BUUCTF：九连环

原创

末 初 于 2020-09-23 15:03:06 发布 2079 收藏 3

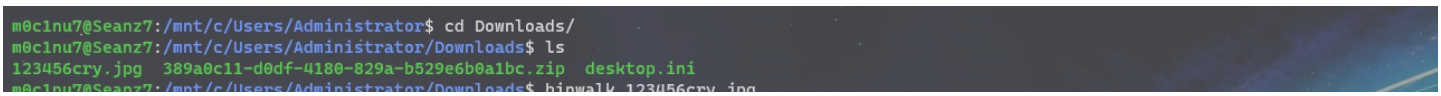
分类专栏： CTF_MISC_Writeup

本文链接：https://blog.csdn.net/mochu7777777/article/details/108752016

题目地址：https://buuoj.cn/challenges#%E4%B9%9D%E8%BF%9E%E7%8E%AF

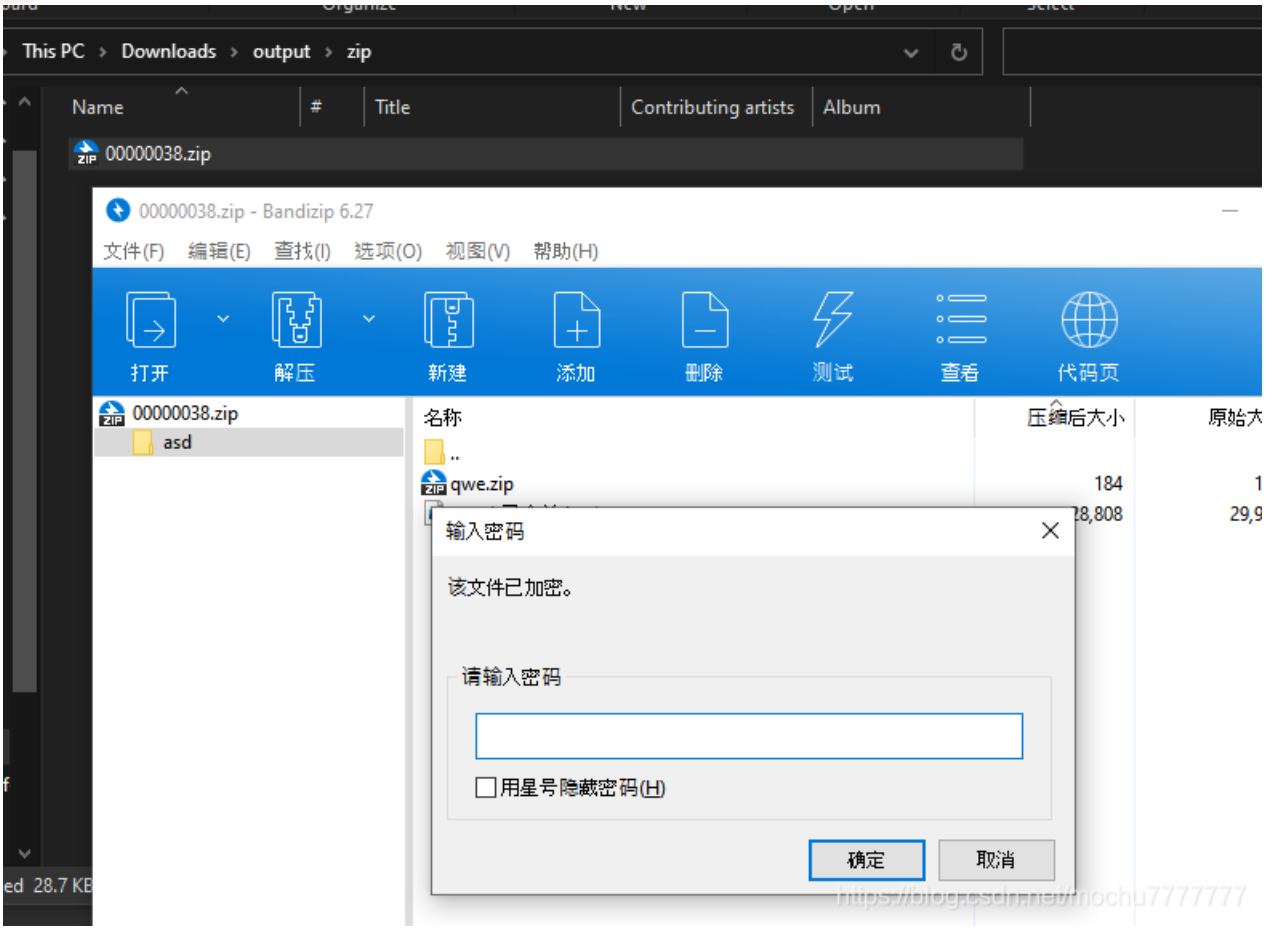
题目如下：

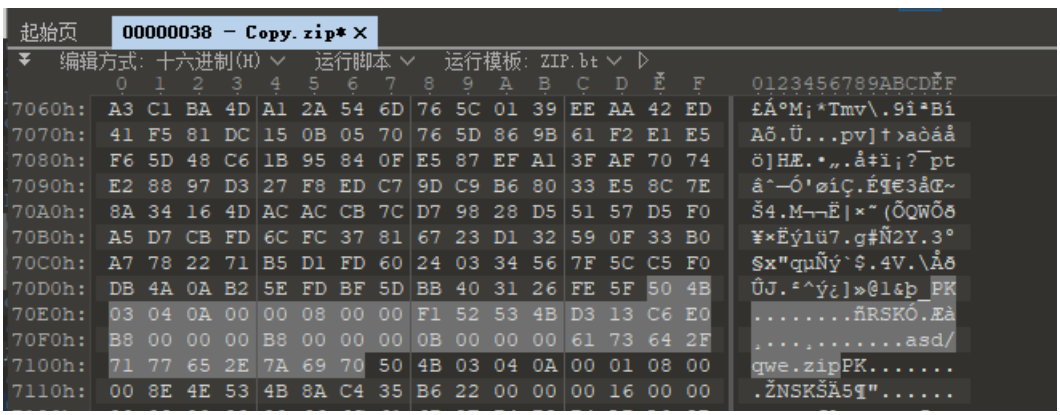
`binwalk` 分析， `foremost` 分离

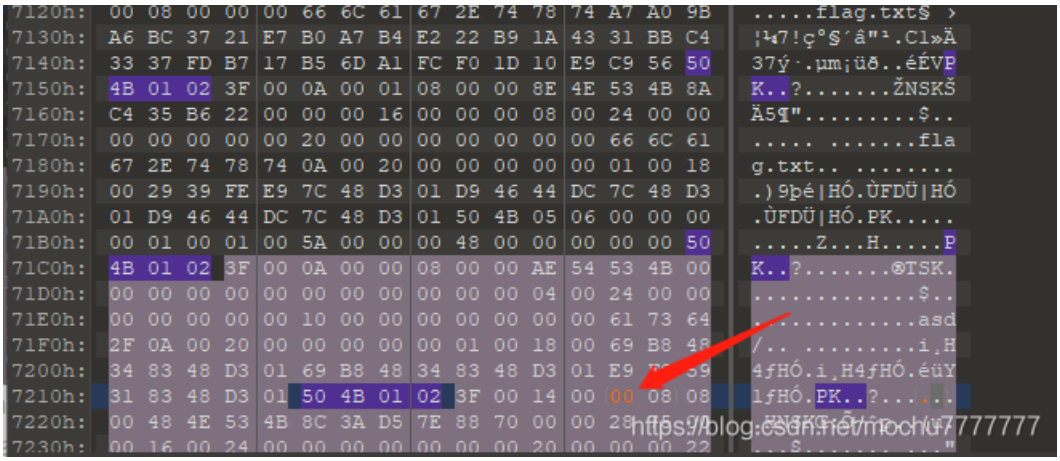


```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
19560         0x4C68          Zip archive data, at least v1.0 to extract, name: asd/
48454         0xBD46          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

m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads$ foremost 123456cry.jpg
Processing: 123456cry.jpg
|foundat=asd/PK□□□
foundat=asd/good-已合并.jpg◆◆    <◆a◆6◆◆◆◆◆wF□
ſf◆lI*!◆T◆□R◆M◆◆◆[◆◆LQI◆◆B◆>◆"Kvf!}◆2nf◆O◆◆}◆◆{◆◆}◆◆◆◆◆◆3◆◆u_◆u◆◆q□◆u◆◆◆1◆◆◆□.Z◆X◆XX@ □◆/◆1□:◆◆◆◆◆ↄN◆◆◆◆◆h      r◆◆◆◆◆◆□□□da□dat◆ ◆q◆◆□□
foundat=asd/qwe.zipPK□□

*|
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads$ ls
123456cry.jpg  389a0c11-d0df-4180-829a-b529e6b0a1bc.zip  desktop.ini  output
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads$
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads$ tree output/
output/
├── audit.txt
├── jpg
│   └── 00000000.jpg
└── zip
    └── 00000038.zip

2 directories, 3 files
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads$
```

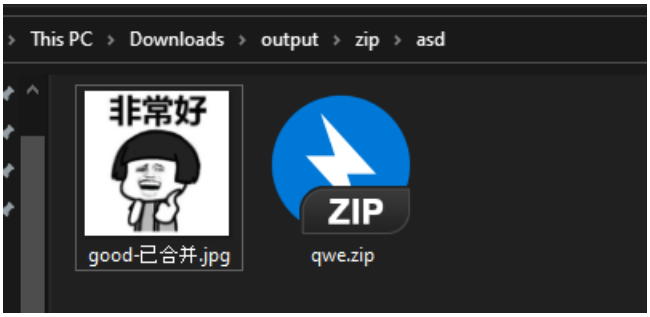

zip伪加密



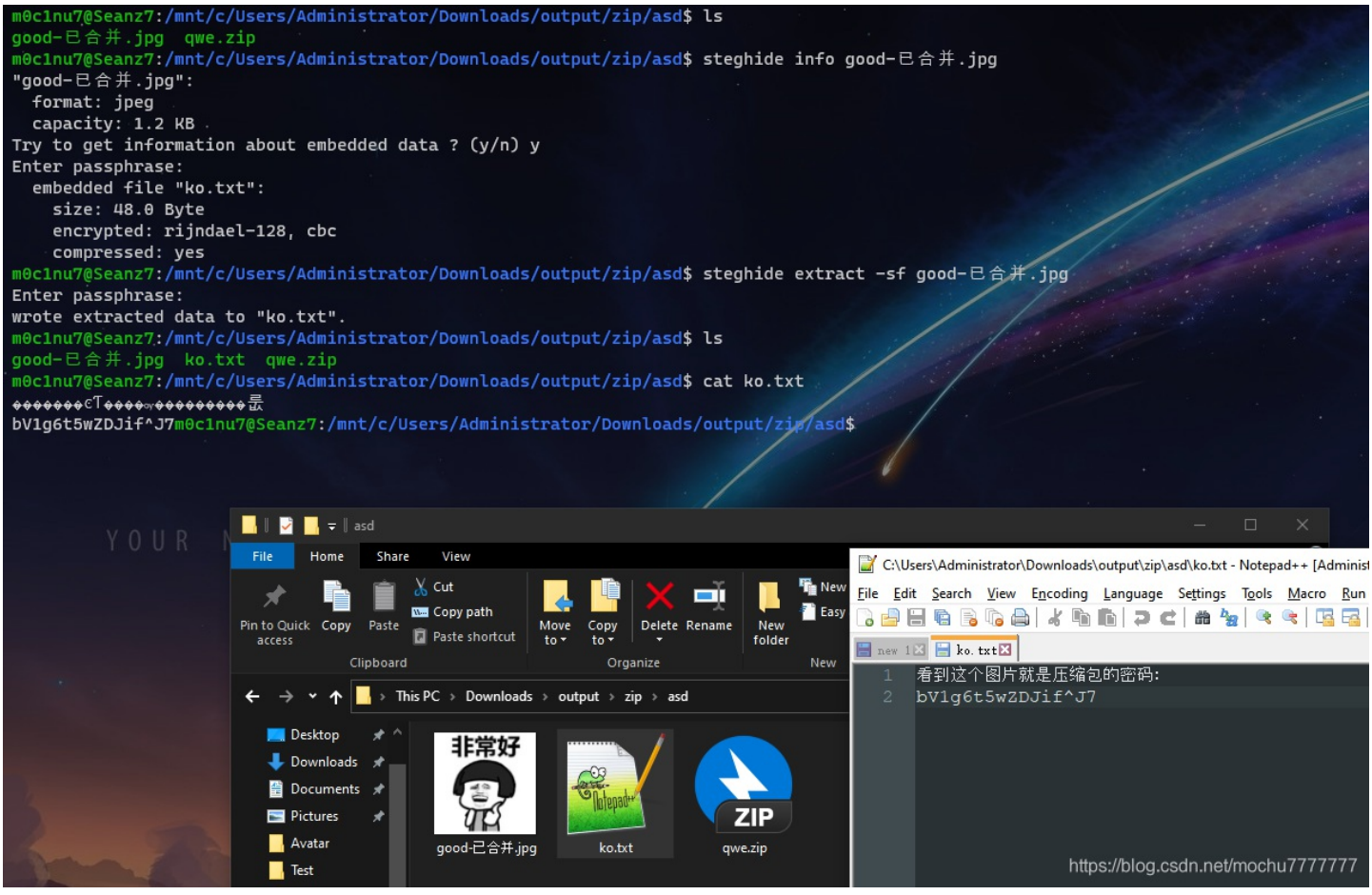




解压得到



使用`steghide`发现图片有隐写文件，使用`steghide extract -sf good.jpg`，空密码即可



使用解压密码解压`qwe.zip`即可得到flag

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