hgame_week1_misc_writeup

misc1

misc1处理非常简单，没什么可说的，我直接在图片的exif区域修改了几个字节，所以使用十六进制编辑器winhex\c32asm都可以看到，这里要提到一个图片分析的神器叫做Stegsolve

这里这个功能可以看到对文件不同信息块的整理，我在这里放了第一个flag，非常简单，就不多说了

misc2

事实上，如果在没接触到图片隐写之前，接触过的最多隐藏信息在在图片里的方式，应该是一

个叫做图种的东西，相信很多人都听说过。

分析信息之前，一般我们会判断文件的类型

```
lorexxar@icy:~/Documents/hgame$ file misc1.jpg
misc1.jpg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segme
nt length 16, baseline, precision 8, 664x586, frames 3
```

这里应该是在第一部就做的事情，因为misc里下载到的文件，很可能我们不知道是什么类型，所以我们需要通过file命令来判断

然后就要提到一个叫binwalk的工具，可以帮我们分析文件构成

```
lorexxar@icy:~/Documents/hgame$ binwalk misc2.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard  1.01
45486         0xB1AE          gzip compressed data, from Unix, last modified: Su
n Jan 15 16:19:26 2017
45633         0xB241          PNG image, 1500 x 1072, 8-bit/color RGB, non-inter
laced
45674         0xB26A          Zlib compressed data, default compression, uncompr
essed size >= 229376

lorexxar@icy:~/Documents/hgame$
```

看到有东西，就说明有问题，因为图片中是不会存在另一张图的。

这里就要提到一些东西了，几乎看所有的wp中，分割图片都是用了dd命令，我不知道是不是看了这篇文章

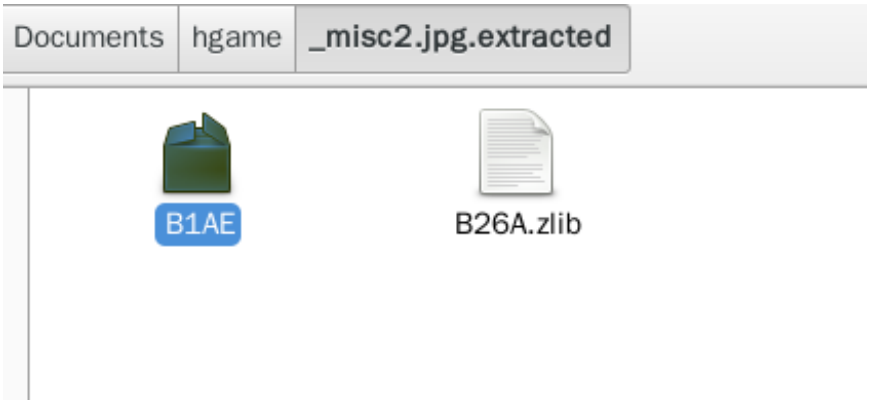
http://www.tuicool.com/articles/VviyAfY

但我想肯定有py行为，因为有起码2~3种方式比dd简单，这里不多提了，我这里说两种

1、既然binwalk可以分析，为什么不能分割呢，答案是可以

```
lorexxar@icy:~/Documents/hgame$ binwalk -e misc2.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard  1.01
45486         0xB1AE          gzip compressed data, from Unix, last modified: Su
n Jan 15 16:19:26 2017
45633         0xB241          PNG image, 1500 x 1072, 8-bit/color RGB, non-inter
laced
45674         0xB26A          Zlib compressed data, default compression, uncompr
essed size >= 229376
```



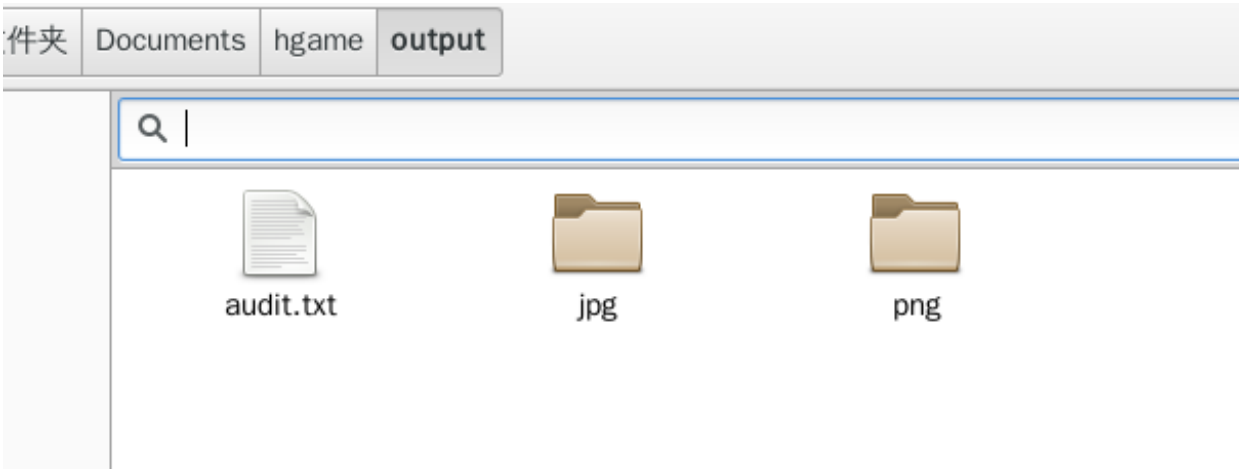
左边这个就是上面的gzip信息，但是因为这个压缩包不完整，所以在linux没办法直接打开，你可以修复或者选择在windows下打开，就可以看到第二个flag

misc3

这里提到第二种方式，因为你看到了，有张图片没有被分割出来

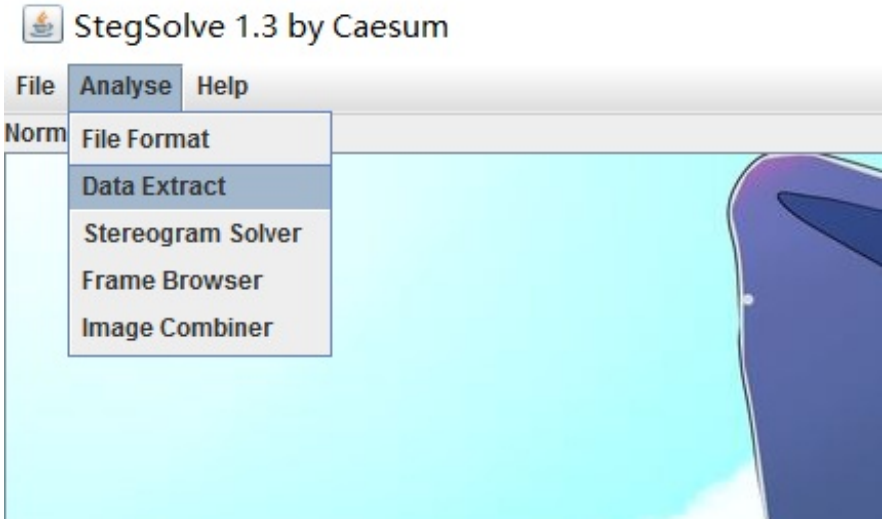
有个好用的工具叫做foremost

```
lorexxar@icy:~/Documents/hgame$ foremost misc2.jpg
Processing: misc2.jpg
|*|
```

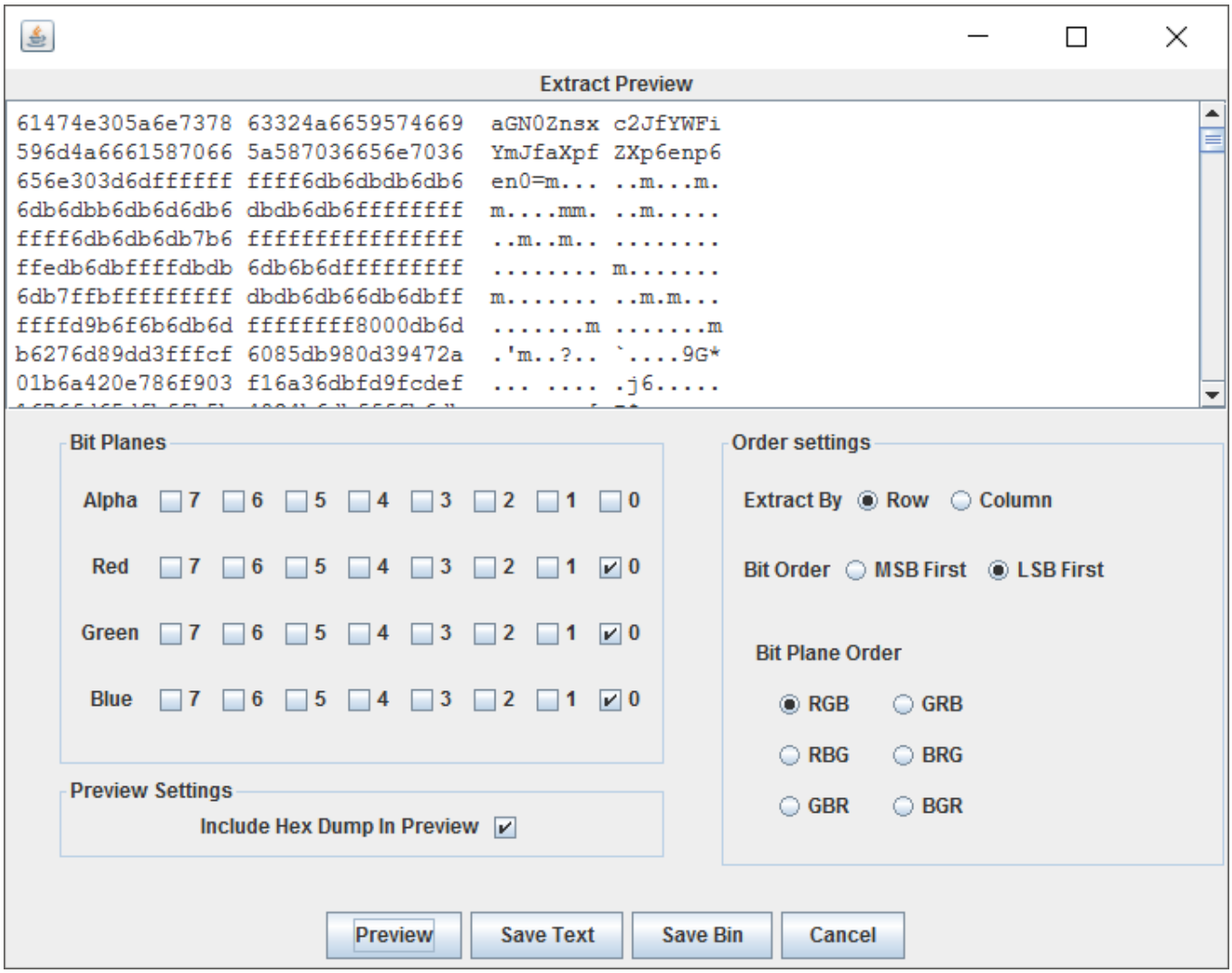


这里我们得到了下一张图

回到神器，用第二个功能



最简单的LSB是指把信息存放在图片每个像素点的最低位中，所以勾选0通道



我们看到了base64编码过的flag

但是并不是什么时候我们都有运气使用工具，所以这里我贴上lsb的解密脚本

```
# coding: utf-8
from PIL import Image

im = Image.open('flag.png')


width = im.size[0]
height = im.size[1]

a = ""
aa = ""

for y in xrange(height):
    for x in xrange(width):

        pixel = im.getpixel((x, y))

        for i in xrange(3):
            aa += str(pixel[i]%2)

for i in xrange(len(aa)):
    try:
        a += chr(int(aa[i*8:i*8+8],2))
    except:
        break

fflag = open("test.txt","w")

fflag.write(a)
fflag.close()
```

代码有一点儿问题，就不修了