

bugku猫片

转载

[a111b11100](#) 于 2019-08-26 11:04:00 发布 151 收藏

原文链接: <http://www.cnblogs.com/lzxxxx/p/11411333.html>

版权

这个猫片思路清奇，真的让我长知识了。

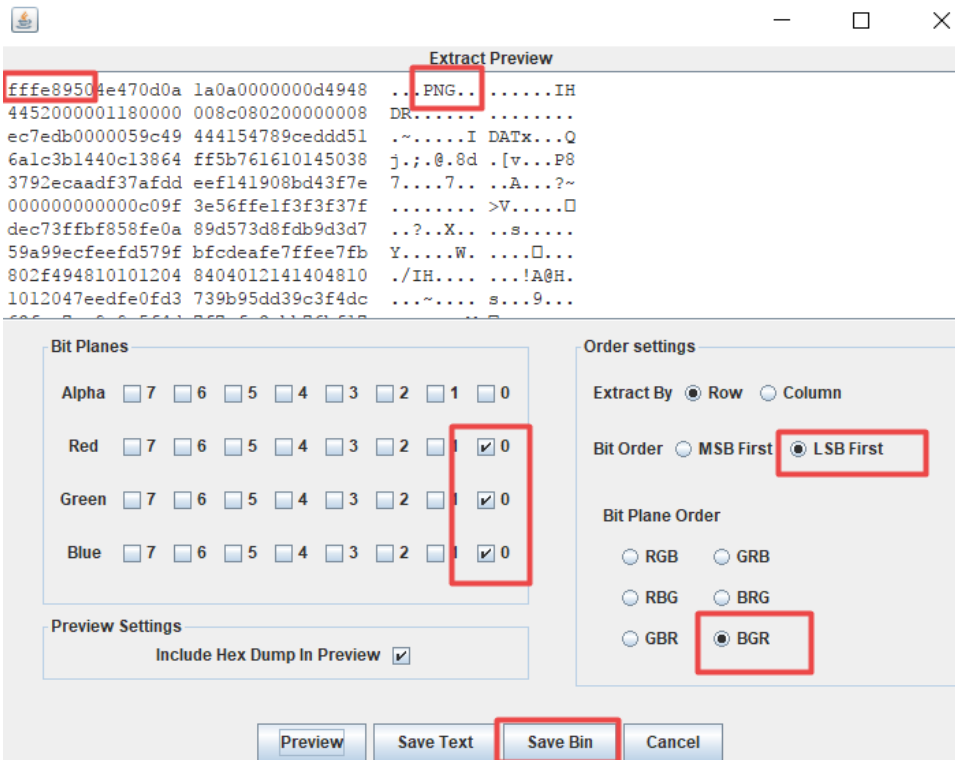
开局一只猫，挺可爱的。



拿到图片，老套路来一波，首先 winhex打开是正常png图片，binwalk，stegslope都没有任何收获。折腾了好久没有任何思路放弃了，找到了网上的writeup，原来是一道比赛题，而且原题是有提示的：

hint: LSB BGR NTFS

打开stegslope，将三原色改为零，勾选lsb，bgr如下图所示，发现是个png图片，将这个图片保存，

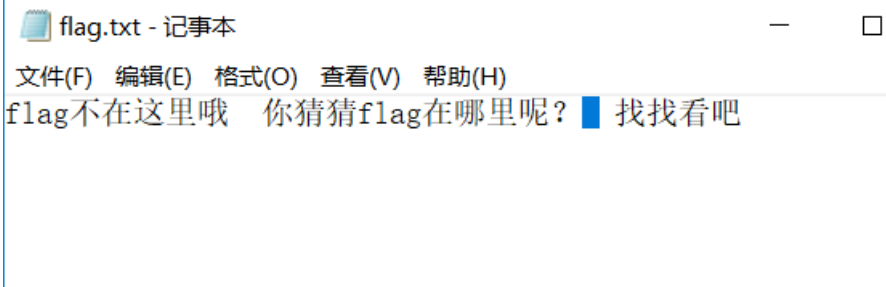


发现打不开，使用winhex发现头文件错的，png图片头文件是89504e，修改头文件。

成功将图打开了，但是只有半个二维码，打开属性查看高度是280*140，winhex修改高度为280*280，完整的二维码出现了。

使用research扫一下这个二维码，是一个百度网盘的地址，下载下来文件解压（一定要用WinRAR来解压）

打开，发现不是flag



再次瞪眼，没办法求助于教程，是NTFS流隐写，用ntfstreamseditor查看文件里的数据流是个python编译后的文件 将文件导出在线工具反编译得到源码，是个加密算法，按这个算法写一个解密的脚本跑一下。

```
File Edit View Navigate Code Refactor Run Tools VCS Window Help
Scratches > scratch_2.py
scratch_2.py x
1 def jiemi():
2     lz = ['96', '65', '93', '123', '91', '97', '22', '93', '70', '102', '94', '132', '46', '112', '64', '97', '88', '80', '82', '15
3     flag=''
4     lz.reverse()
5     for i in range(len(lz)):
6         if i%2==0:
7             s=int(lz[i])-10
8         else:
9             s=int(lz[i])+10
10        s=chr(i`s)
11        flag+=s
12        print(flag)
13    jiemi()
14
15
Run: scratch_2 x
flag{Y@e_C13veR_C
flag{Y@e_C13veR_C1
flag{Y@e_C13veR_C1E
flag{Y@e_C13veR_C1Ev
flag{Y@e_C13veR_C1Eve
flag{Y@e_C13veR_C1Ever
flag{Y@e_C13veR_C1Ever!
flag{Y@e_C13veR_C1Ever!!
Process finished with exit code 0
68% 0.1K/s 0.2K/s
IDE and Plugin Updates
PyCharm is ready to update.
```

成功得到得到flag（这题真的让我获益匪浅）

转载于:<https://www.cnblogs.com/lzlzzzzz/p/11411333.html>



[创作打卡挑战赛](#)
[赢取流量/现金/CSDN周边激励大奖](#)