杂项------文件隐写

原创

Sylvia_j 于 2020-04-12 17:21:32 发布 1694 收藏 12

分类专栏： 笔记

本文链接：https://blog.csdn.net/qq_46927150/article/details/105469929

学习链接：https://www.bilibili.com/medialist/play/ml776247675

一、文件内容隐写

> 文件内容隐写，就是直接将KEY以十六进制的形式写在文件中，通常在文件的开头或结尾部分,分析时通常重点观察文件开头和结尾部分。
> 如果在文件中间部分，通常搜索关键字KEY或者flag来查找隐藏内容。

使用场景: windows下， 搜索隐写的文件内容

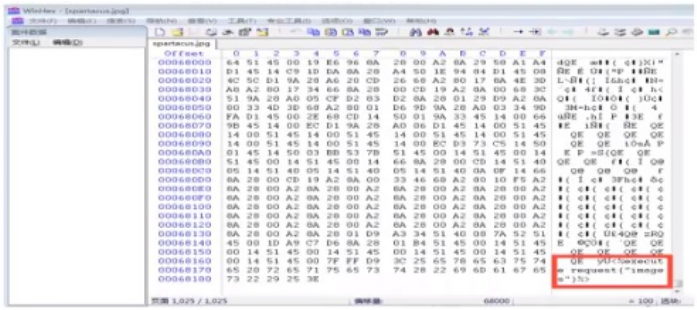
1.Winhex/010Editor

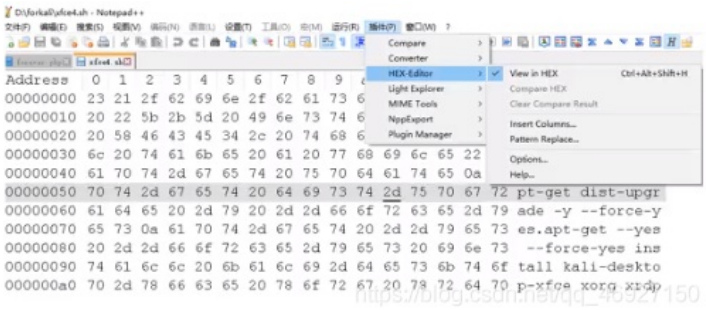
通常将要识别的文件拖入winhex中，查找具有关键字或明显与文件内容不和谐的部分，通常优先观察文件首部和尾部,搜索flag或key等关键字，最后拖动滚轮寻找。

2.Notepad++

使用notepad++打开文件，查看文件头尾是否有含有关键字的字符串，搜索flag或key等关键字， 最后拖动滚轮寻找。

另外通过安装插件HEX- Editor可以实现winhex的功能。





二、图片文件隐写

**图片隐写的常见隐写方法：

1.细微的颜色差别

2. GIF图多帧隐藏

(1).颜色通道隐藏

(2).不同帧图信息隐藏

(3). 不同帧对比隐写

3. Exif信息隐藏

4.图片修复

(1).图片头修复

(2). 图片尾修复

(3). CRC校验修复

(4). 长宽、高度修复

5.最低有效位LSB隐写

6.图片加密

(1). Stegdetect

(2). outguess

(3). Jphide

(4). F5

三、几种图片隐写中可能会用到的工具

1.Firework

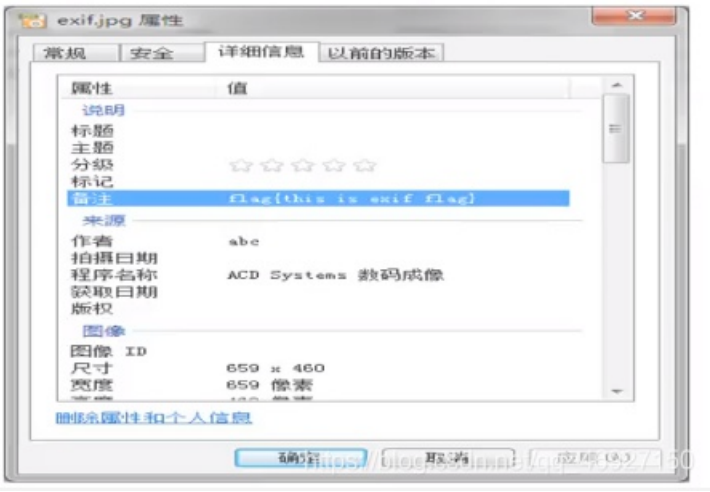
使用winhex打开文件时会看到文件头部中包含firework的标识，通过firework可以找到隐藏图片。

使用场景:查看隐写的图片文件

2. Exif

Exijf按照PEG的规格在PEG中插入一些图像/数字相机的信息数据以及缩略图像可以通过与JPEG兼容的互联网测览器/图片浏览器/图像处理等一些软件来查看Exif格式的图像文件就跟浏览通常的PEG图像文件一样

图片右键属性，查看exif或查看详细信息，在相关选项卡中查找flag信息。



3.Stegsolve

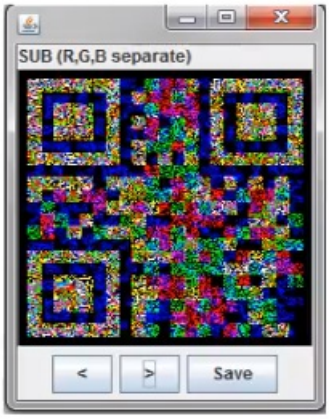
当两张jpg图片外观、大小、像素都基本相同时，可以考虑进行结分析，即将两个文件的像素RGB值进行XOR、ADD、SUB等操作，看能否得到有用的信息，StegSolve可以方便的进行这些操作。

使用场景:两张图片信息基本相同

PS：用notepad++打开第一张图片，发现最后面有一个链接，点进去下载第二张图片

（1）.打开第一张图片，点击analyse->Image combiner（注意顺序，先打开的是重新下载的图片）

（2）.在弹出的窗口中点击左右按钮
选择处理方式，点击save保存有价值的结果。



**图片文件隐写-LSB

4.LSB (最低有效位Least Significant Bit)

LSB替换隐写基本思想是用嵌入的秘密信息取代载体图像的最低比特位，原来的的7个高位平面与替代秘密信息的最低位平面组合成含隐藏信息的新图形。

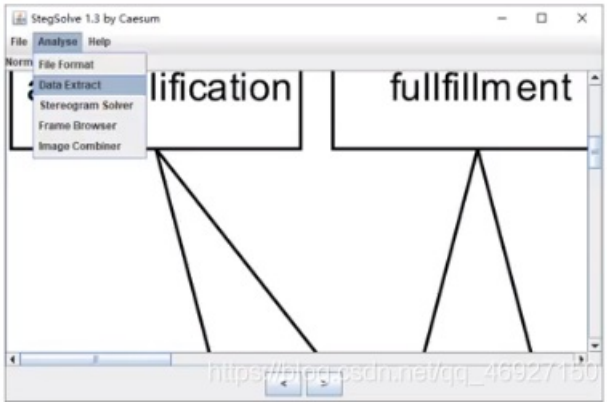
1.像素三原色(RGB)

2.通过修改像素中最低位的1bit来达到隐藏的效果

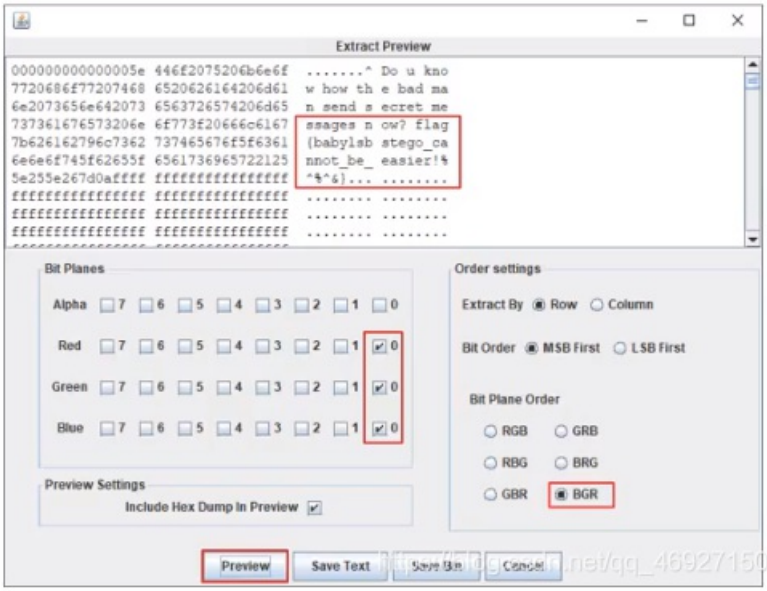
3.工具: stegsolve、 zsteg、 wbstego4、 python脚本

（1）Stegsolve.jar工具

第一步、打开文件>> Analyse > Data Extract



第二步、调整Bit Planes，Bit Order，Bit Plane Order



（2）zsteg工具

Installation

```
root@kali:/# gem install zsteg
```

检测LSB隐写

```
zsteg xxx.png
```

（3）wbstego4.工具

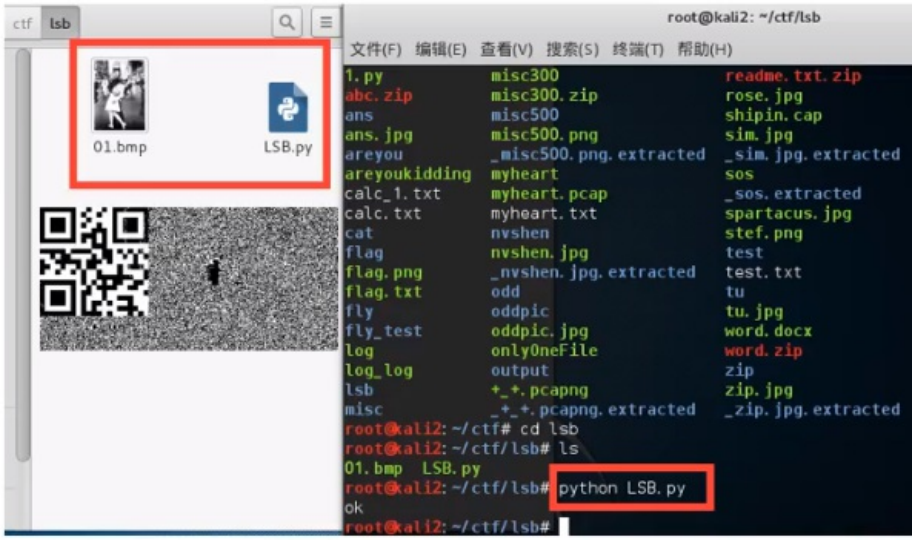
解密通过lsb 加密的图片（主要针对后缀名为.bmp、pdf等图片）

（4）python脚本来处理

将以下脚本放在kali中运行，将目标文件放在脚本同目录下，将脚本中的文件名修改为文件名，运行python 即可（跑脚本或者将该图片转成png后用steg查看通道）

```
LSB.py
#coding:utf-8
import PIL.Image
def foo():
    im = PIL.Image.open('01.bmp')
    im2 = im.copy()
    pix = im2.load()
    width,height=im2.size

    for x in xrange(0,width):
        for y in xrange(0,height):
            if pix[x,y]&0x1 == 0:
                pix[x,y]=0
            else:
                pix[x,y]=255
    im2.show()
    pass
if __name__ == '__main__':
    foo()
    print 'ok.'
    pass
```



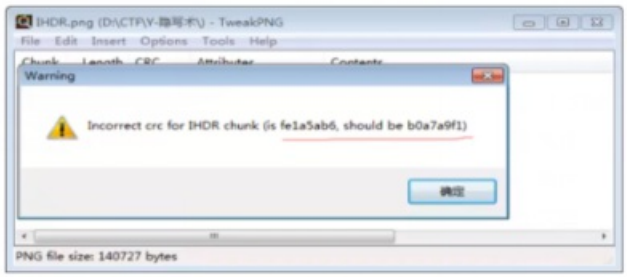
5.TweakPNG

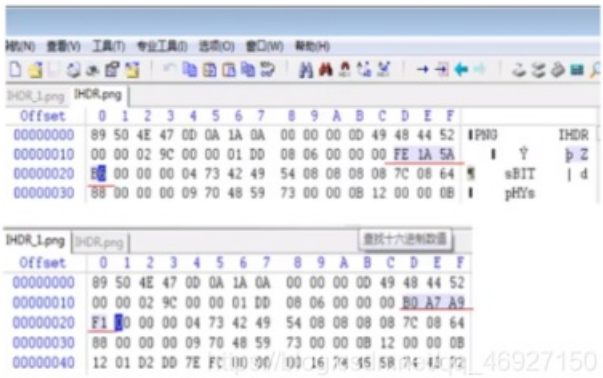
TweakPNG是一款简单易用的PNG图像浏览工具,它允许查看和修改一 些PNG图像文件的元信息存储。

使用场景:文件头正常却无法打开文件，利用TweakPNG修改CRC

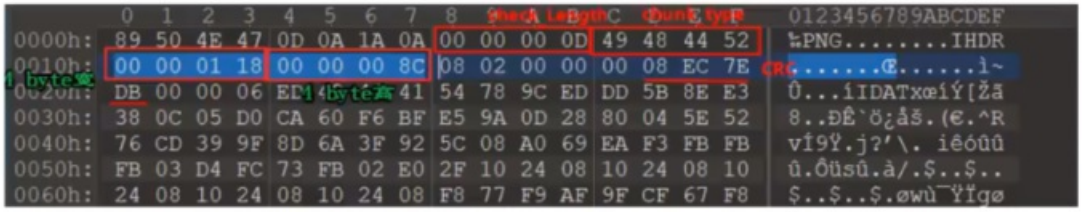
例:

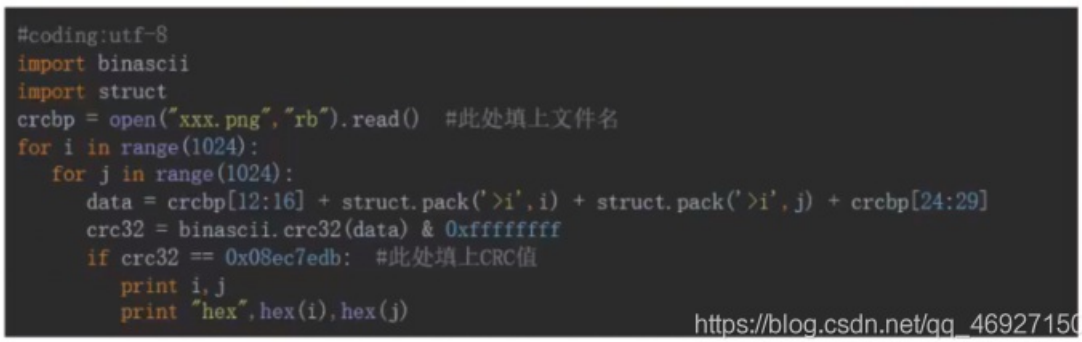
1.当PNG文件头正常但无法打开文件，可能是CRC校验出错，可以尝试通过TweakPNG打开PNG， 会弹出校验错误的提示，这里显示CRC是fe1a5ab6，正确的是b0a7a9f1。打开winhex搜索fe1a5ab6将其改为b0a7a9f1。





有时CRC没有错误，但是图片的高度或者宽度发生了错误，需要通过CRC计算出正确的高度或者宽度。





6. Bftools

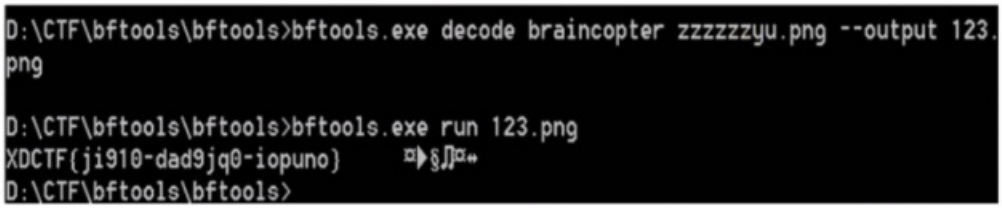
   bftools用于解密图片信息。

   使用场景:在windows的cmd下， 对加密过的图片文件进行解密

   格式:

   Bftools. exe decode braincopter要解密的图片名称-output输出文件名

   Bftools.exerun.上一步输出的文件



7.SilentEye

silenteye是一款 可以将文字或者文件隐藏到图片的解密工具。

使用场景: windows下打开silentEye工具，对加密的图片进行解密

例:

1.使用silentEye程序打开目标图片，点击image->decode，点击decode，可以查看隐藏文件，点击保存即可

2.如果需要密码，勾选encrypted data,输入密码和确认密码，点击decode再解密

四、JPG图像加密

1.Stegdetect工具探测加密方式

> Stegdetect程序主要用于分析PEG.文件。因此用Stegdetect 可以检测到通过Steg.
> JPHide. OutGuess. Invisible Secrets. F5. appendX
> 和Camouflage等这些隐写工具隐藏的信息。

格式：

stegdetect xx.jpg

stegdetect -s敏感度xx.jpgexi

2.phide

> Jphide是基于最低有效位LSB的JPEG格式图像隐写算法.

例:

Stegdetect提示jphide加密时，可以用Jphs. 工具进行解密，打开jphswin.exe, 使用open jpeg打开图片，点击seek,输入密码和确认密码，在弹出文件框中选择要保存的解密文件位置即可，结果保存成txt文件。

3.Outguess

outguess一般用于解密文件信息。

使用场景: Stegdetect识别出来或者题目提示是outguess加密的图片

该工具需编译使用: ./configure && make && make install

格式: outguess-r 要解密的文件名输出结果文件名

4.F5

F5一般用于解密文件信息。

使用场景: Stegdetect识别出来 是F5加密的图片或题目提示是F5加密的图片

进入F5-steganography_ F5目录，将图片文件拷贝至该目录下，从CMD进入该目录

格式: Java Exrtact要解密的文件名-p密码

运行结束后我们可以直接在目录下的output.txt中看到结果。

五、二维码处理

1.使用二维码扫描工具CQR.exe打开图片,找到内容字段

2.如果二维码某个定位角被覆盖了，该工具有时候也可以自动识别，如果识别失败，需要使用PS或画图工具将另外几个角的定位符移动到相应的位置，补全二维码。

3.如果某个二维码的定位点中间是白色，可能被反色了，使用画图工具把颜色反色回来再扫描即可。