CTF之图片隐写

原创

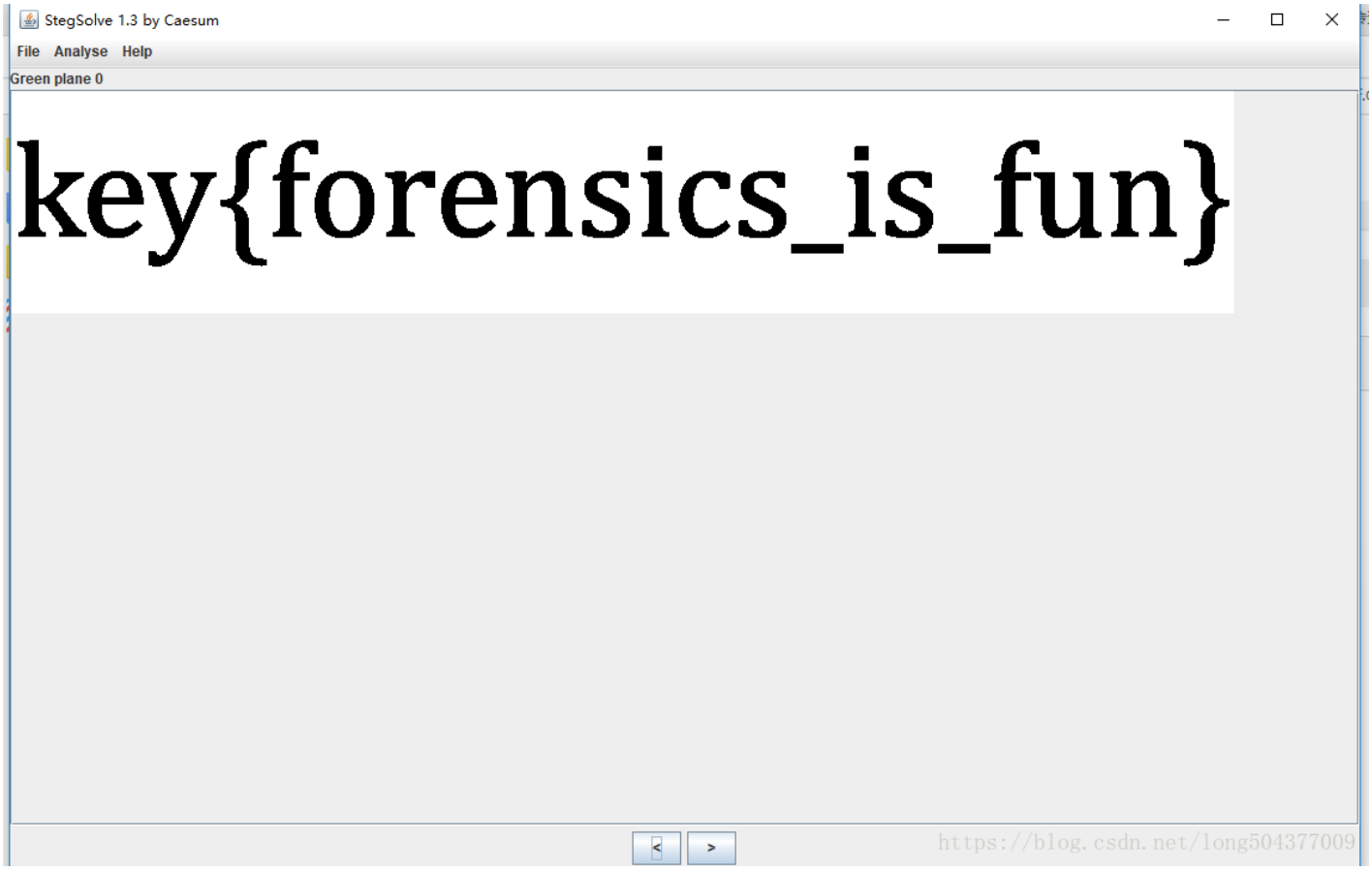
long504377009 于 2018-08-15 16:04:47 发布 53401 收藏 189
分类专栏： CTF 文章标签： CTF

本文链接：https://blog.csdn.net/attitudeisaltitude/article/details/81698719


CTF 专栏收录该内容
2 篇文章 2 订阅
订阅专栏

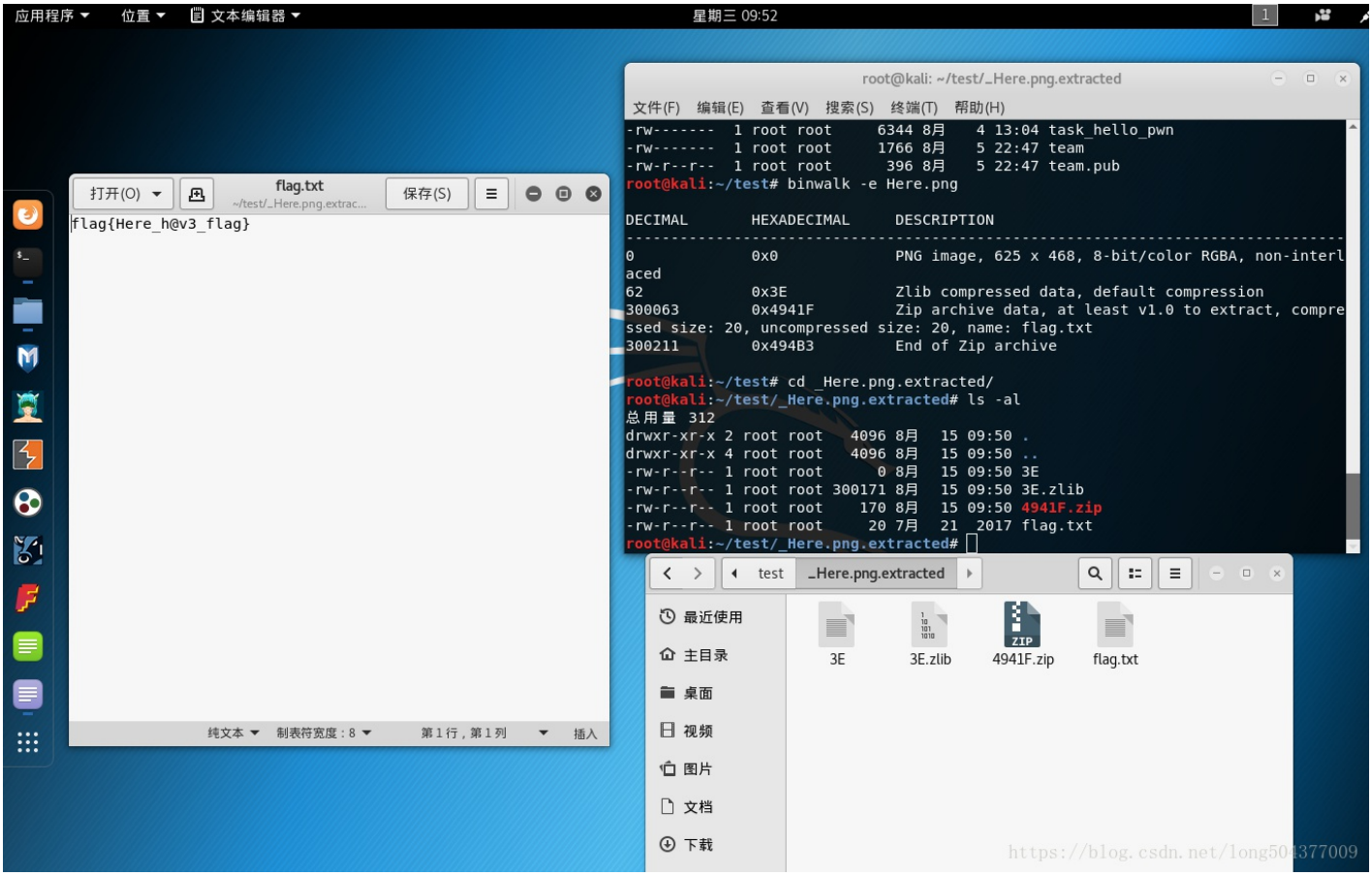
图片隐写1：chal.png，图片如下：

题目图片即为一张白板，用Stegsolve.jar工具打开，向右疯狂点箭头得到flag：



题目2：Here.png：

直接拖到kali里用binwalk -e Here.png得到释放出的文件夹中有flag.txt，打开即得到flag。

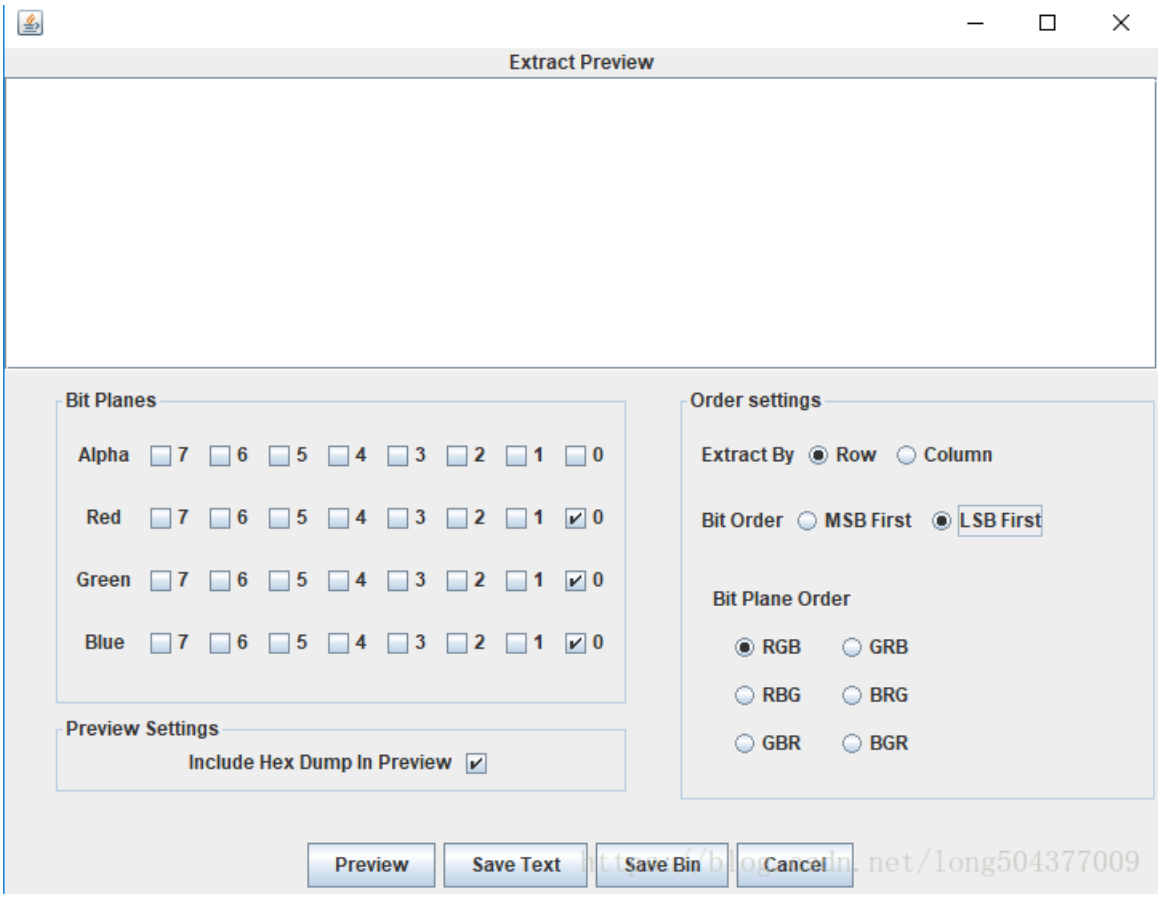


题目3：flag.png：

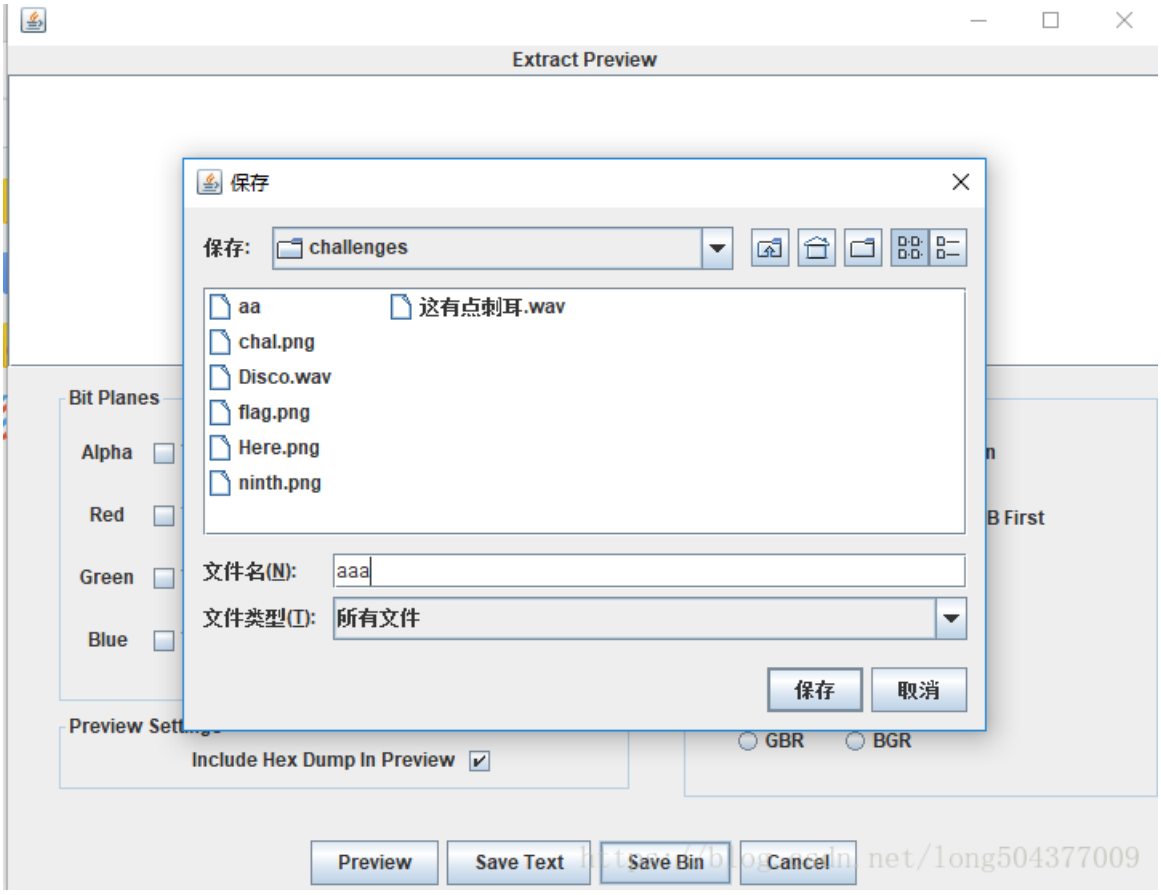
这个是LSB隐写：

首先用Stegsolve.jar打开

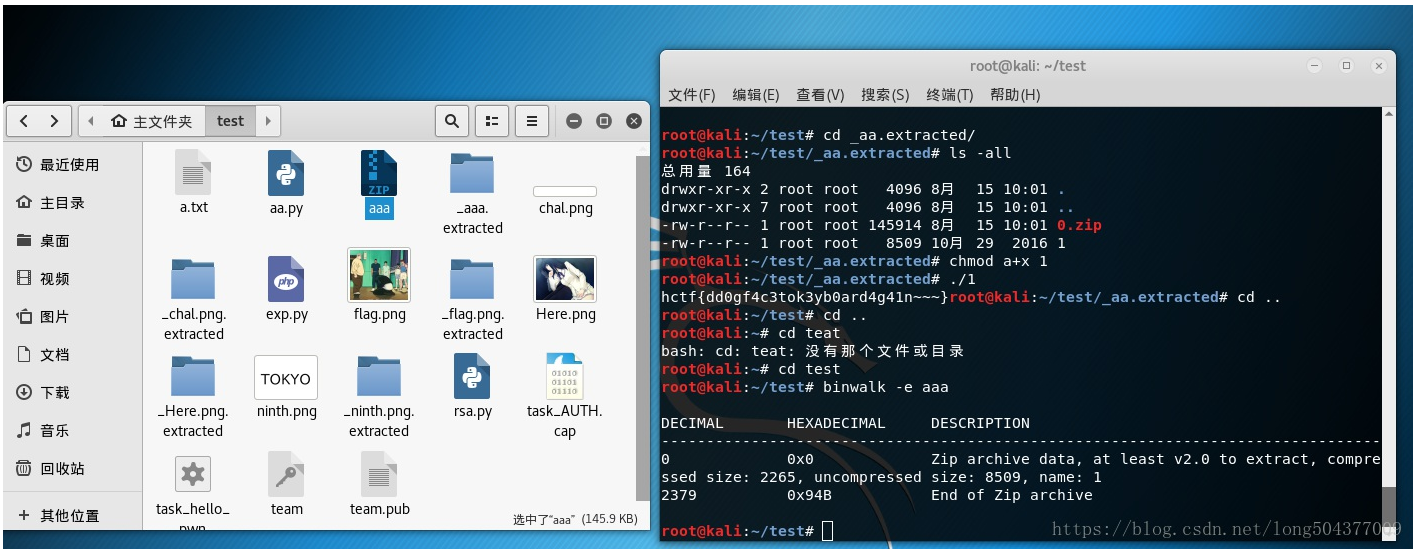
analyse->data extract->



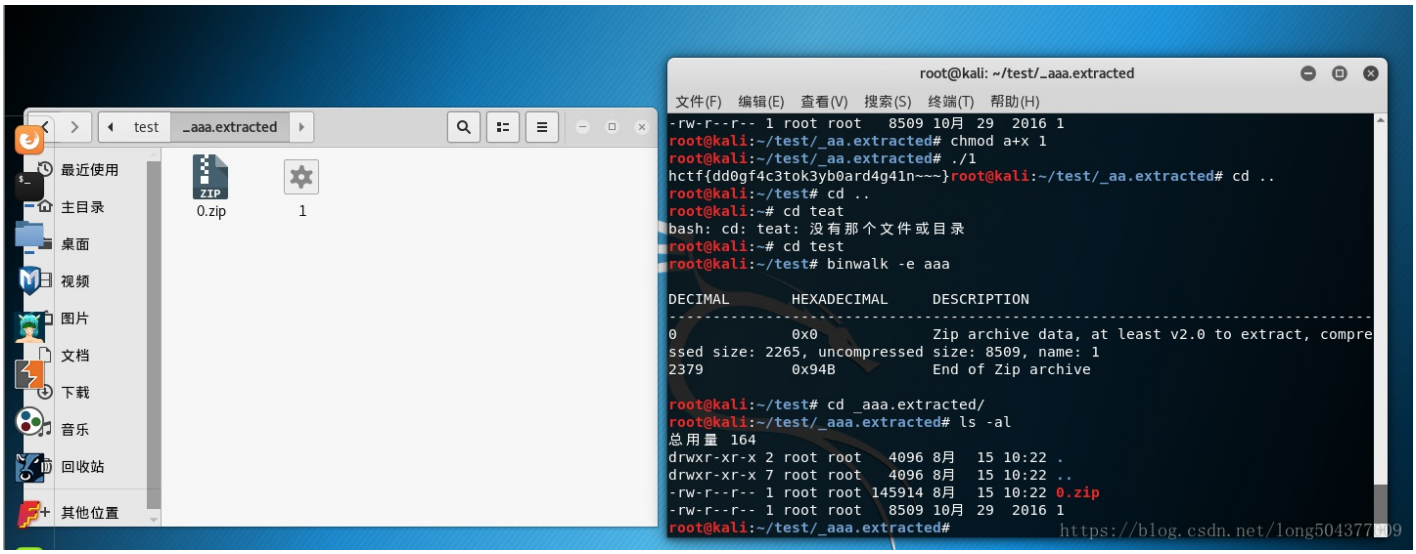
分别选中red,green,blue的最低0位，然后右侧选中LSB First，然后Save Bin



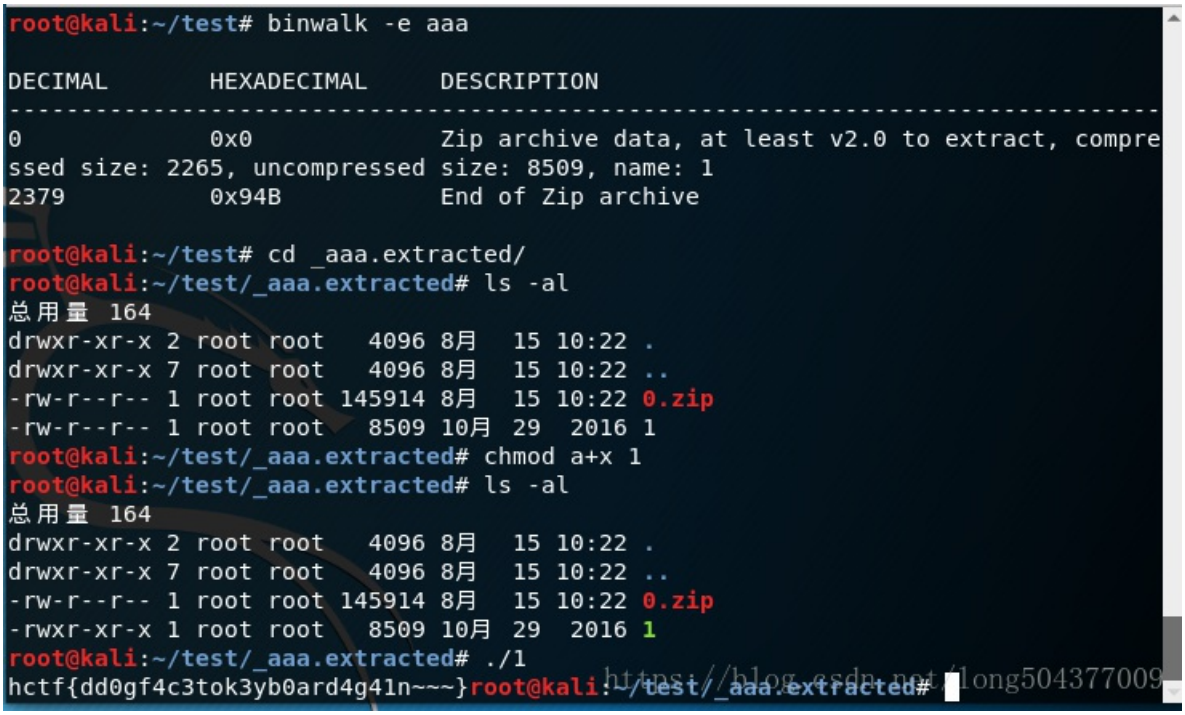
保存得到aaa文件，将aaa文件拖入kali中binwalk之



得到释放后的_aaa.extracted进入看到：



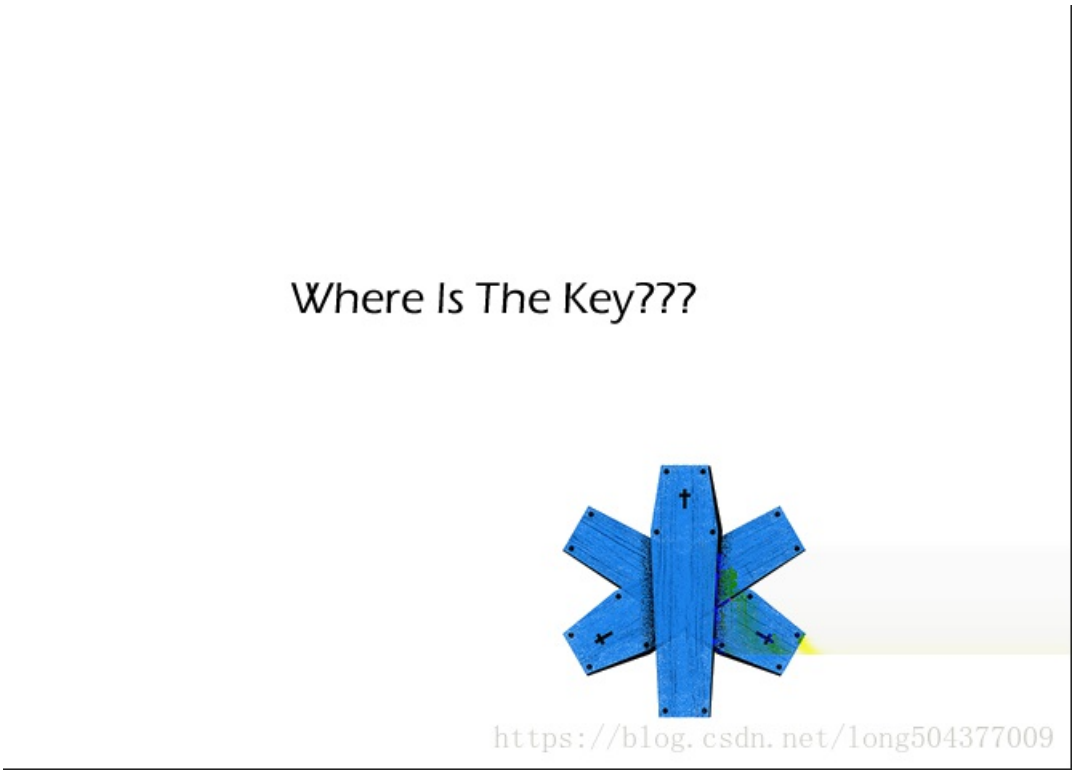
有一个1文件,利用chmod a+x 1 改变文件1位可执行并执行得到flag



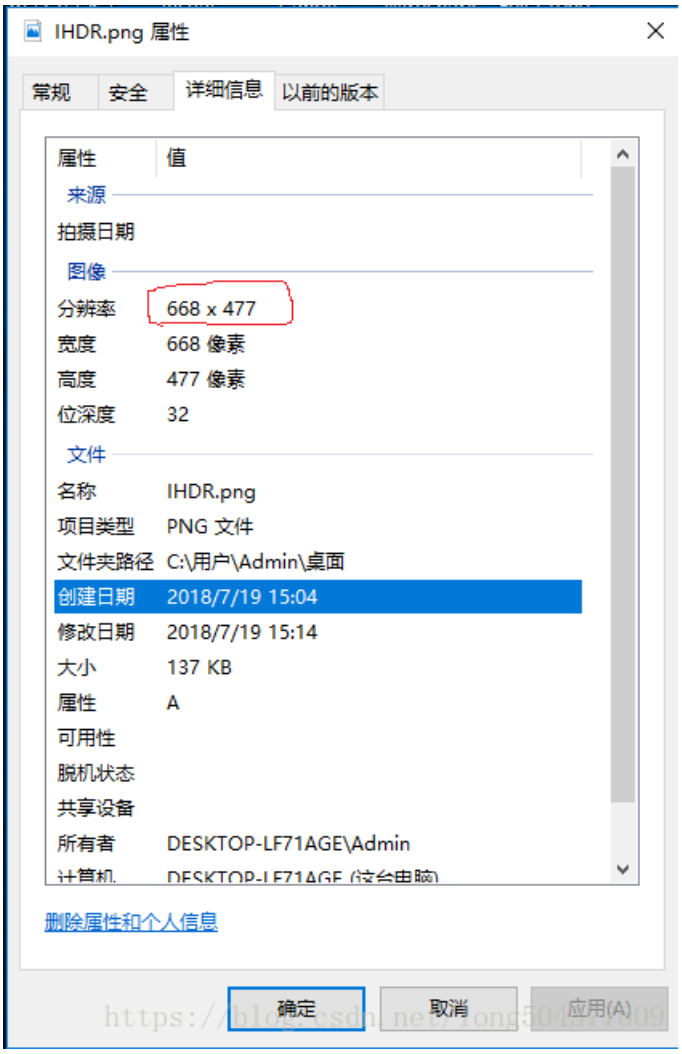
由上可得flag。

lsb隐写，一般都藏在0,1,2这些低位里面，在软件功能选项中查看Analyse→Data Extract，逐个调试。

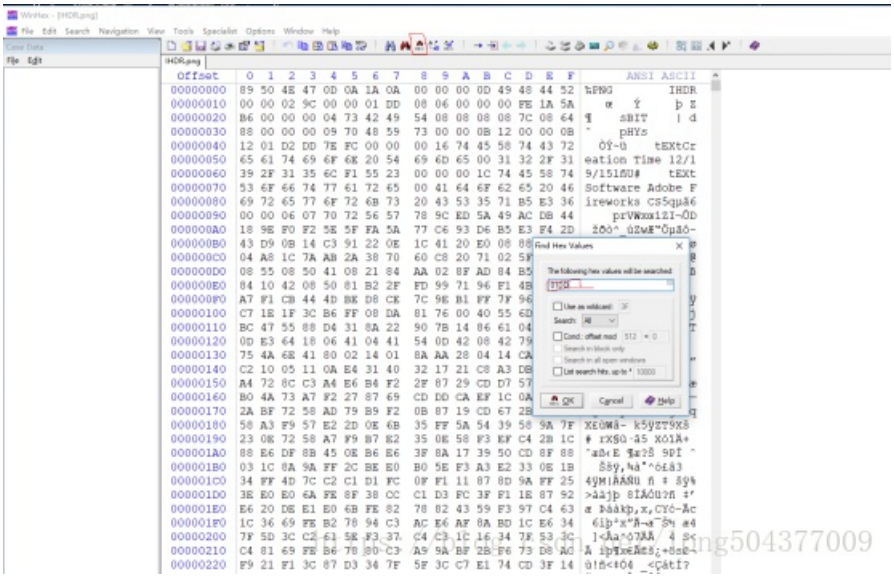
题目4：图片拉长： 



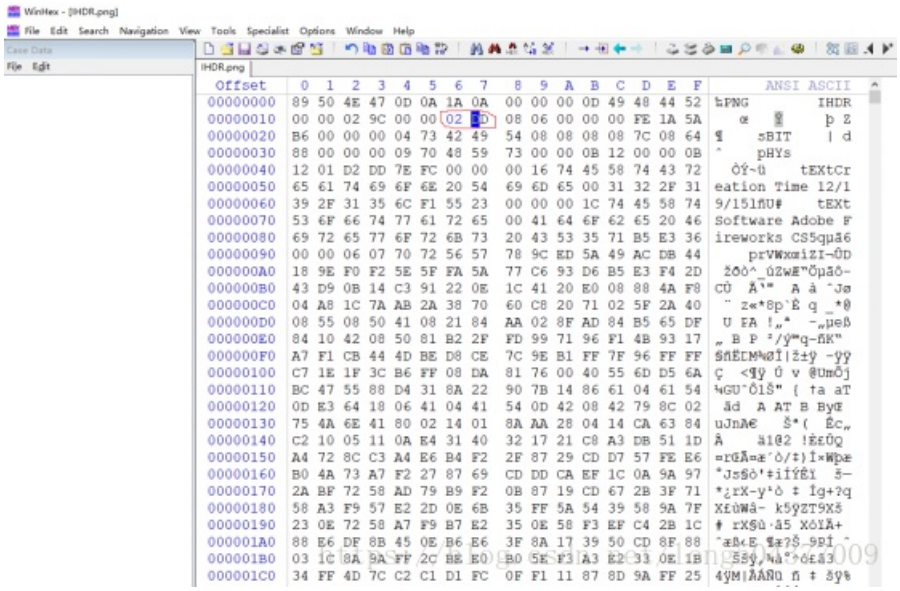
图片属性，查看图片像素



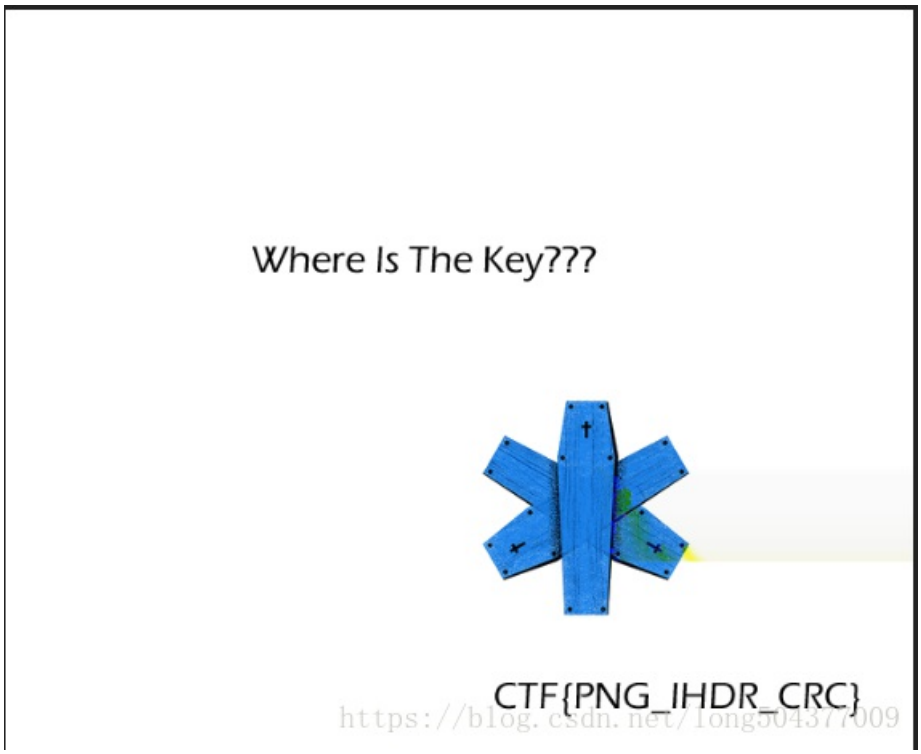
高为0477，利用calc.exe命令调出计算器，换算成十六进制为01DD。利用打开图片搜索十六进制01DD



找到后改为02DD拉长（对于png文件，其第二行第六列是高度位，改这一位即可）



保存可以看到flag



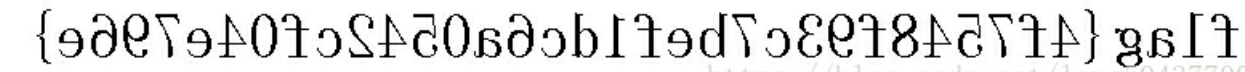
记住改第2行，第6列。

题目5：图片逆转：1.reverseMe：

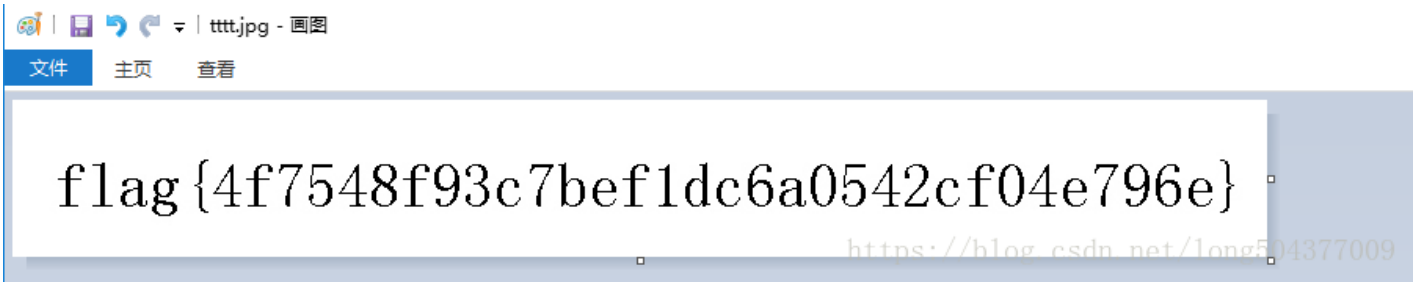
下载下来的文件用winhex查看一下发现头部D9FF很眼熟啊，想起来和JPEG文件格式的尾部FFD9正好反过来而且题目是reverseMe，赶紧去看看尾部D8FF正好是JPEG文件头倒过来，编写脚本：

```
#!usr/bin/python
f = open('C:\\jiaoben\\tttt.jpg','wb')
g = open('C:\\jiaoben\\1.reverseMe','rb')
f.write(''.join(g.read()[::-1]))
g.close()
f.close()
```

注意文件存放的目录，运行完成后生成tttt.jpg



利用mspaint windows自带的画图工具水平翻转即可:



最后把题目和工具上传。