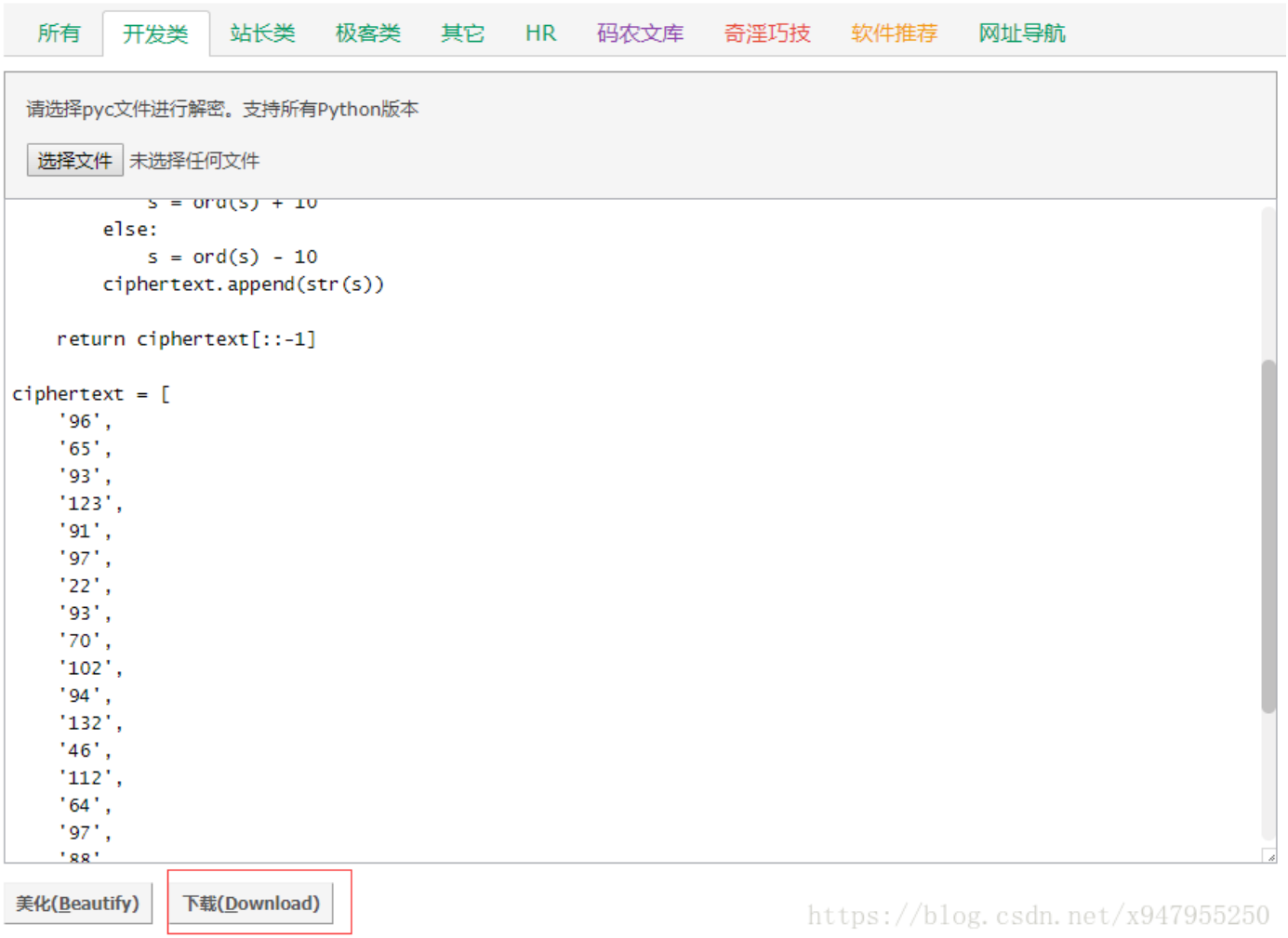
https://www.jianshu.com/p/abc44c54857a

接下来。。就按照大佬的做法。。用NtfsStreamsEditor查看数据流，然后导出，

PS：flag.rar这个压缩文件一定要用winrar来解压才能找得到数据流。。。



.pyc文件，直接丢到这。。https://tool.lu/pyc/


所有
开发类
站长类
极客类
其它
HR
码农文库
奇淫巧技
软件推荐
网址导航
请选择pyc文件进行解密。支持所有Python版本
选择文件
未选择任何文件
s = ord(s) + 10
else:
s = ord(s) - 10
ciphertext.append(str(s))
return ciphertext[::-1]
ciphertext = [
'96',
'65',
'93',
'123',
'91',
'97',
'22',
'93',
'70',
'102',
'94',
'132',
'46',
'112',
'64',
'97',
'88'
美化(Beautify)
下载(Download)
https://blog.csdn.net/x947955250

下载之后写解密的脚本。。。

```
def decode():
    ciphertext = [
    '96',
    '65',
    '93',
    '123',
    '91',
    '97',
    '22',
    '93',
    '70',
    '102',
    '94',
    '132',
    '46',
    '112',
    '64',
    '97',
    '88',
    '80',
    '82',
    '137',
    '90',
    '109',
    '99',
    '112']
    ciphertext.reverse()
    flag = ''
    for i in range(len(ciphertext)):
        if i % 2 == 0:
            s = int(ciphertext[i]) - 10
        else:
            s = int(ciphertext[i]) + 10
        s=chr(i^s)
        flag += s
    return flag

def main():
    flag = decode()
    print(flag)

if __name__ == '__main__':
    main()
```

```
C:\Users\ITuser05\Desktop>python untitled.py
flag{Y@e_Cl3veR_C1Ever!}
```


最后得出 flag{Y@e_Cl3veR_C1Ever!}