

# BUUCTF 九连环

原创

Bnessy 于 2022-03-25 11:21:23 发布 22 收藏

分类专栏: CTF 文章标签: 安全 web安全 信息安全

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 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/weixin\\_44895005/article/details/123731116](https://blog.csdn.net/weixin_44895005/article/details/123731116)

版权



[CTF 专栏收录该内容](#)

19 篇文章 0 订阅

订阅专栏

题目 解题快手榜

## 九连环

1

注意: 得到的 flag 请包上 flag{} 提交

389a0c11-d...

Flag

提交

CSDN@Bnessy

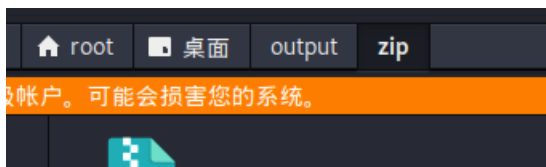
使用biwnalk分析, 发现图片中有压缩包

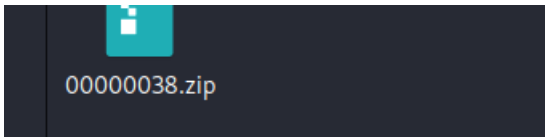
```
(root@kali)~[~/桌面]
# binwalk 123456cry.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
19560	0x4C68	Zip archive data, at least v1.0 to extract, name: asd/
48454	0xBD46	Zip archive data, at least v1.0 to extract, compressed size: 184, uncompressed size: 184, name: asd/qwe.zip
48657	0xBE11	End of Zip archive, footer length: 22
48962	0xBF42	End of Zip archive, footer length: 22

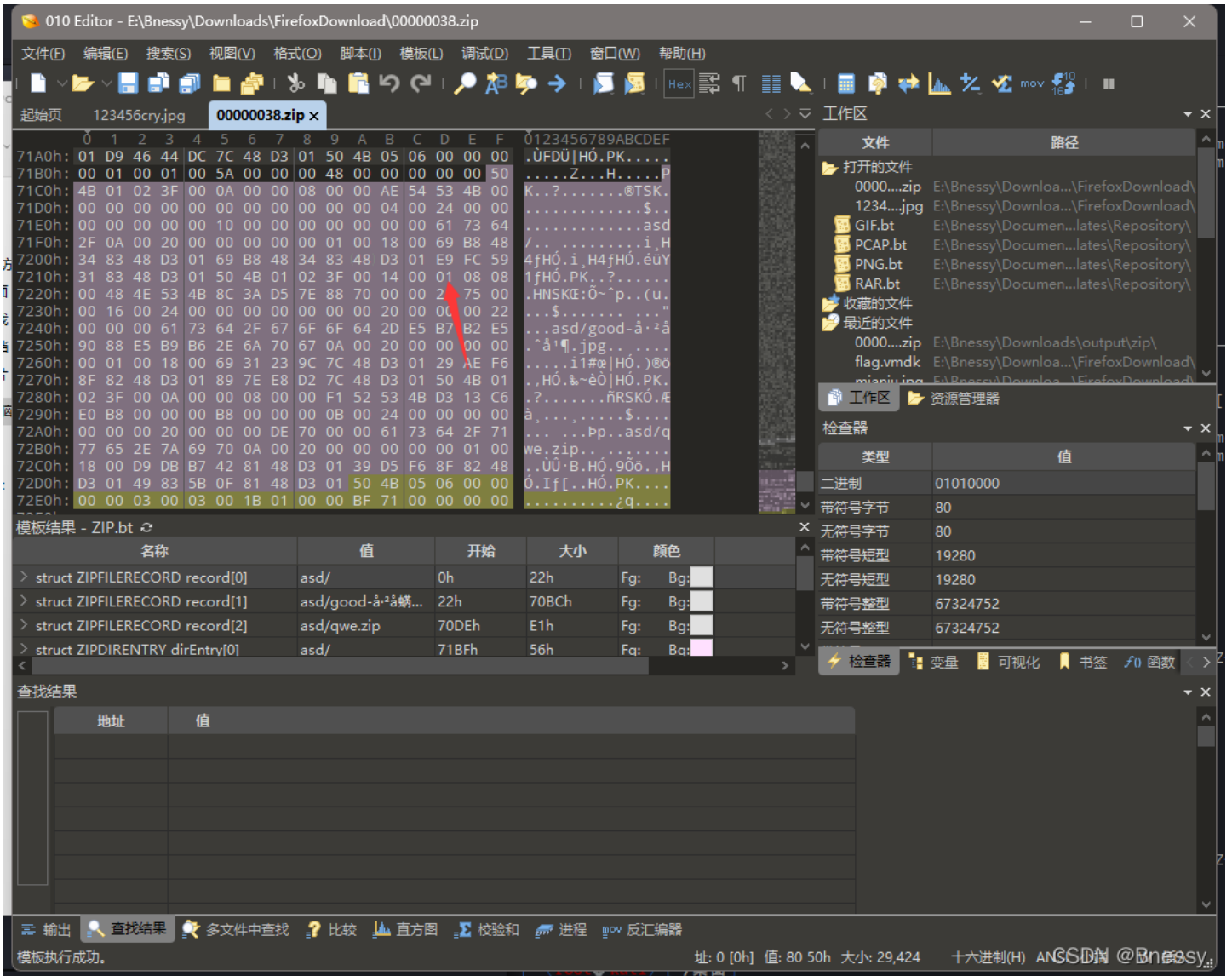
使用foremost进行分离, 得到一个压缩包

```
(root@kali)~[~/桌面]
# foremost 123456cry.jpg
```





有密码，使用010打开分析之后发下是伪加密



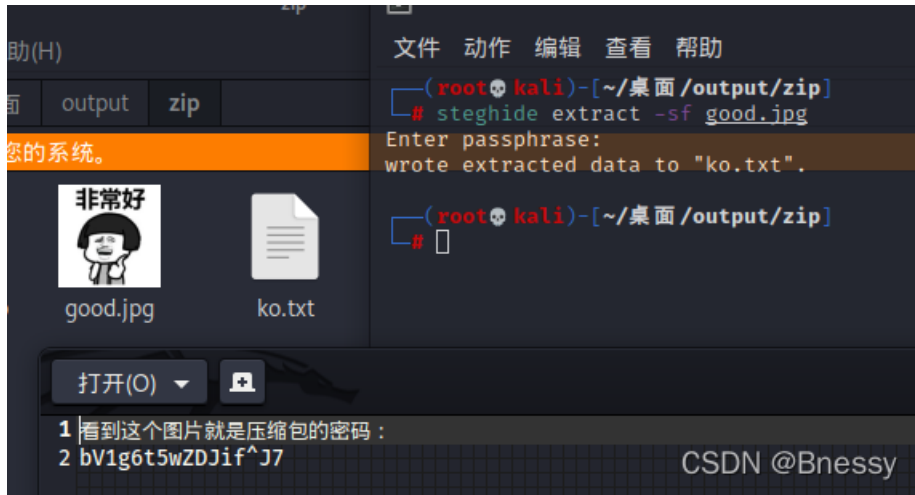
将01改为00就能进行解压了，有一张图片和一个加密的压缩包

# 非常好



CSDN @Bnessy

密码应该在图片中，使用 `steghide extract -sf good.jpg` 将图片中的文件分离出来，得到解压密码



flag{1RTo8w@&4nK@z\*XL}