

# BUUCTF 喵喵喵

原创

[Charles Andrew](#) 于 2021-11-24 21:13:40 发布 56 收藏

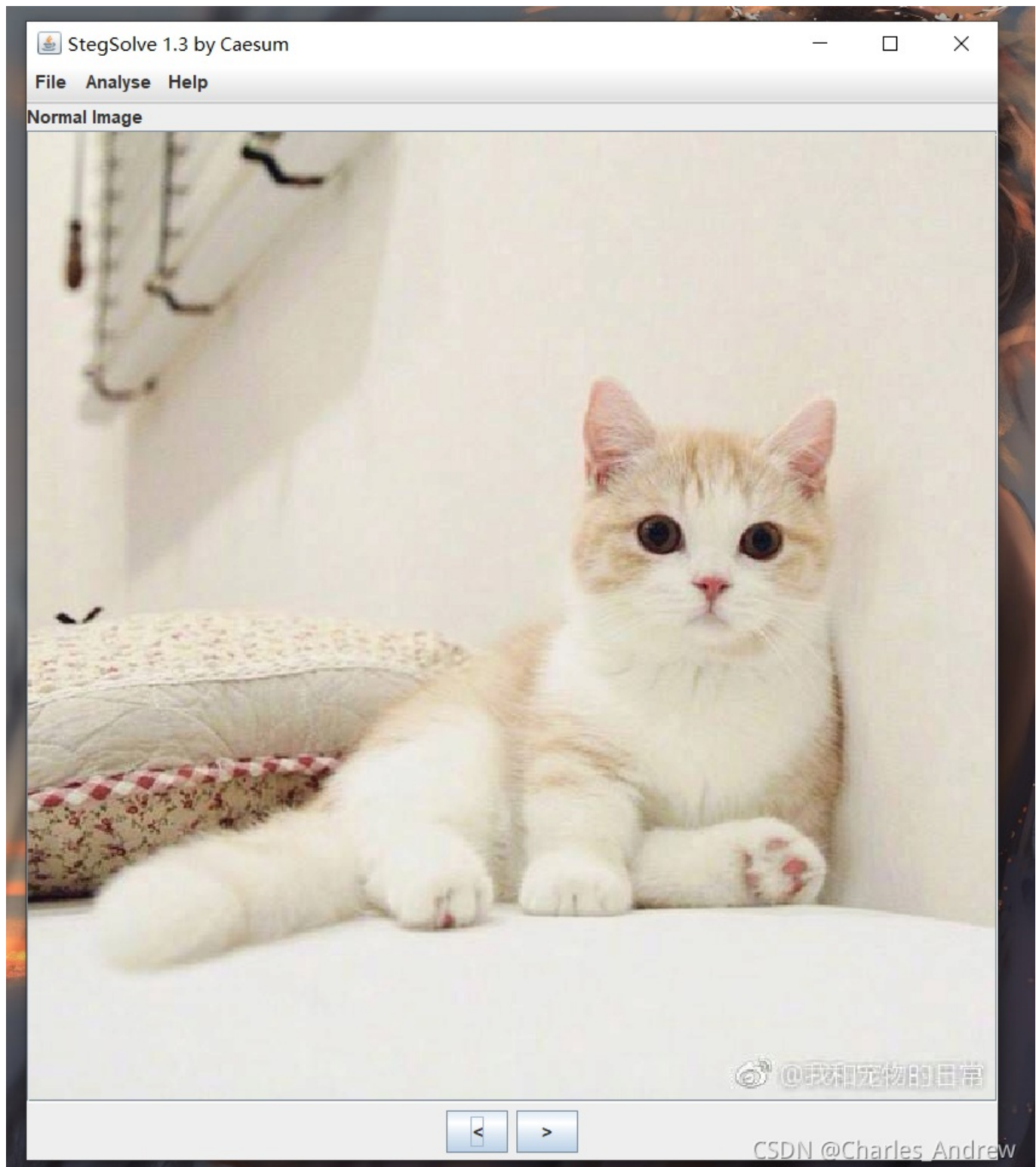
文章标签: [unctf](#) [安全](#) [web安全](#)

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。

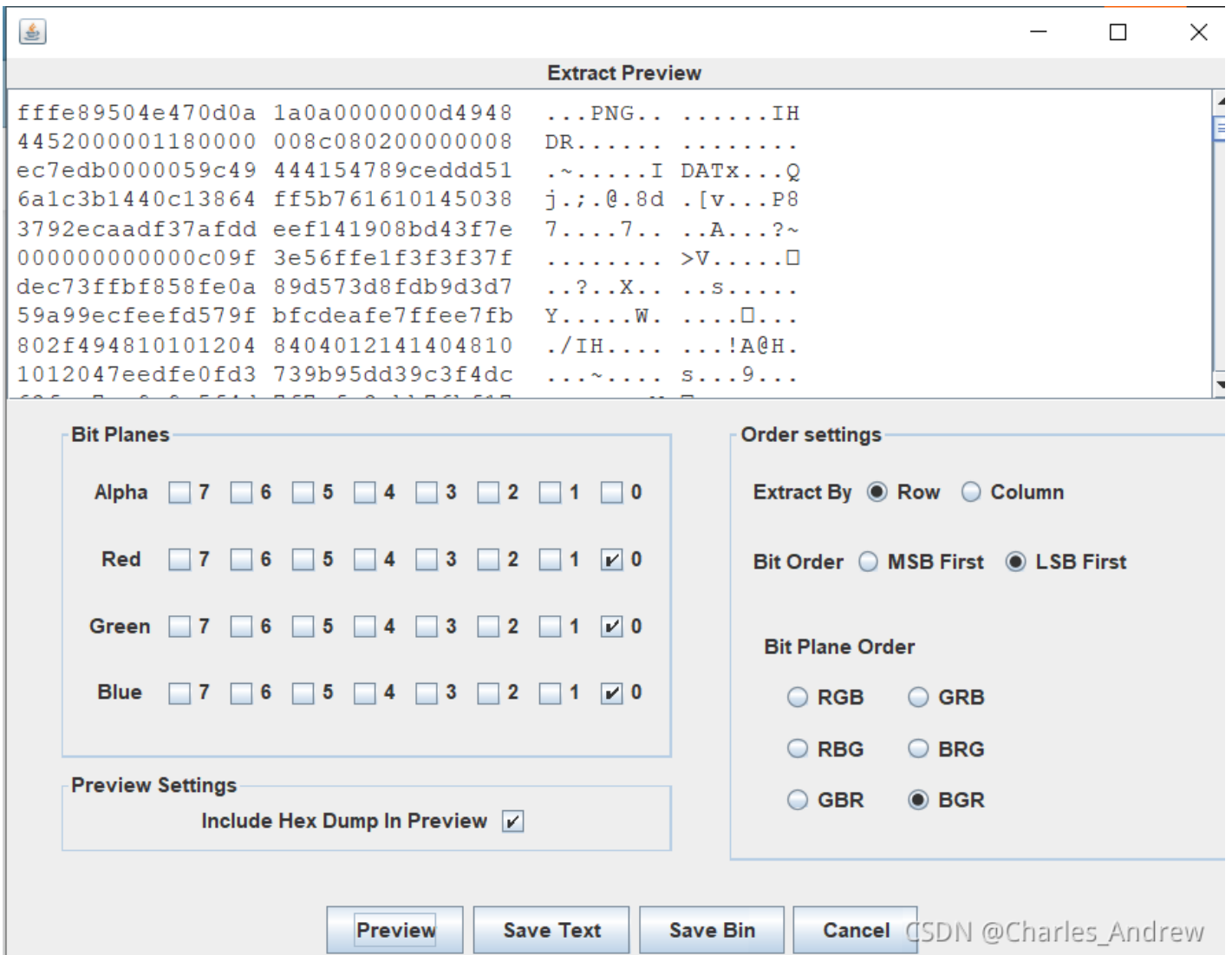
本文链接: [https://blog.csdn.net/Charles\\_Andrew/article/details/121523654](https://blog.csdn.net/Charles_Andrew/article/details/121523654)

版权

文件打开来是张图片

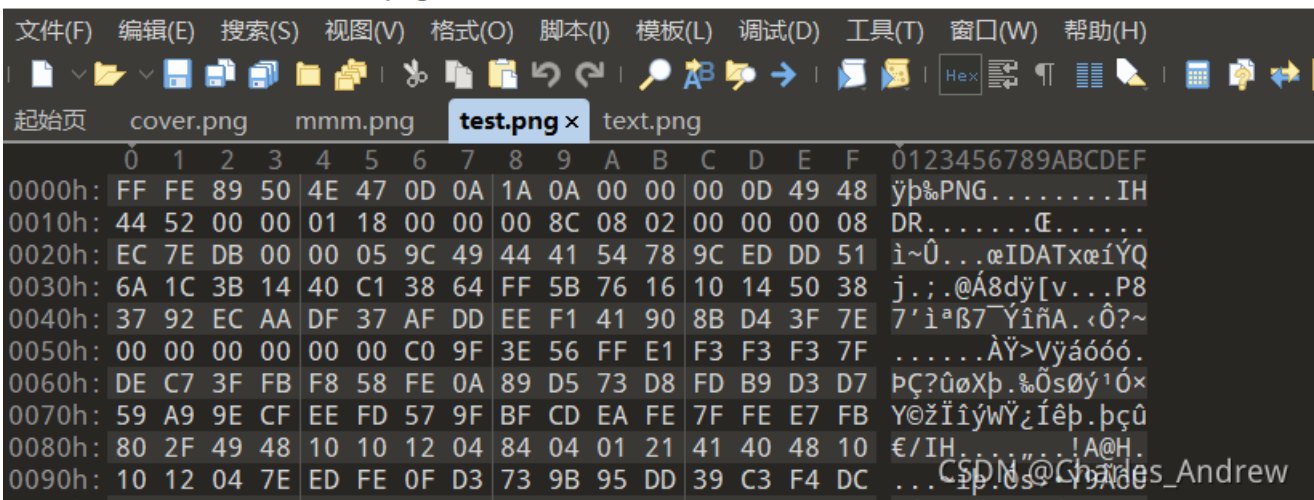


题目也写了扫一扫, 那就直接用stegsolve打开来



发现文件0通道有异常，是LSB隐写，保存为.png文件，并用010打开

010 Editor - F:\解压\临时\test.png




发现文件头有问题，将FF FF删去保存



发现二维码只有一半，使用010更改高度

起始页	cover.png	mmm.png	test.png x	text.png
0000h:	89 50 4E 47	0D 0A 1A 0A	00 00 00 0D	49 48 44 52
0010h:	00 00 01 18	00 00 01 BC	08 02 00 00	08 EC 7E
0020h:	DB 00 00 05	9C 49 44 41	54 78 9C ED	DD 51 6A 1C
0030h:	3B 14 40 C1	38 64 FF 5B	76 16 10 14	50 38 37 92
0040h:	EC AA DF 37	AF DD EE F1	41 90 8B D4	3F 7E 00 00
0050h:	00 00 00 00	C0 9F 3E 56	FF E1 F3 F3	F3 7F DE C7
0060h:	3F FB F8 58	FE 0A 89 D5	73 D8 FD B9	D3 D7 59 A9
0070h:	9E CF EE FD	57 9F BF CD	EA FE 7F FE	E7 FB 80 2F
0080h:	49 48 10 10	12 04 84 04	01 21 41 40	48 10 10 12
0090h:	04 7E ED FE	0F D3 73 9B	95 DD 39 C3	F4 DC 63 FA
00A0h:	E7 AE 9C 9A	5F 4D 7F 7E	FA 3A BB 76	BF 17 2B 12
00B0h:	04 84 04 01	21 41 40 48	10 10 12 04	84 04 01 21
00C0h:	41 60 7B 8E	B4 52 ED 27	39 35 37 58	99 9E F3 4C
00D0h:	EF 47 AA AE	73 6A 7E B5	7B FD 5D D5	FD 58 91 20
00E0h:	20 24 08 08	09 02 42 82	80 90 20 20	24 08 08 09
00F0h:	02 D9 1C E9	75 A7 CE 7F	DB 35 BD AF	69 75 9D 53
0100h:	E7 E9 BD C2	8A 04 01 21	41 40 48 10	10 12 04 84
0110h:	04 01 21 41	40 48 10 30	47 8A 9D 7A	5F D0 6D D7
0120h:	99 9E A7 DD	C6 8A 04 01	21 41 40 48	10 10 12 04
0130h:	84 04 01 21	41 40 48 10	C8 E6 48 AF	CC 07 5E 39
0140h:	CF AD DA 2F	34 7D 6E DE	A9 EF FD B6	BF 37 2B 12
0150h:	04 84 04 01	21 41 40 48	10 10 12 04	84 04 01 21
0160h:	41 60 7B 8E	54 BD 97 E6	94 53 FB 6D	4E 7D 7E E5
0170h:	B6 EB EF 5E	E7 36 56 24	08 08 09 02	42 82 80 90
0180h:	20 20 24 08	08 09 02 42	82 C0 5D 9B	3A 1E 32 3D
0190h:	27 99 7E 5F	D3 4A 35 47	DA BD FE EB	AC 48 10 10
01A0h:	12 04 84 04	01 21 41 40	48 10 10 12	04 84 04 81
01B0h:	EC 5C BB EF	B6 FF A4 DA	47 54 79 E5	3C BA E9 7D
01C0h:	50 65 DD 57	63 45 82 80	00 20 30 24	08 08 00 00



使用 QR扫码，即可发现网址：<https://pan.baidu.com/s/1pLT2J4f>



纠错等级	掩码
H(30%)	Auto
版本	尺寸
Auto	4
<input type="checkbox"/> Auto	

已解码数据 1:

位置:(2.0,4.0)-(332.0,4.0)-(2.0,334.0)-(332.0,334.0)  
颜色反色, 正像  
版本: 4  
纠错等级:H, 掩码:1  
内容:  
<https://pan.baidu.com/s/1pLT2J4f>

CSDN @Charles\_Andrew

.txt打开后显示没有，结果.....

flag.txt - 记事本

flag不在此处哦 你猜猜flag在哪里呢？ 找找看吧

CSDN @Charles\_Andrew

最后上网查找了一下，结果发现可能是NTFS流，放到NtfsStreamsEditor2中发现了



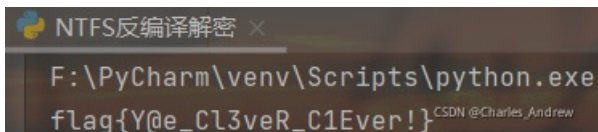
请选择pyc文件进行解密。支持所有Python版本

选择文件 未选择文件

```
4
5 def encode():
6     flag = '*****'
7     ciphertext = []
8     for i in range(len(flag)):
9         s = chr(i ^ ord(flag[i]))
10        if i % 2 == 0:
11            s = ord(s) + 10
12        else:
13            s = ord(s) - 10
14        ciphertext.append(str(s))
15
16    return ciphertext[::-1]
17
18 ciphertext = [
19    '96',
20    '65',
21    '93',
22    '123',
23    '91',
24    '97',
25    '22',
26    '100'
```

CSDN @Charles\_Andrew

有反编译解密可以得到



```
NTFS反编译解密 ×
F:\PyCharm\venv\Scripts\python.exe
flag{Y@e_Cl3veR_C1Ever!}
```

flag{Y@e\_Cl3veR\_C1Ever!}