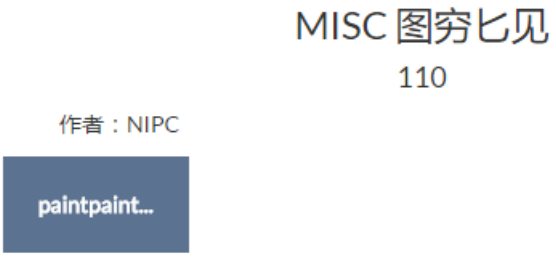
Bugku - Misc图穷匕见 - Writeup

转载

Bugku - Misc图穷匕见 - Writeup

> 原文链接：http://www.cnblogs.com/WangAoBo/p/6950547.html

题目



给了一个jpg图片，下载图片

分析

图片下载后，先右键查看属性，有如下发现：

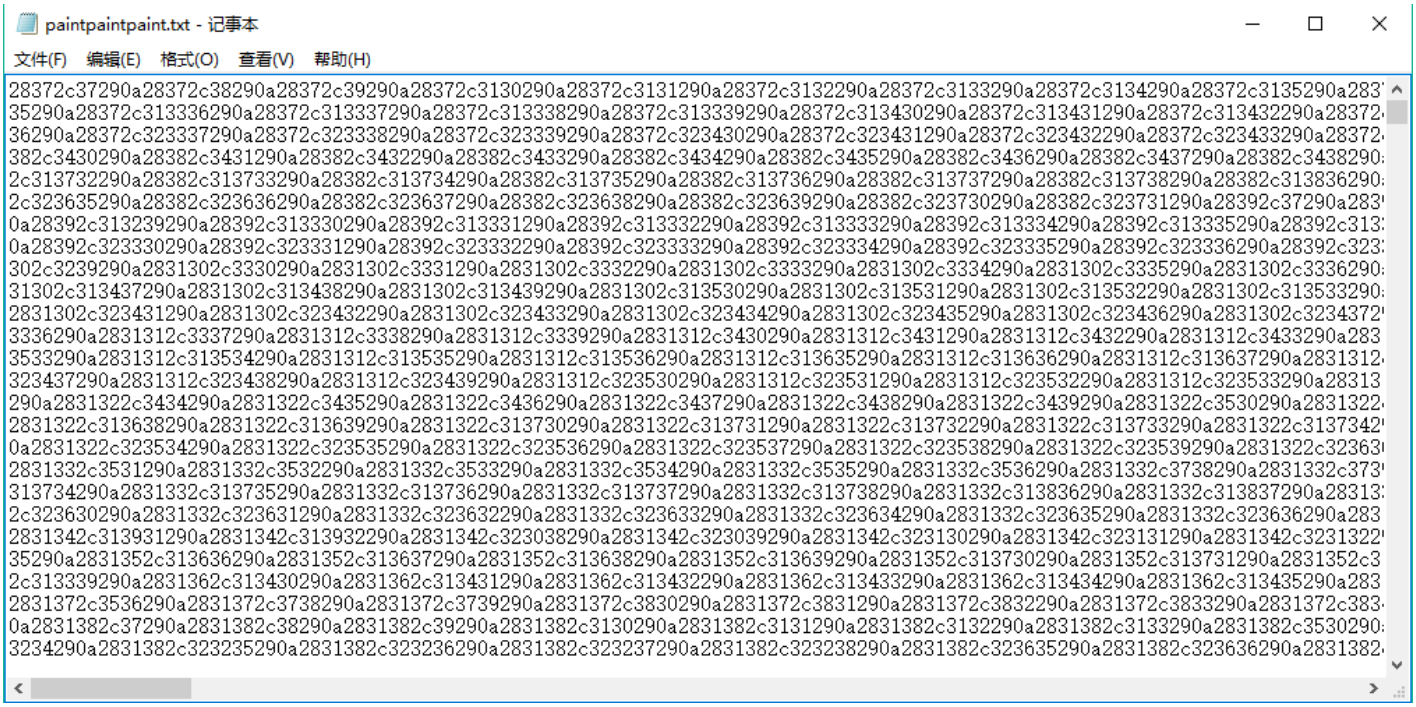
图片的标题**图穷flag见**以及题目**图穷匕见**都暗示该图片在文件末尾隐藏了信息，主题**会画图吗**的作用下文再分析

步骤

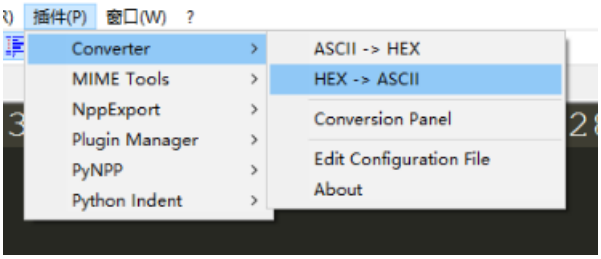
用16进制编辑器（如010editor）打开图片，找到jpg的文件尾**FF D9**，发现其后还有大量的数据

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F    0123456789ABCDEF
5290h: 21 69 02 93 B9 42 11 54 36 49 08 44 07 E6 F6 50   !i."¹B.T6I.D.æöP
52A0h: EE 5E A8 42 95 60 3C 95 0D 8A 10 80 6E E8 76 E8   î^¨B•`<•.Š.€nèvè
52B0h: 42 7E 03 98 52 EE 68 42 80 3F 2A 63 72 84 20 A6   B~.˜RîhB€?*cr„ ¦
52C0h: EC 87 21 0B 47 E9 1D D5 72 42 13 F4 09 0E 48 42   ì‡!.Gé.ÕrB.ô..HB
52D0h: 06 A2 A7 2F 54 21 11 68 42 15 02 10 85 00 84 21   .¢§/T!.hB.....„!
52E0h: 00 84 21 50 24 84 28 1A 10 84 02 10 85 40 84 21   .„!P$„(..„...…@„!
52F0h: 00 84 21 07 FF D9 32 38 33 37 32 63 33 37 32 39   .„!.ÿÙ28372c3729
5300h: 30 61 32 38 33 37 32 63 33 38 32 39 30 61 32 38   0a28372c38290a28
5310h: 33 37 32 63 33 39 32 39 30 61 32 38 33 37 32 63   372c39290a28372c
5320h: 33 31 33 30 32 39 30 61 32 38 33 37 32 63 33 31   3130290a28372c31
5330h: 33 31 32 39 30 61 32 38 33 37 32 63 33 31 33 32   31290a28372c3132
5340h: 32 39 30 61 32 38 33 37 32 63 33 31 33 33 32 39   290a28372c313329
5350h: 30 61 32 38 33 37 32 63 33 31 33 34 32 39 30 61   0a28372c3134290a
5360h: 32 38 33 37 32 63 33 31 33 35 32 39 30 61 32 38   28372c3135290a28
5370h: 33 37 32 63 33 31 33 36 32 39 30 61 32 38 33 37   372c3136290a2837
```

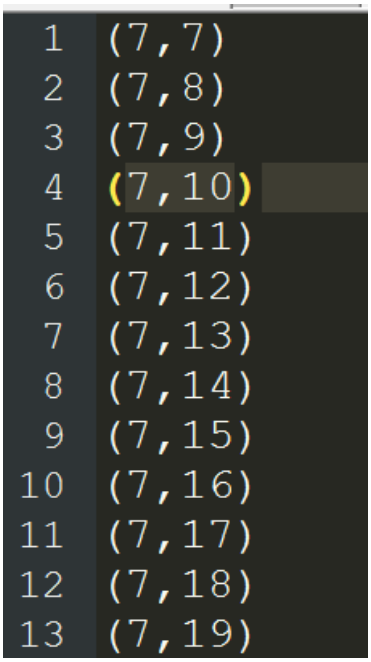
将之后的数据保存到txt中



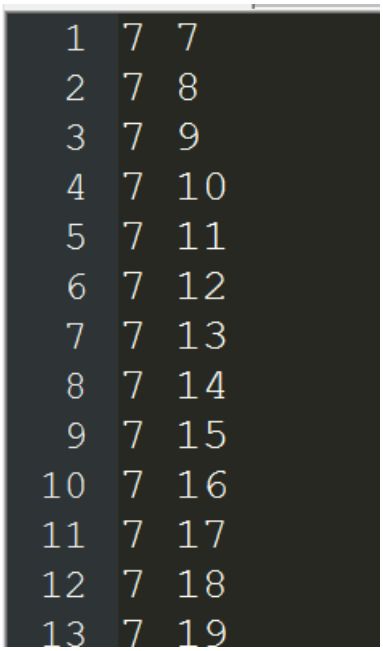
乍一看无从下手，其实只要尝试将数据按**16进制->ASCII**方式解码，思路就很明显了，下图中使用的是notepad++中的插件Converter进行解码



解码结果如下，很明显是坐标的形式



这时候再结合**会画图吗**的提示，将这些坐标做成一张图即可，用**gnuplot**这个工具比较方便，因此将坐标转为gnuplot能识别的格式 **坐标1 坐标2**



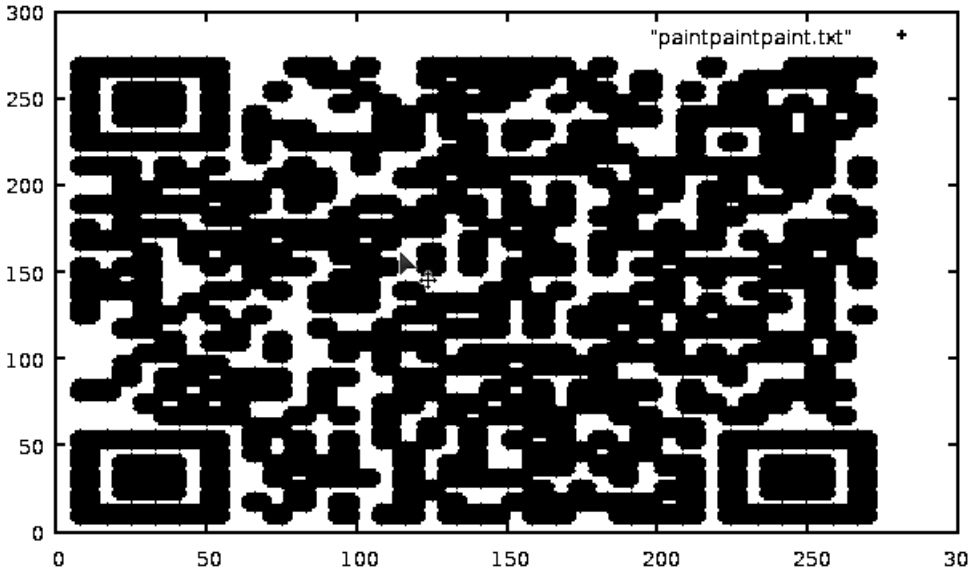
在Linux中使用

> gunplot
>
> plot "文件名"（注意“）

如下图

得到一个二维码

对该二维码在做灰度等的处理后，扫描可得flag



flag为**flag{40fc0a979f759c8892f4dc045e28b820}**

当然，作为程序员为什么不自己写代码处理呢？附脚本：

https://gist.github.com/bash-c/6c178705bb4cca51d43a048feb62f395#file-coordinate2img-py

效果也很不错：

转载于:https://www.cnblogs.com/WangAoBo/p/6950547.html