0x005图片隐写之双图对比+RGB通道隐写

原创

任骏锋 于 2018-07-02 08:30:05 发布 4622 收藏 7
分类专栏： CTF之图片隐写 文章标签： 图片隐写 Misc CTF 学习笔记

本文链接：https://blog.csdn.net/u010391191/article/details/80863887

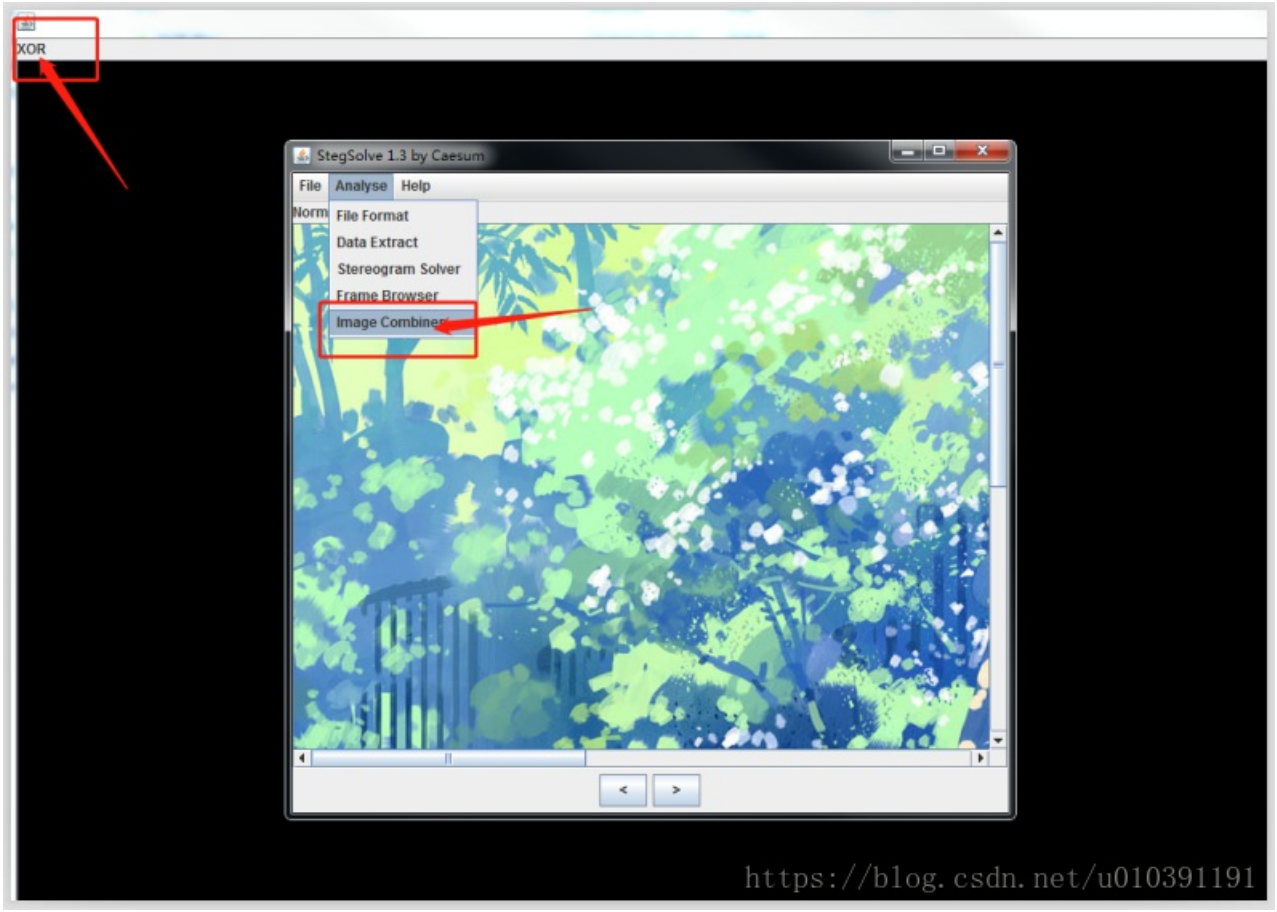

CTF之图片隐写 专栏收录该内容
7 篇文章 0 订阅
订阅专栏

k

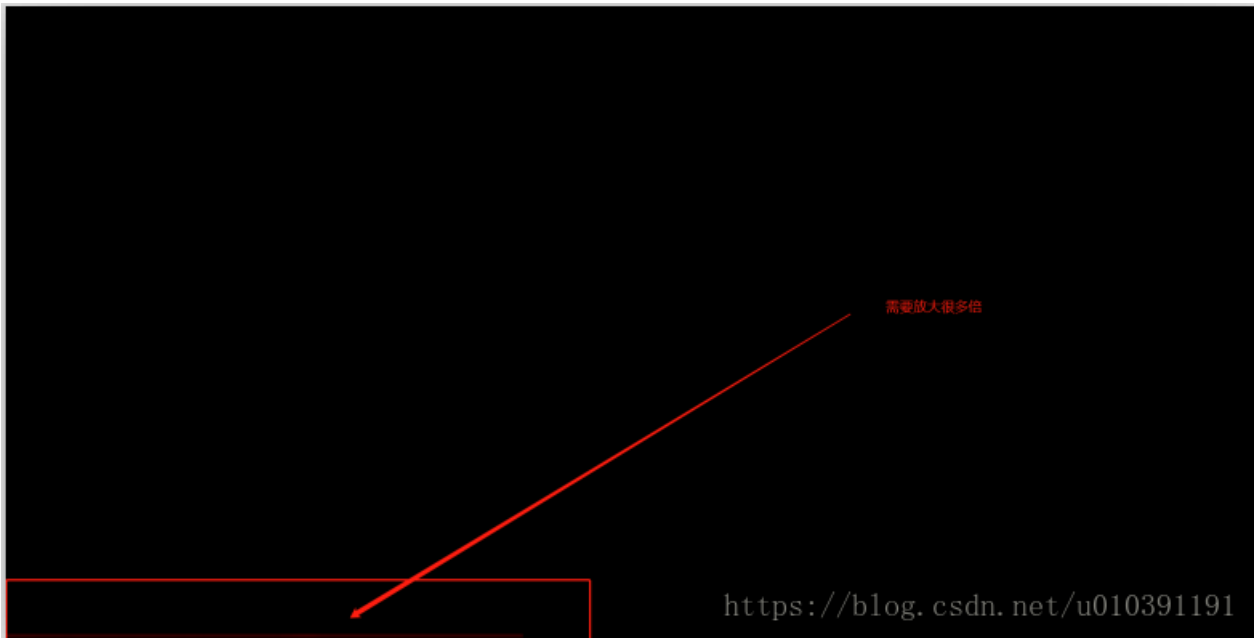
图片链接：https://pan.baidu.com/s/1l6KeF-RFRBYGwYTFe6GhCQ 密码：576c

1、拿到图片常规操作扔到binwalk看一眼，binwalk跑一下发现含多个图片；binwalk跑一下发现分离多个文件（不知是版本问题还是啥的，总觉得自己的binwalk有问题，用foremost再跑一边，发现有2张一模一样的图查看大小也一样）

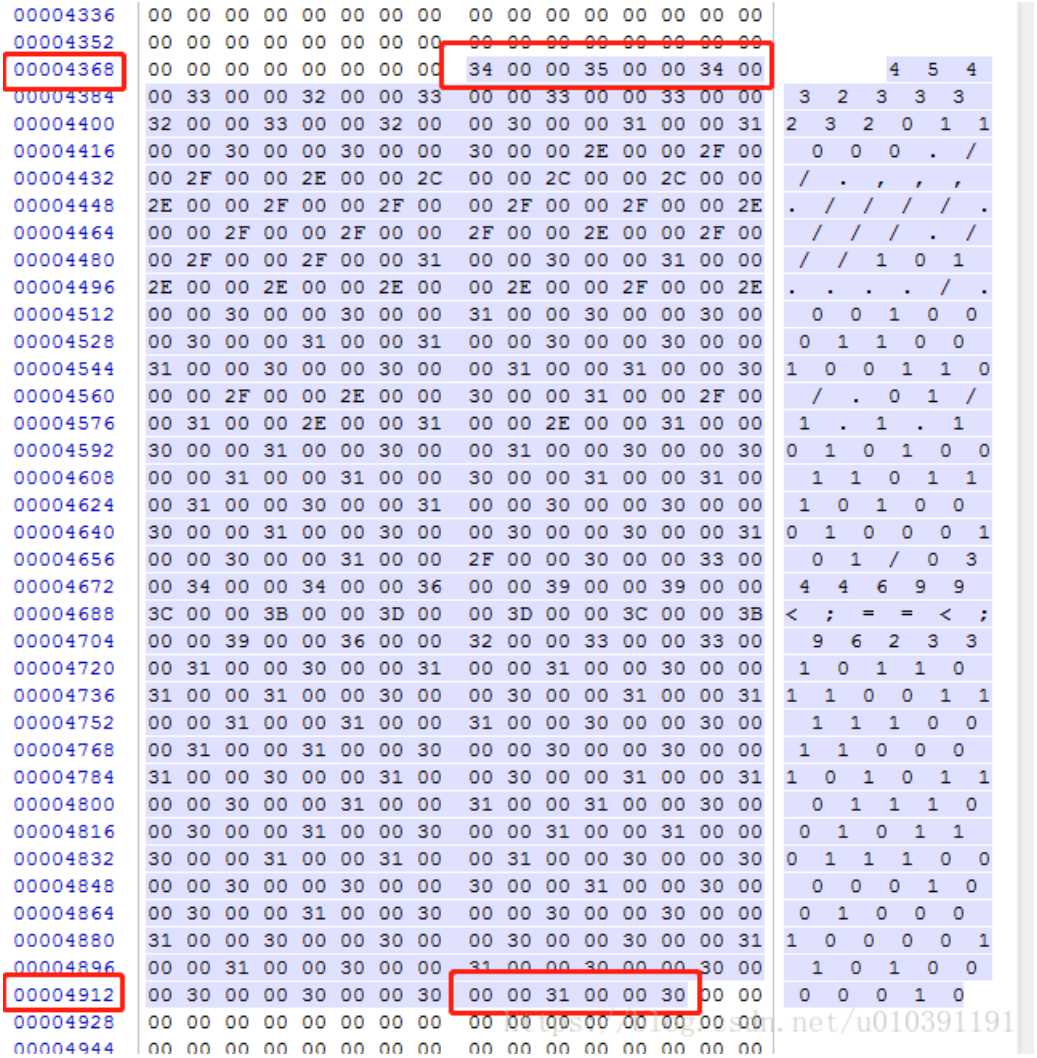
2、拿到2张图，猜想信息应该是隐藏在两张图片中，用StegSolve　Xor异或跑一下，发现一片黑。　注意了首先此题的信息肯定影藏在2张图片中，不可能全部都是黑



如果全黑代表着两张图片一模一样每一个字节都一样（因为异或运算，00为黑）。放大图片发现果然



对上图异或的sloved.bmp图片，进行winhex查看，找出非黑色的偏移处。即非00处。

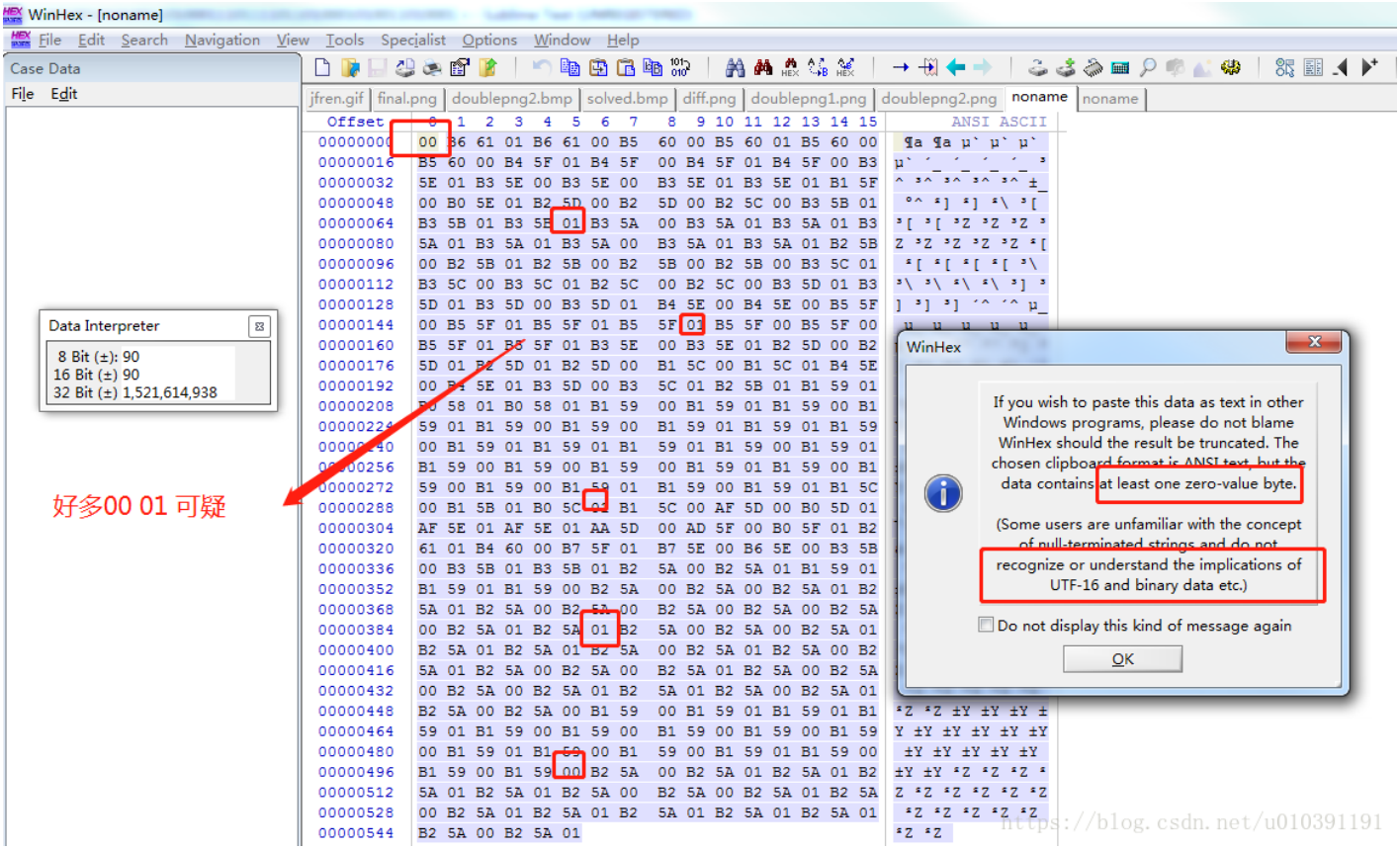


这里为图片不一样处，打开两张图片分别找到对应偏移处（注意这里需要把分离出来的2张图片先转成bmp，一是因为XOR的图片格式为BMP需要使用相同格式的图片寻找差异处，另外一点bmp）

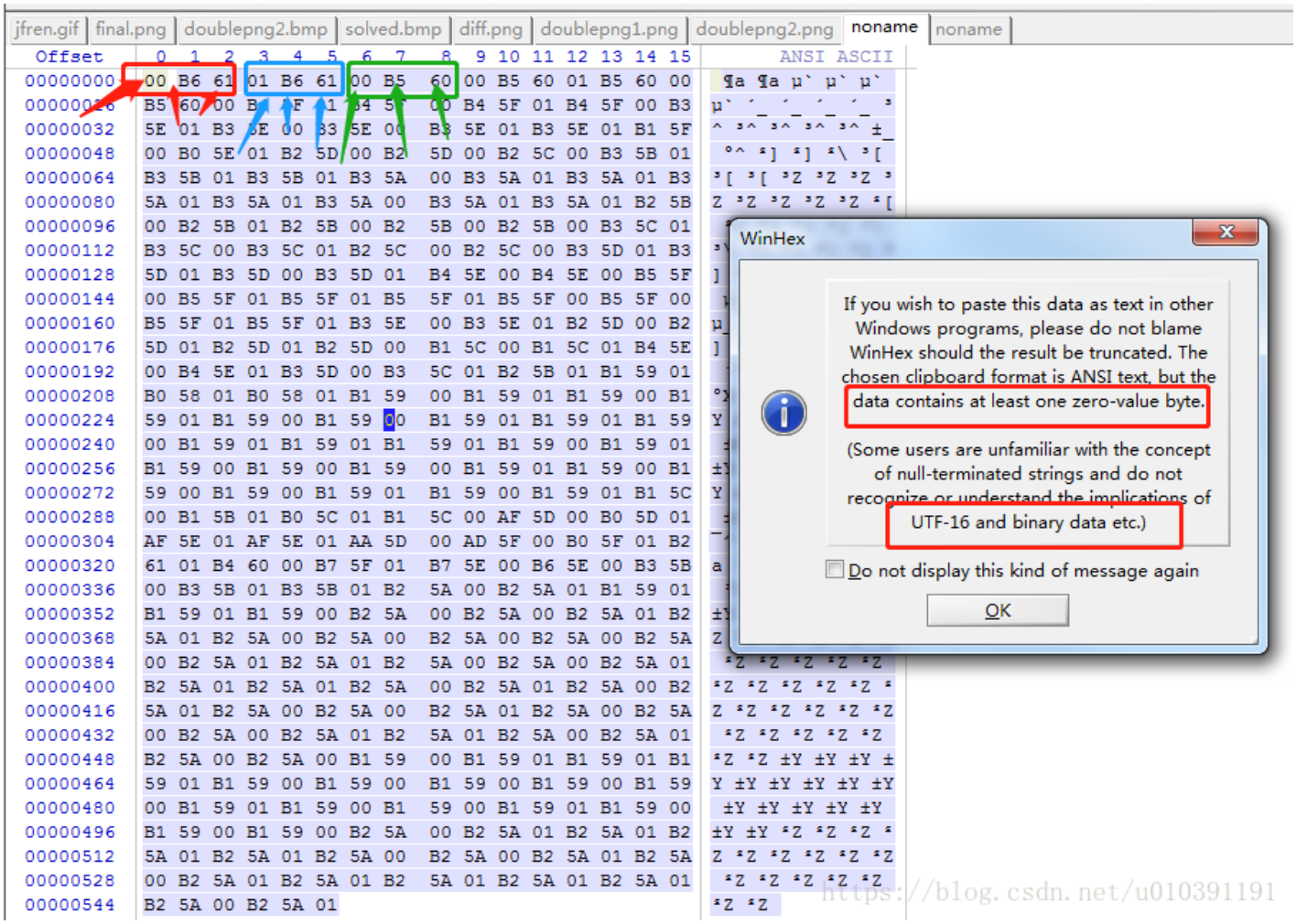
这里就是两张图片不一样的地方。也是信息隐藏点。对这一数据块进行深入分析

将信息影藏数据块复制出来，发现无法复制。

然后发现有很多00 01



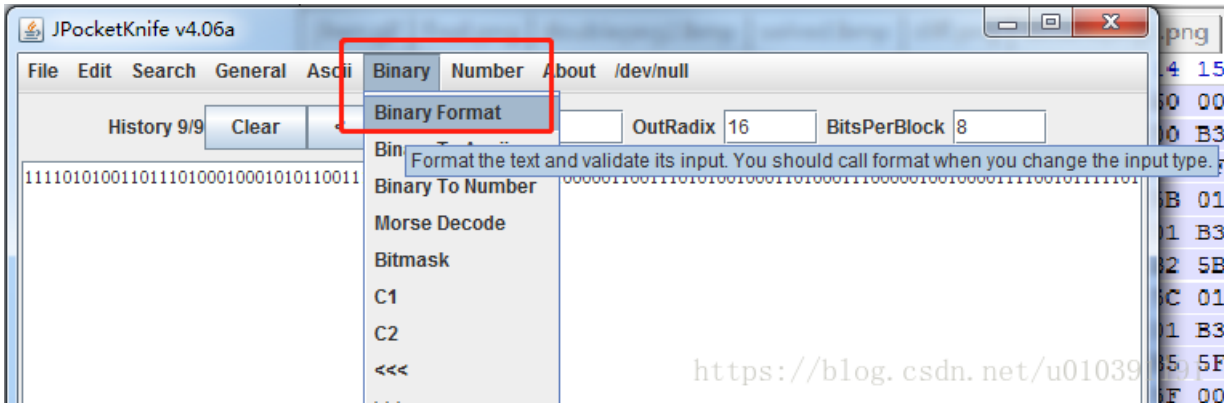
再仔细观察发现RGB在每个R通道里都是00/01，信息隐藏在R通道中， 其他通道都是图片的正常像数信息，想办法过滤。（每3个Hex的第一个hex的值都是00/01）

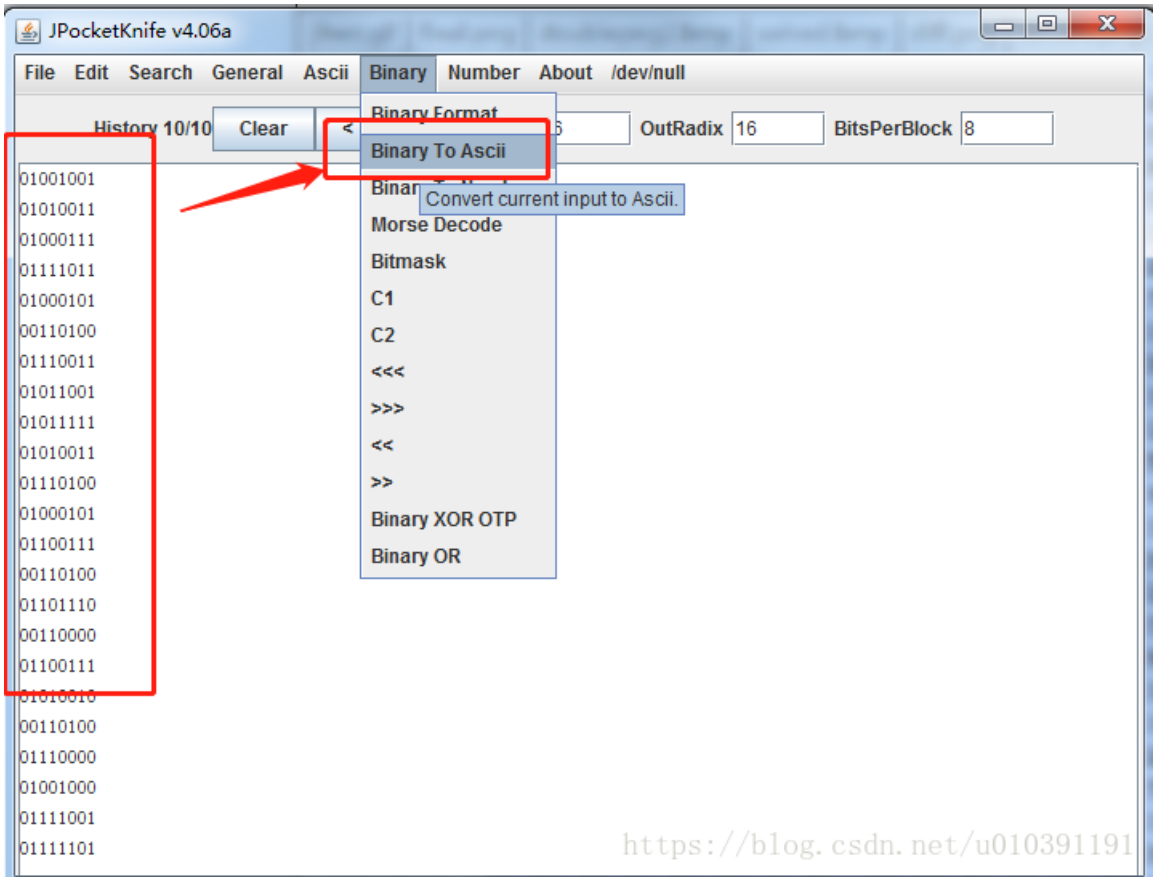


无法拷贝出，使用笨方法，打开TXT文档手动将所有00/01敲进去= =~

再仔细观察，想到用常见的0101处理的几种方法：二维码发现不是某数的平方、binary编码发现不可见字符都无法解决，再回看RGB通道中的R通道信息，发现全是00 或者01 ，按照出题人的思路，可能是将一串binary写入R通道中的时候，0变成了00， 1变成了01。尝试一下将00替换成0、01替换成1。（脑洞/经验）.

发现是8的倍数






JPocketKnife v4.06a
File Edit Search General Ascii Binary Number About /dev/null
History 11/11 Clear < > InRadix 16 OutRadix 16
ISG{E4sY pHy}
最终得到flag...
http://blog.csdn.net/u010391191

ヽ(￣▽￣)~~