# 春秋杯2021-勇者山峰 helloshark

原创

A丶R 于 2021-11-28 22:27:03 发布 268 收藏

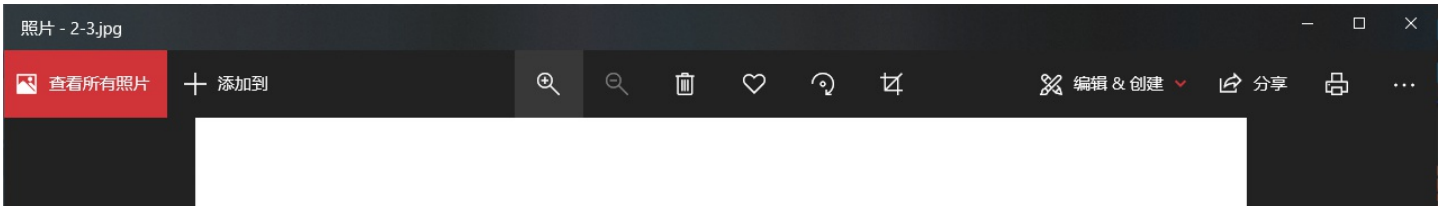
分类专栏： CTF-Misc 文章标签： web 网络安全 经验分享

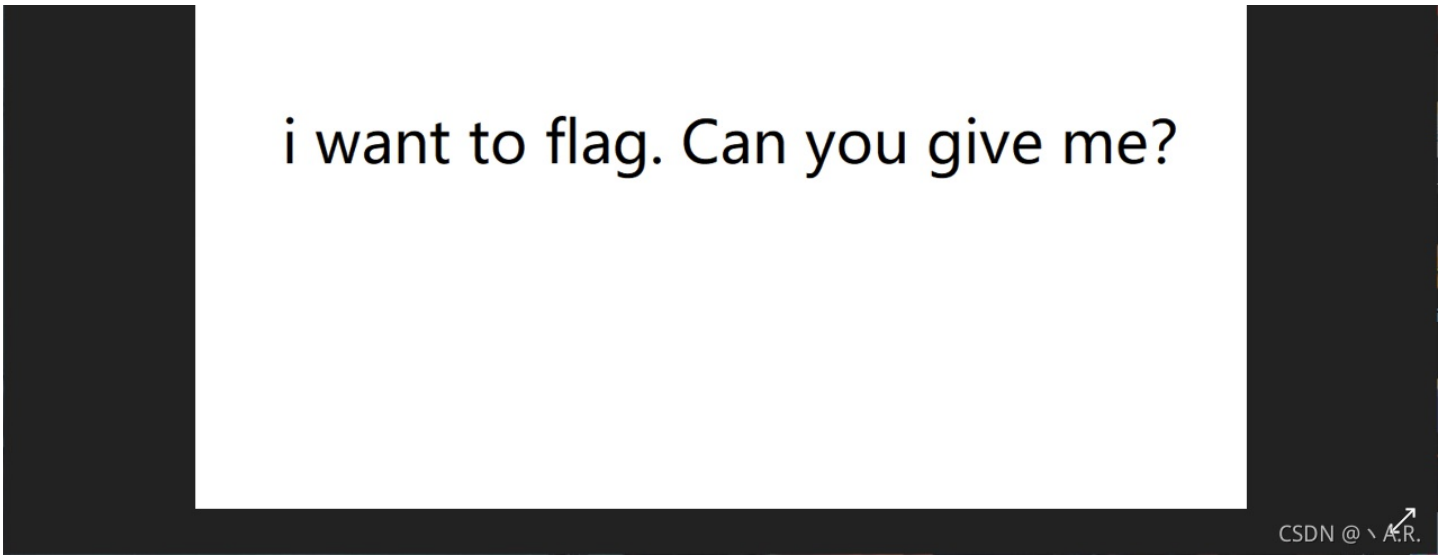


本文链接：https://blog.csdn.net/weixin_51804748/article/details/121599076

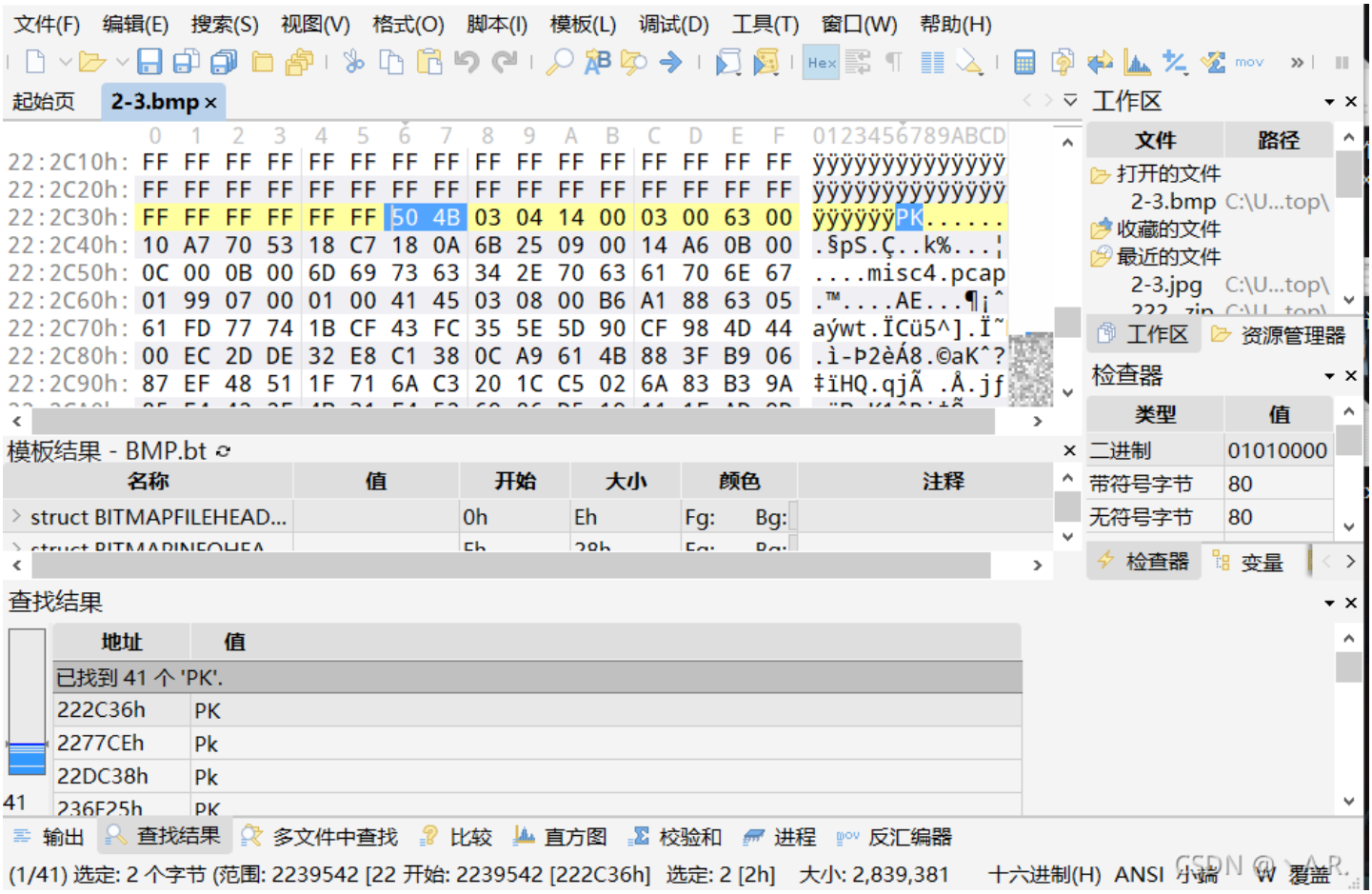



本题附件打开是一个bmp图片

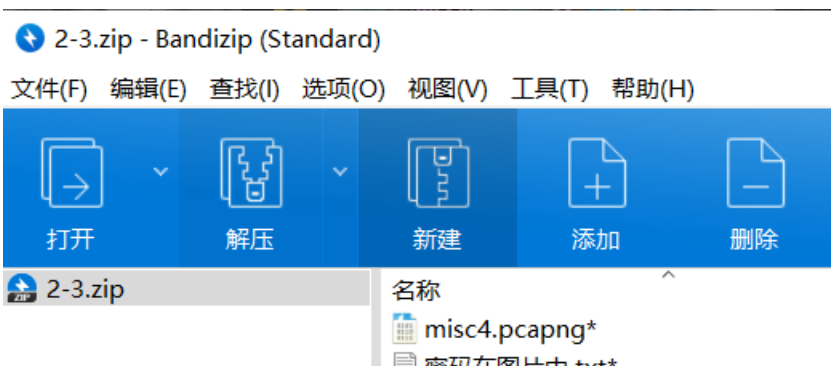





尝试用010查看该文件，搜索PK文本

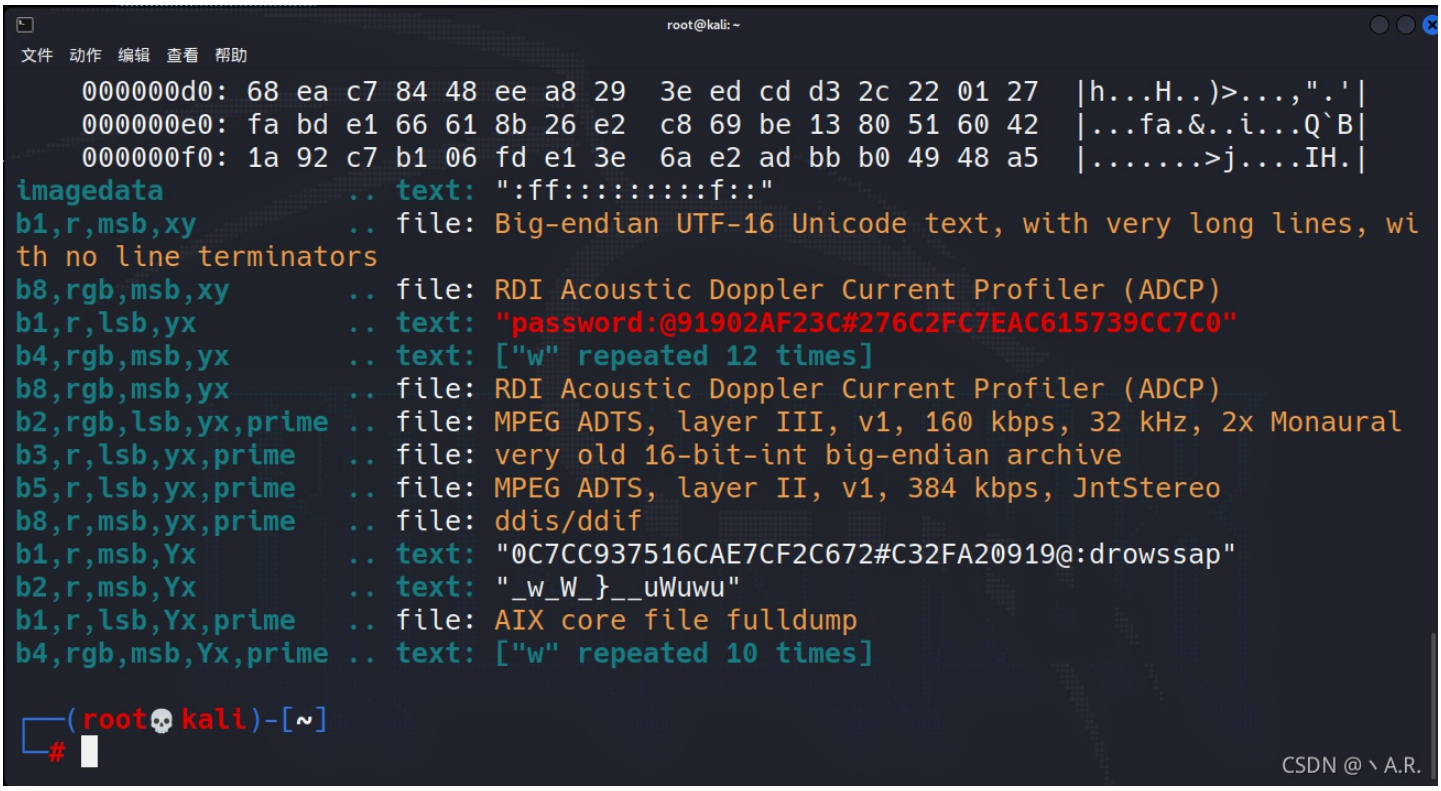



发现文件末尾隐藏了一个压缩包

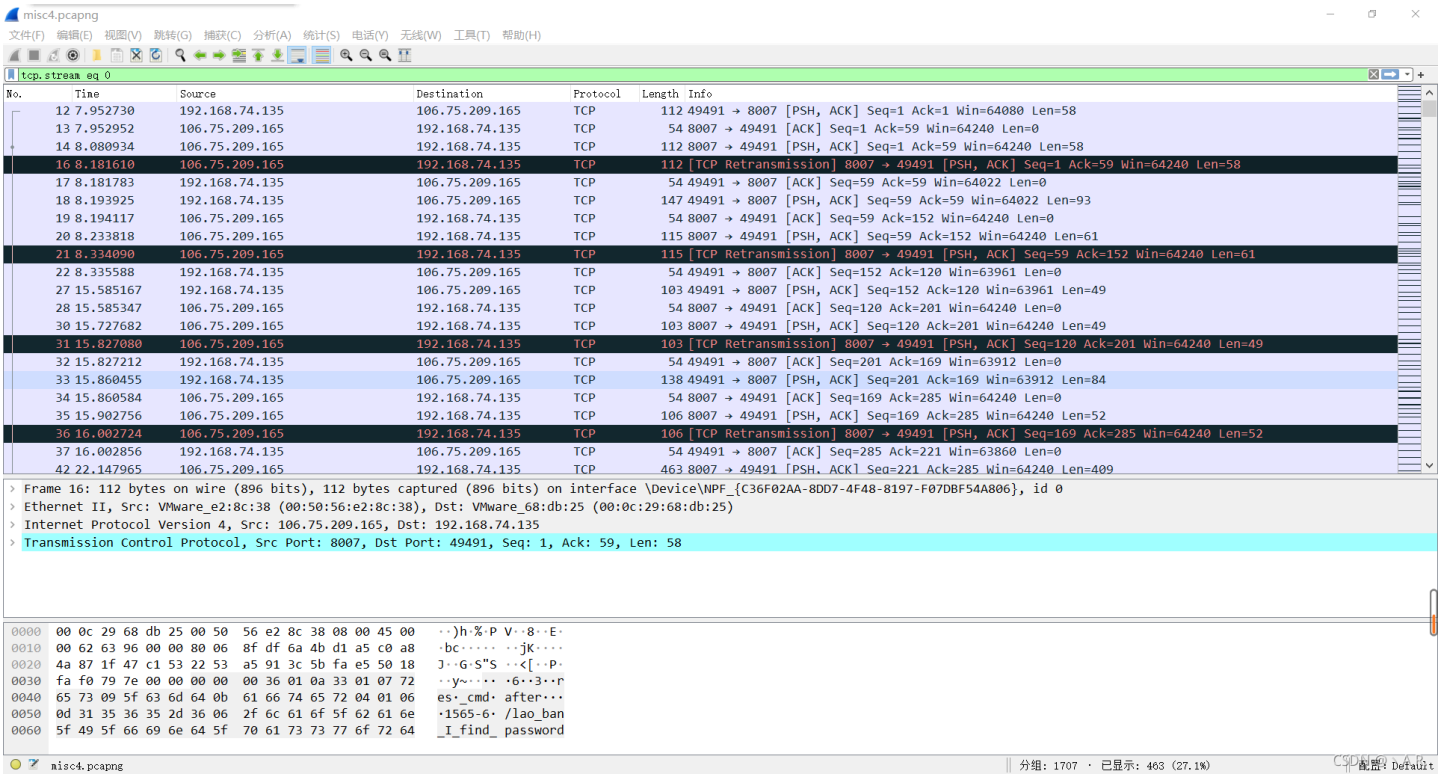


将后缀名改为zip后打开压缩包，发现有两个文件，但是解压需要密码，其中有提示说密码在图片中。
尝试各种工具来解析这个图片，最后可以用`zsteg`来得到压缩包密码

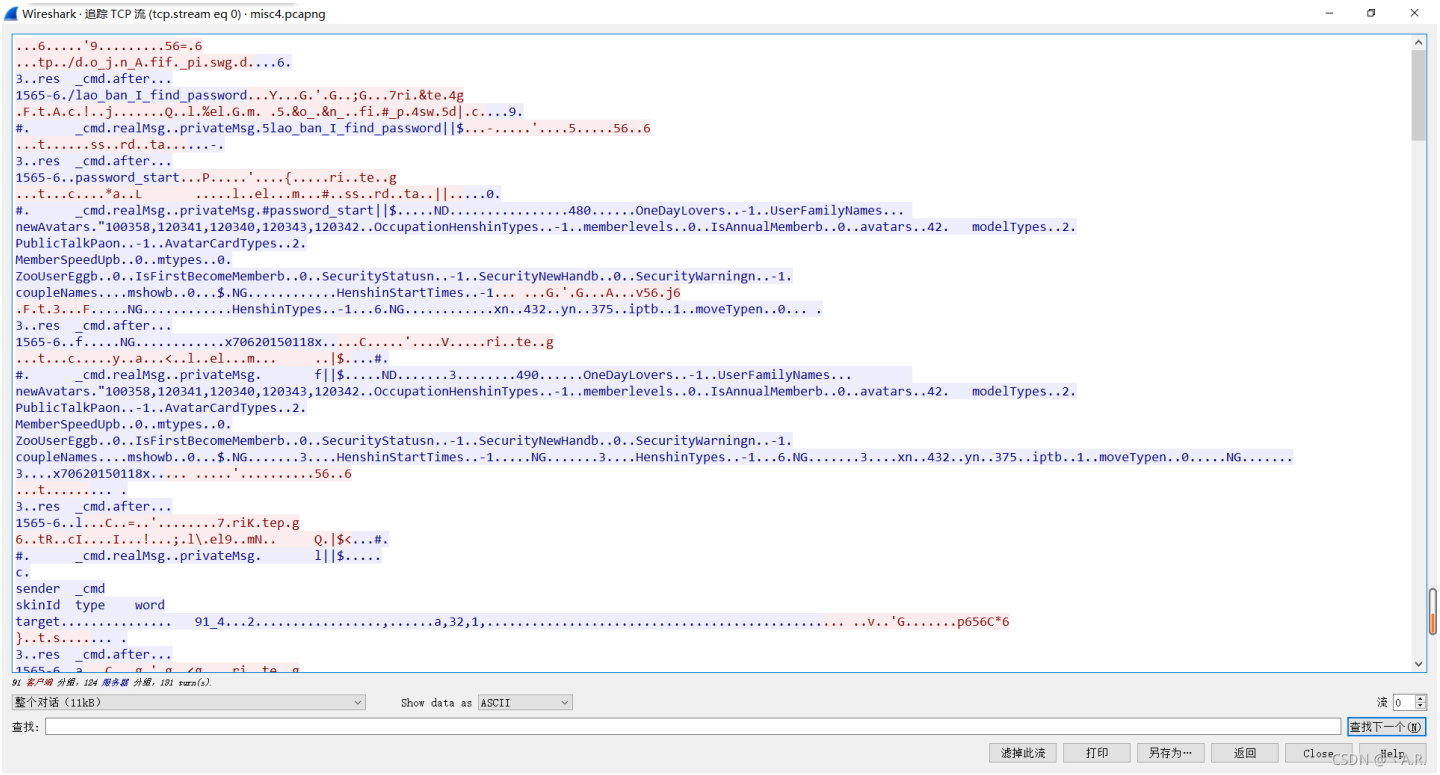
```
zsteg -a 文件名
```




用密码解压文件，用wireshark打开流量包



追踪tcp流得到疑似flag的字符串文本




写脚本跑出结果

```
import base64

flag=''
for line in open("ws.txt"):
    rs = line.replace('\n', '')
    if "cmd.realMsg..privateMsg" in rs:
        tmp=rs.split('||')
        flag+=tmp[0][-1]
    print(flag)
```