




记一道MISC图片题（拖延癌晚期）

原创

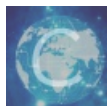
薛定谔的呱  于 2019-02-23 20:17:54 发布  1750  收藏 7

分类专栏: [ctf](#) 文章标签: [ctf misc](#)

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_36360189/article/details/87896569

版权



[ctf 专栏收录该内容](#)

2 篇文章 0 订阅

订阅专栏

title: 记一道misc图片题

date: 2017-10-26 15:17:12

tags: MISC

记一道MISC图片题（拖延癌晚期）

几个月前实验班考核的一个杂项

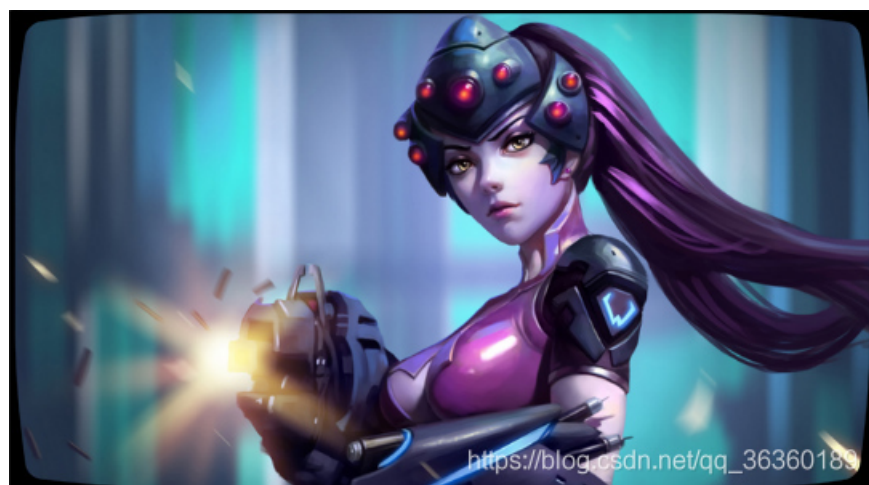
这个题是今年实验班考核的时候一个学长出的300分的杂项, 然后当时没做出来...回来之后在学长的提示下做出来了otz...

就是一道脑洞题...不过学到了一些新的工具使用。所以总结一下。

最近清理window虚拟机找到了一些做的时候的截图什么的想起来了这事。觉得有的东西还是觉得记录一下。-(虽然本拖延癌晚期患者已经拖了几个月...)-

原本好像是zip伪加密方式(记不太清楚了), 做出来可以得到一张jpg图。

这是一张守望屁股里黑百合的jpg图。



用16进制分析工具分析一下。

ffd8文件头没问题，搜索一下文件尾ffd9。

```
70h: 98 BF B9 27 FD FD 1F E1 46 83 F7 83 30 F7 49 3F : 桶? 器余?桶?
80h: EF E8 FF 00 0A 5A 0C 9E 5B 88 DE D2 DE D6 38 E4 : 罐...Z...湖探建??
90h: 4F 26 E2 59 0B BC A1 61 DE 10 60 OD A3 18 D9 EA : 0新 肌倍...?司
a0h: 7A F6 C7 29 2D 6E 37 63 FF D9 32 38 33 37 32 63 : r(空)-n7c...?28372c
b0h: 33 37 32 39 30 61 32 38 33 37 32 63 33 38 32 39 : 37290a28372c3829
c0h: 30 61 32 38 33 37 32 63 33 39 32 39 30 61 32 38 : 0a28372c39290a28
d0h: 33 37 32 63 33 31 33 30 32 39 30 61 32 38 33 37 : 372c3130290a2837
e0h: 32 63 33 31 33 31 32 39 30 61 32 38 33 37 32 63 : 2c3131290a28372c
f0h: 33 31 33 32 32 39 30 61 32 38 33 37 32 63 33 31 : 3132290a28372c31
00h: 33 33 32 39 30 61 32 38 33 37 32 63 33 31 33 34 : 33290a28372c3134
10h: 32 39 30 61 32 38 33 37 32 63 33 31 33 35 32 39 : 290a28372c313529
20h: 30 61 32 38 33 37 32 63 33 31 33 36 32 39 30 61 : 0a28372c3136290a
30h: 32 38 33 37 32 63 33 31 33 37 32 39 30 61 32 38 : 28372c3137290a28
40h: 33 37 32 63 33 31 33 38 32 39 30 61 32 38 33 37 : 372c3138290a2837
50h: 32 63 33 31 33 39 32 39 30 61 32 38 33 37 32 63 : 2c3139290a28372c
60h: 33 32 33 30 32 39 30 61 32 38 33 37 32 63 33 32 : 3230290a28372c32
70h: 33 31 32 39 30 61 32 38 33 37 32 63 33 32 33 32 : 31290a28372c3232
80h: 32 39 30 61 32 38 33 37 32 63 33 32 33 33 32 39 : 290a28372c323329
90h: 30 61 32 38 33 37 32 63 33 32 33 34 32 39 30 61 : 0a28372c3234290a
a0h: 32 38 33 37 32 63 33 32 33 32 33 35 32 39 30 61 : 28372c3235290a28
b0h: 33 37 32 63 33 32 33 36 32 39 30 61 32 38 33 37 : 372c3236290a2837
c0h: 32 63 33 32 33 37 32 39 30 61 32 38 33 37 32 63 : 2c3237290a28372c
d0h: 33 32 33 38 32 39 30 61 32 38 33 37 32 63 33 32 : 3238290a28372c32
e0h: 33 39 32 39 30 61 32 38 33 37 32 63 33 33 33 30 : 39290a28372c3330
f0h: 32 39 30 61 32 38 33 37 32 63 33 33 33 31 32 39 : 290a28372c333129
00h: 30 61 32 38 33 37 32 63 33 33 33 32 32 39 30 61 : 0a28372c3332290a
10h: 32 38 33 37 32 63 33 33 33 33 33 32 39 30 61 32 : 28372c3333290a28
20h: 33 37 32 63 33 33 33 34 32 39 30 61 32 38 33 37 : 372c3334290a2837
30h: 32 63 33 33 33 35 32 39 30 61 32 38 33 37 32 63 : 2c3335290a28372c
40h: 33 33 33 36 32 39 30 61 32 38 33 37 32 63 33 33 : 3336290a28372c33
50h: 33 37 32 39 30 61 32 38 33 37 32 63 33 33 33 38 : 37290a28372c3338
60h: 32 39 30 61 32 38 33 37 32 63 33 33 33 39 32 39 : 290a28372c333929
70h: 30 61 32 38 33 37 32 63 33 34 33 30 32 39 30 61 : 0a28372c3430290a
80h: 32 38 33 37 32 63 33 34 33 31 32 39 30 61 32 38 : 28372c3431290a28
90h: 33 37 32 63 33 34 33 32 32 39 30 61 32 38 33 37 : 372c3432290a2837
a0h: 32 63 33 34 33 33 32 39 30 61 32 38 33 37 32 63 : 2c3433290a28372c
b0h: 33 34 33 34 32 39 30 61 32 38 33 37 32 63 33 34 : 3434290a28372c34
c0h: 33 35 32 39 30 61 32 38 33 37 32 63 33 34 33 36 : 35290a28372c3436
d0h: 32 39 30 61 32 38 33 37 32 63 33 34 33 37 32 39 : 290a28372c343729
e0h: 30 61 32 38 33 37 32 63 33 34 33 38 32 39 30 61 : 0a28372c3438290a
f0h: 32 38 33 37 32 63 33 34 33 39 32 39 30 61 32 38 : 28372c3439290a28
100h: 33 37 32 63 33 35 33 30 32 39 30 61 32 38 33 37 : 372c3530290a2837
```

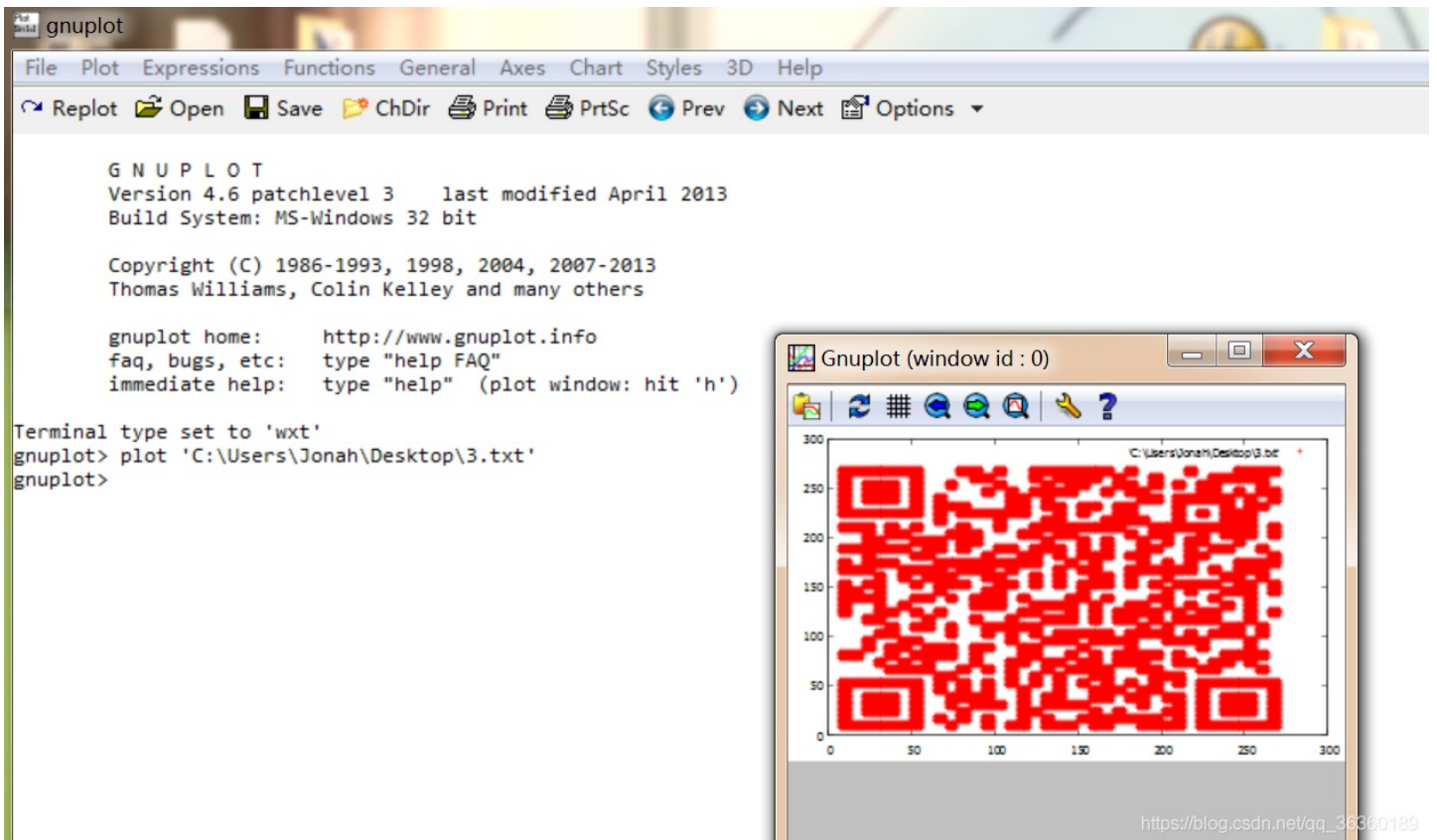


```
3.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
7 8
7 9
7 10
7 11
7 12
7 13
7 14
7 15
7 16
7 17
7 18
7 19
7 20
7 21
7 22
7 23
7 24
```

https://blog.csdn.net/qq_36360189

这种格式)

然后运行gnuplot。



https://blog.csdn.net/qq_36360189

然后扫描二维码flag就出来了...

总结一下常用的图片文件头标识:

JPEG/JPG - 文件头标识 (2 bytes): FF D8 FF,文件结束标识 (2 bytes): FF, D9

PNG - 文件头标识 (8 bytes) 89 50 4E 47 0D 0A 1A 0A

GIF - 文件头标识 (6 bytes) 47 49 46 38 39(37) 61

G I F 8 9 (7) a

BMP - 文件头标识 (2 bytes) 42 4D B M

以及

gnuplot直接用“plot 函数/文件”可以导出图片 (更复杂的操作应该还用不上)

这道题就是脑洞题...

因为以前做的图片题都是hex / binwalk+foremost / stegsolve/ (上次实验班考核还新get了一个silenteye的图片加密解密工具)

不过get了新的姿势, 还是记一下。