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

本文链接：https://blog.csdn.net/qq_36360189/article/details/87896569

---

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

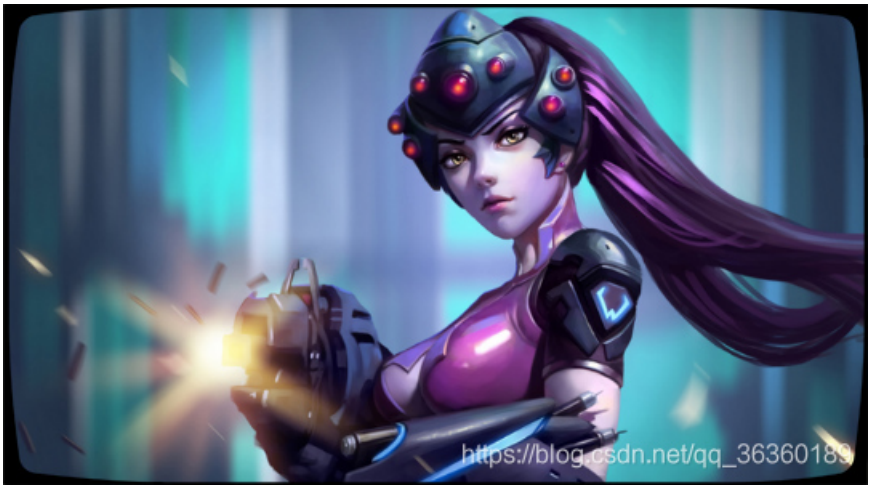
这个题是今年实验班考核的时候一个学长出的300分的杂项，然后当时没做出来…回来之后在学长的提示下做出来了otz…

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…）~~

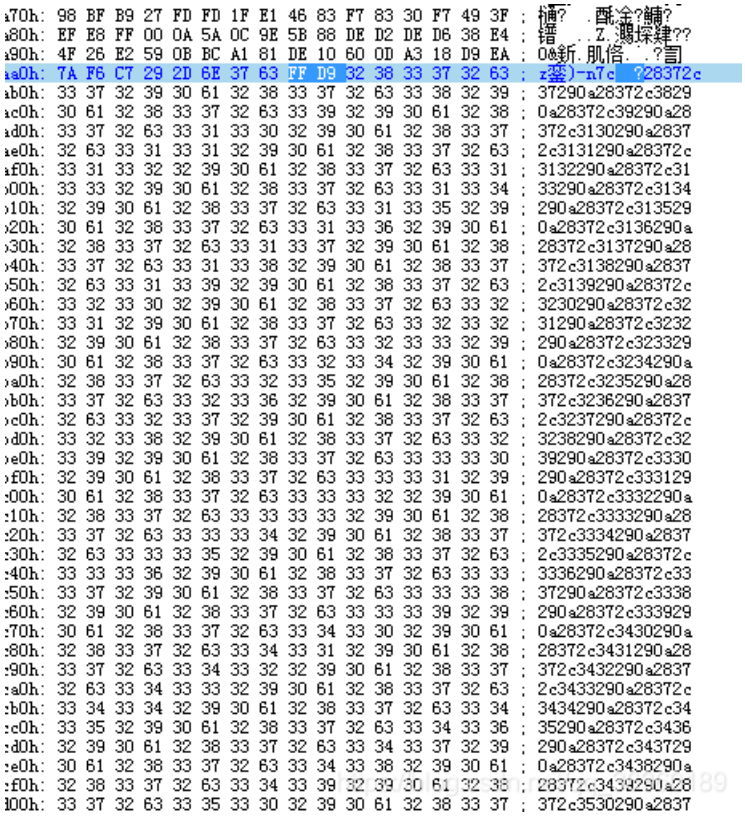
原本好像是zip伪加密方式（记不太清楚了），做出来可以得到一张jpg图。

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。



可以看到ffd9的文件后包含了一些其他的东西。
这是16进制的编码，通过在线进制转换回ascii码，得到一堆的坐标点。

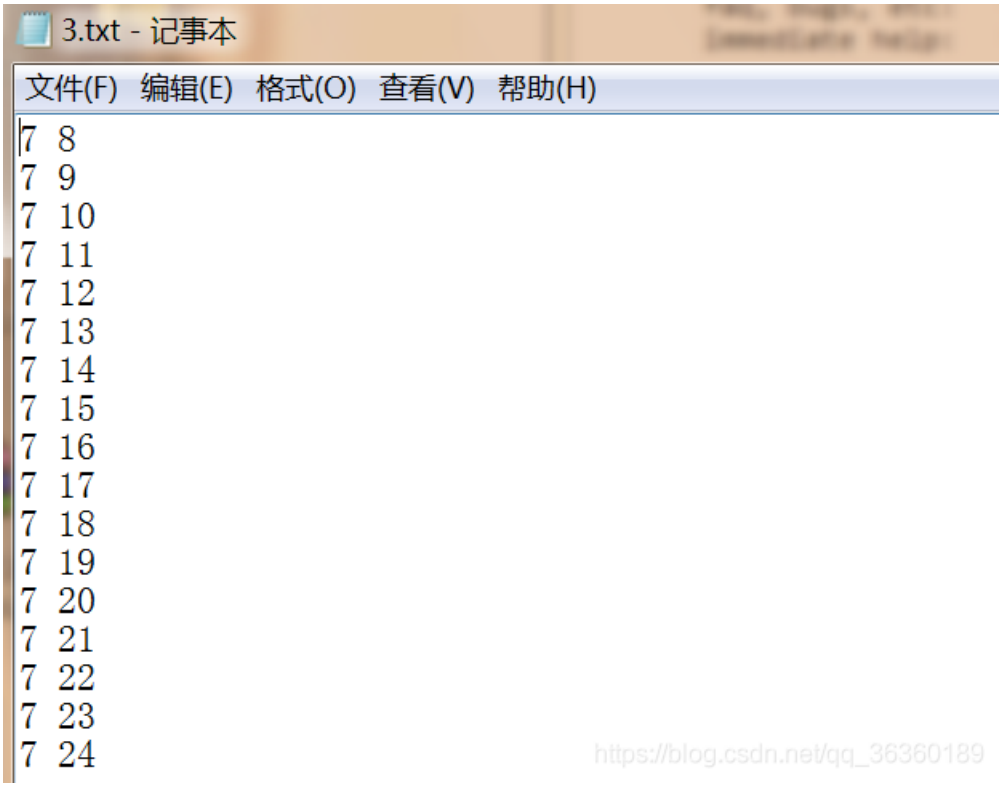
学习到了一个工具…能将坐标点转化成图像的——gnuplot。

通过命令plot直接就能将一组坐标转化为图片，真四神奇啊！

但是用gnuplot跑的时候发现有个问题…它不能直接识别（x，y）这种格式的。

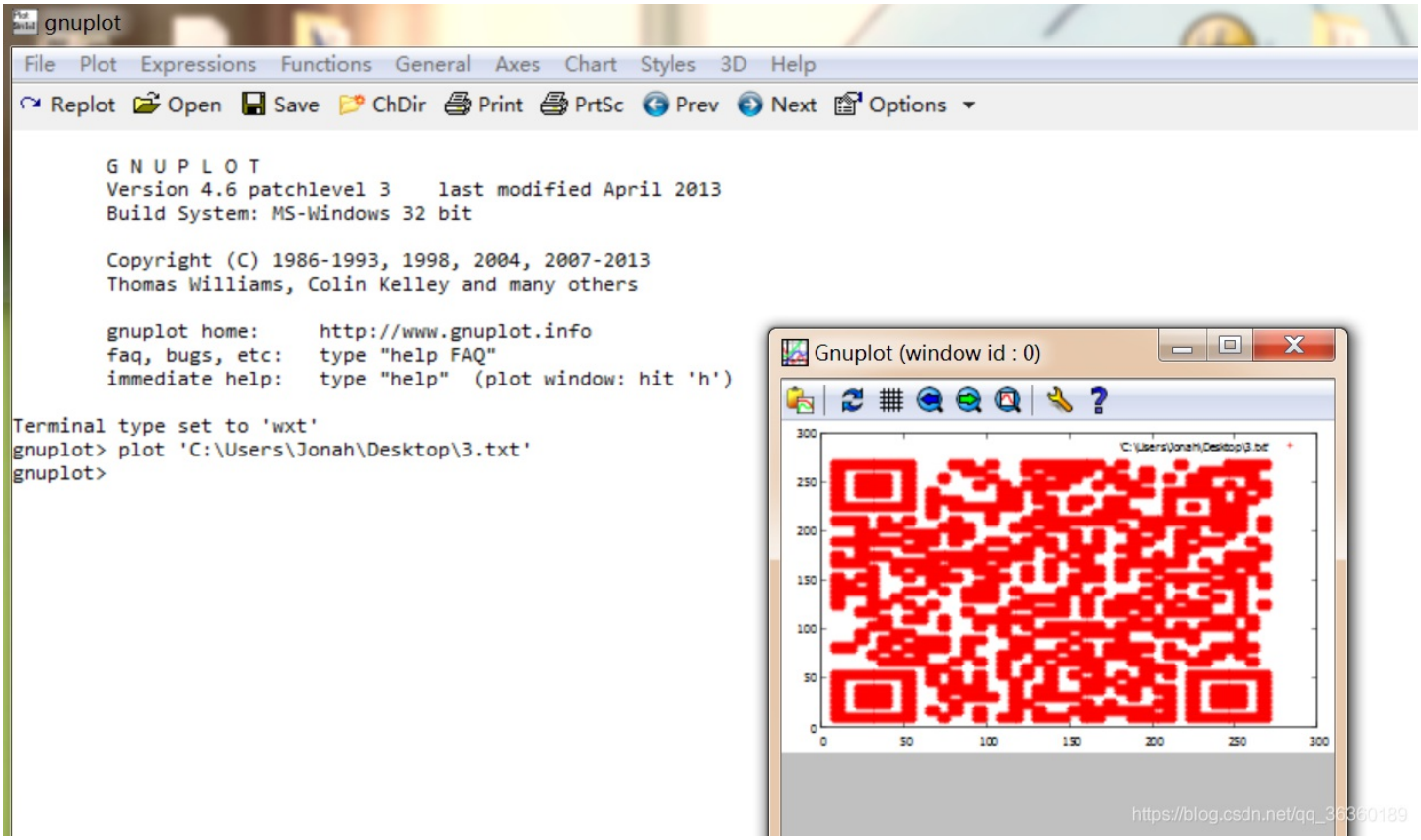
我：“…”

…然后找了很久，找了个文本编辑器。editplus，轻量级，还能直接转html格式，以及统计字数什么的…非常方便，运用替换（，）为空，然后首行缩进，将文本导出为3.txt。



这种格式）

然后运行gnuplot。



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。