


实验三：隐写与取证(图片LSB/JPEG文件隐写)

原创

ZERO-A-ONE  于 2021-04-27 10:58:19 发布  631  收藏 1

分类专栏: [大学实践作业](#) 文章标签: [python](#) [java](#) [信息安全](#) [linux](#)

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/keixLZ/article/details/116195159>

版权



[大学实践作业](#) 专栏收录该内容

16 篇文章 5 订阅

订阅专栏

一、实验目的

明白信息隐藏原理, 了解相关软件操作过程, 掌握提取隐藏信息方

二、实验题目

(1) 找出图片 01.png 中隐藏的信息, flag 为 32 位随机序列, 并且为第 2 小题的密

提示: 使用 Stegsolve.jar

(2) 找出图片 02.jpg 中隐藏的信息

提示: 使用 Stegdetect 和 JPHS, kali 中命令: stegdetect -tjopi -s 10.0 ./02.jpg

(3) 找出 03.jpg 文件中隐藏的信息

提示: 隐藏了一只猫猫

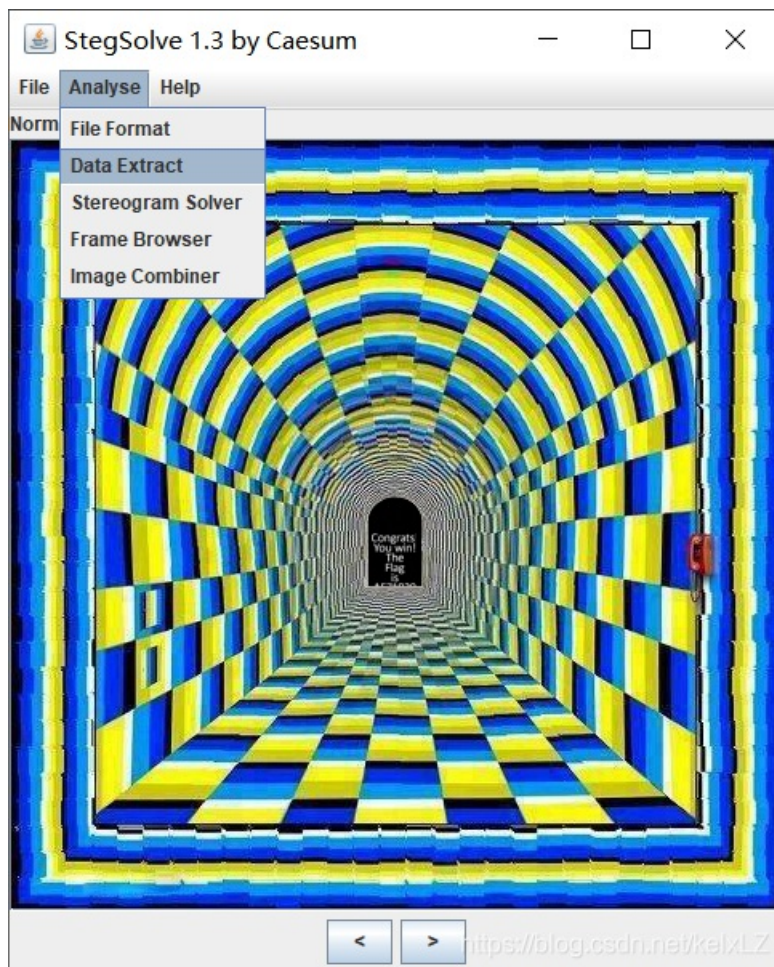
三、实验环境工具

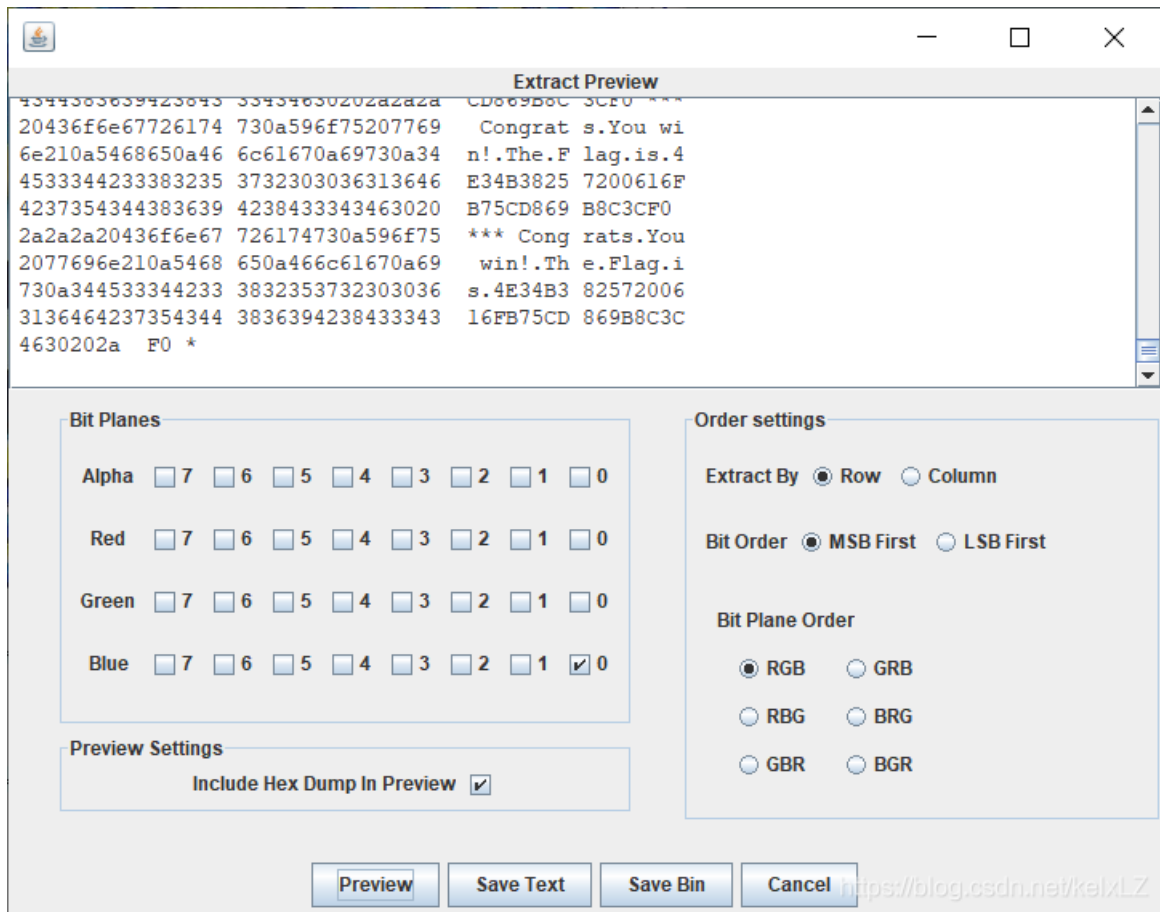
- Windows 7系统或以上、连接Internet的主机
- winhex软件, Stegsolve.jar软件
 - Stegsolve菜单主要功能:
 - File Format: 文件格式, 查看图片的具体信息参数, 有时候 flag 会写在图片信息里
 - Data Extract: 数据提取, 如LSB隐写中在图片中隐藏数据的提取
 - Stereogram Solver: 立体视图, 可以左右移动控制偏移量
 - Frame Browser: 逐帧浏览, 对GIF之类的动图进行分解, 便于查看
 - Image Combiner: 拼图, 图片结合, 可以对两张图片进行xor、add、sub等运算
- 隐写工具 Stegdetect可以检测到通过JSteg、JPHide、OutGuess、Invisible Secrets、F5、appendX和Camouflage等这些隐写算法隐藏的信息, 并且还能基于字典暴力破解密码, 以提取通过Jphide、outguess和jsteg-shell方式嵌入的隐藏信息。在kali中安装 Stegdetect 的方法: `apt-get install stegdetect`, 使用Stegdetect查看图片的隐藏信息: `stegdetect -tjopi -s 10.0 ./xxx.jpg`

四、实验步骤及结果

4.1 01jpg

找出图片 01.png中隐藏的信息, flag为32位随机序列, 并且为第2小题的密码。使用Stegsolve.jar工具, 导入01.png图片并进行数据提取操作, 结果如下:





可以发现flag:

The Flag is: 4E34B38257200616FB75CD869B8C3CF

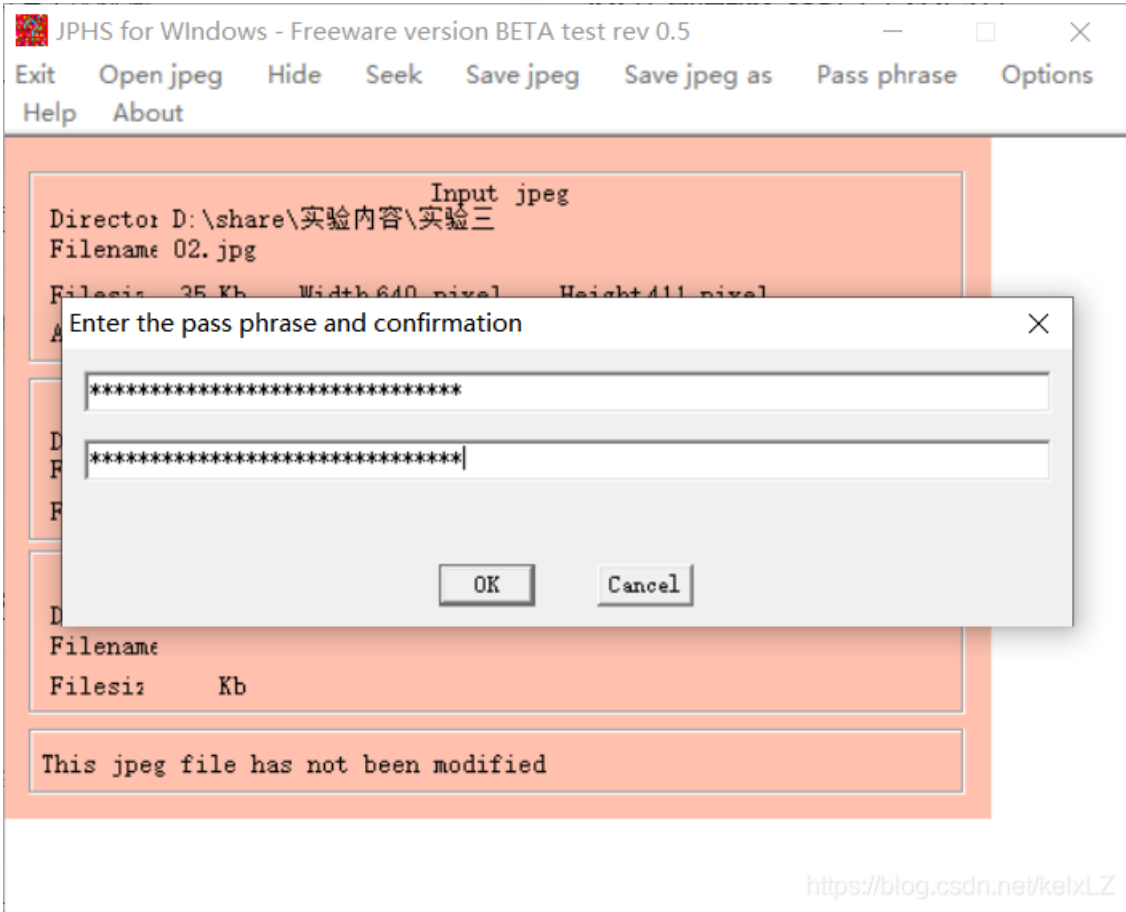
4.2 02.jpg

使用Stegdetect进行检查之后发现是jphide加密

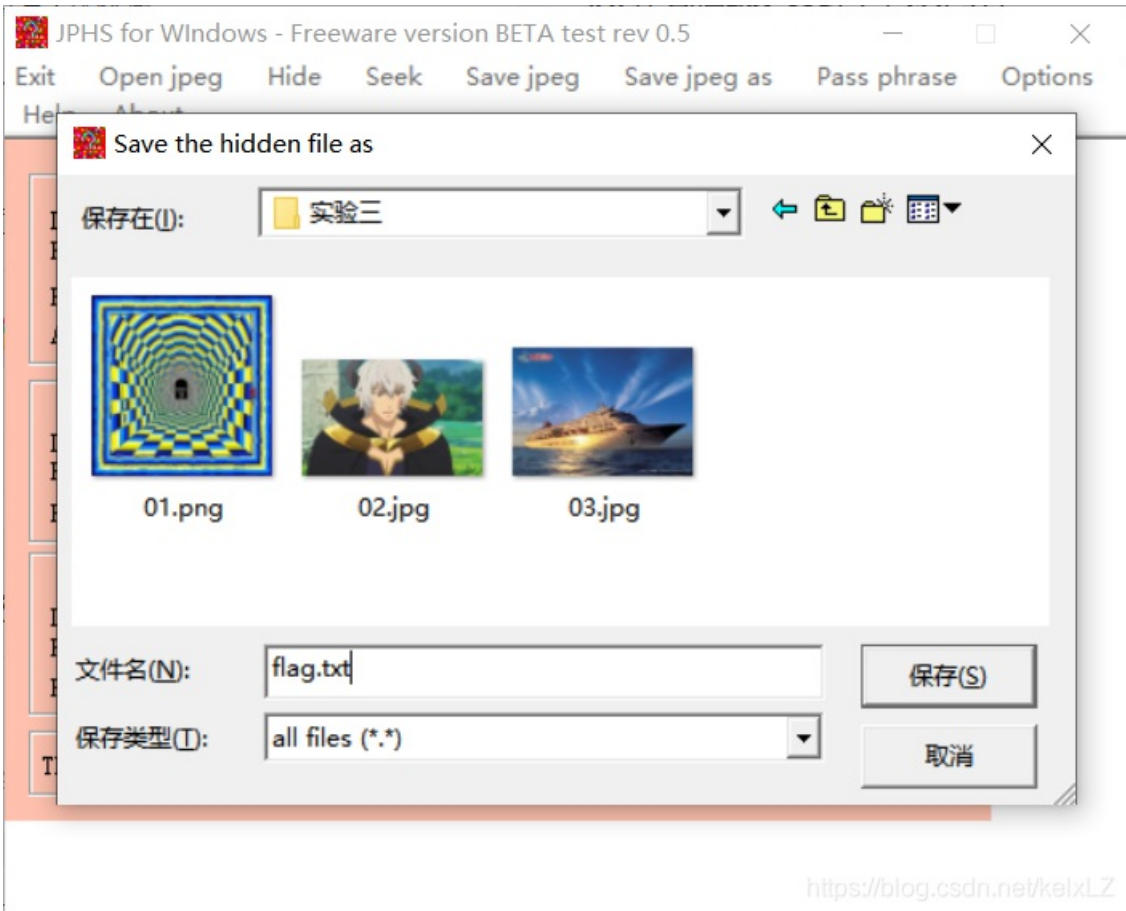
```

D:\QQ文件\实验工具\stegdetect0.4>stegdetect.exe -tjopi -s 10.0 02.jpg
02.jpg : jphide(*)
D:\QQ文件\实验工具\stegdetect0.4>
  
```

后面根据提示，之前的flag为第二题的密码，所以打开JPHS，打开文件之后使用seek功能



保存flag.txt



打开获得flag

flag{rois_2020}

4.3 03jpg

使用Stegsolve.jar逐帧查看，获得猫片



<https://blog.csdn.net/kelxLZ>