

# CTF一些隐写题

原创

[Sandra\\_93](#)  于 2018-09-25 10:44:55 发布  1968  收藏 2

分类专栏: [CTF](#) 文章标签: [CTF\\_隐写术部分](#)

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/Sandra\\_93/article/details/82835700](https://blog.csdn.net/Sandra_93/article/details/82835700)

版权



[CTF 专栏收录该内容](#)

9 篇文章 0 订阅

订阅专栏

之前专攻隐写术时写过一些writeup, 留在这里吧。(下面的黑体是题目名字吧)

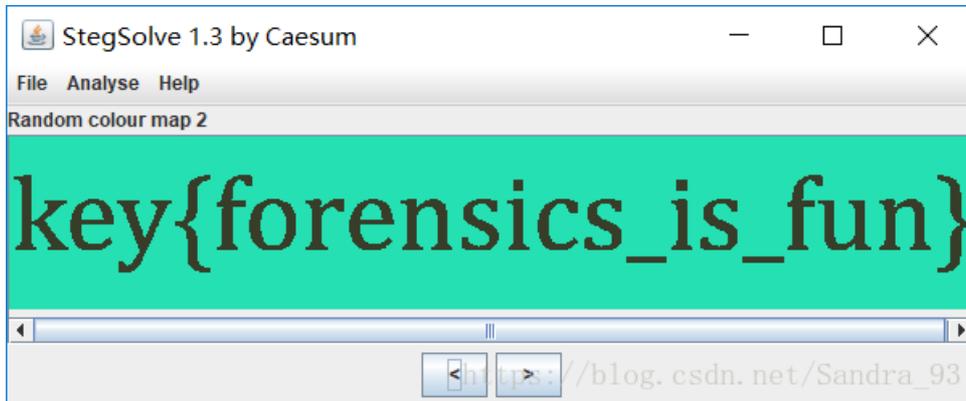
(参考别人的writeup, 以及自己做的)

## SB! SB! SB! (神器 Stegsolve)

拿到图片，使用Stegsolve.jar试试，左右改变，得到二维码的话，可以使用工具CQR.exe 进行解码

## so beautiful so white (神器 Stegsolve)

把压缩包解压，得到一张白色图片和一个压缩包，讲白色图片放到Stegsolve.jar，左右点击，得到压缩包密码



进入压缩包，得到gif动图，到WinHex里打开，再打开一张正常的动图，发现文件头缺失，补充文件头，得到动图a.gif(后面看攻略的)

将动图用Stegsolve.jar打开，然后Analyse-Frame Browser就可以一帧一帧看动图啦

## 女神又和大家见面了(隐藏文件)

拿到一张图片，如果属性，发现图片很大，说明里面可能有压缩包，在虚拟机里打开图片，在终端里运行 `cd /root/桌面`，进入桌面 然后 `binwalk xx.jpg` 得到图片，发现有zip 可以

```
binwalk -e xx.jpg
```

导出压缩包（或者 `foremost xx.jpg -o xx` 导出包）

如果发现包里有音频和一个文本，文本有类似密码的东西，可以考虑用MP3Stego，使用方法：打开终端，输入d: 进行换盘，

然后找到位置，我的是如下，其中，-X后要打开的

文件，注意，文件要拖到Decode.exe同目录下，-P就是密码，输入回车后，到所在目录下，发现新生产一个txt

```
C:\WINDOWS\system32\cmd.exe
C:\>d:
D:\vs code\CTF工具\mp3stego\MP3Stego_1_1_18\MP3Stego>Decode.exe -X music.mp3 -P simctf
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = 'music.mp3' output file = 'music.mp3.pcm'
Will attempt to extract hidden information. Output: music.mp3.txt
the bit stream file music.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=stereo, sblim=32, jsbd=32, ch=2
[Frame 3416]Avg slots/frame = 417.837; b/smp = 2.90; br = 127.963 kbps
Decoding of "music.mp3" is finished
The decoded PCM output file name is "music.mp3.pcm"
D:\vs code\CTF工具\mp3stego\MP3Stego_1_1_18\MP3Stego>
```

[https://blog.csdn.net/Sandra\\_93](https://blog.csdn.net/Sandra_93)

~~欢迎来到地狱（这个看writeup这么简单，可能没做完）

拿到一张图片，可以到WinHex里打开，再打开一张同样后缀名的文件，对比文件头，该添添选中之后，Edit-Copy All-Normal复制，Edit-Clipboard Data-paste粘贴

Wav音件可以考虑用Audacity打开，看看是不是摩斯电码 桌面~~

\*\*

## 将一个文件写进另一个

\*\*

命令：

`copy /b xxx.jpg+xx.zip xxxxx.jpg` 这样可以得到将xx.jpg写入xxx.jpg里的名为xxxxx.jpg的文件，文件不一定为jpg和zip这里只是举个栗子

---