

20220215-CTF-MISC-BUUCTF-爱因斯坦-binwalk分析图片-dd命令分离ZIP文件--图片属性中寻找密码

原创

qq_51550750 于 2022-02-15 19:55:49 发布 1254 收藏 2

分类专栏: [CTF刷题](#) 文章标签: [ctf](#) [buuctf](#) [misc](#) [binwalk](#)

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/qq_51550750/article/details/122950683

版权



[CTF刷题](#) 专栏收录该内容

50 篇文章 1 订阅

订阅专栏

MISC-BUUCTF-爱因斯坦

爱因斯坦

5309 次解出
1 分

CSDN @qq_51550750

Challenge

Top 3 Solves



爱因斯坦

1

注意：得到的 flag 请包上 flag{} 提交

📄 dafbd663-3...

Flag

Submit

CSDN @qq_51550750

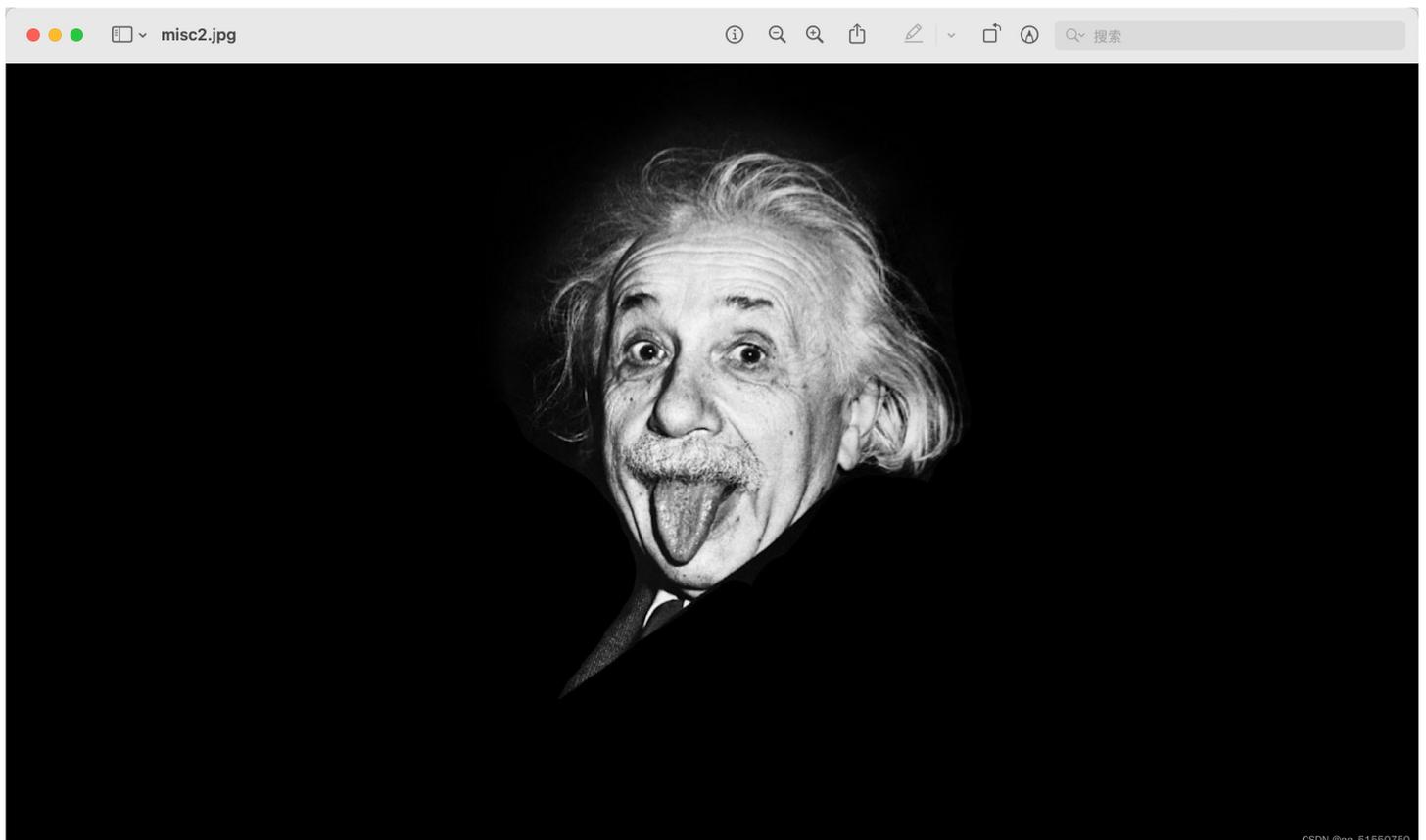
注意：得到的 flag 请包上 flag{} 提交

【1】下载附件，并解压，得到一张图片（misc2.jpg）：

📁 爱因斯坦

🖼️ misc2.jpg

📄 dafbd663-377c-4360-a086-01d685caa52b.zip



CSDN @qq_51550750

【2】binwalk分析:

```
(kali㉿kali)-[~]
└─$ binwalk /home/kali/Desktop/misc2.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
30	0x1E	TIFF image data, big-endian, offset of first image directory: 8
68019	0x109B3	Zip archive data, encrypted at least v1.0 to extract, compressed size: 51, uncompressed size: 39, name: flag.txt
68230	0x10A86	End of Zip archive, footer length: 22

CSDN @qq_51550750

显示里面有一个ZIP压缩包

【3】使用dd命令分离该压缩包:

dd命令格式:

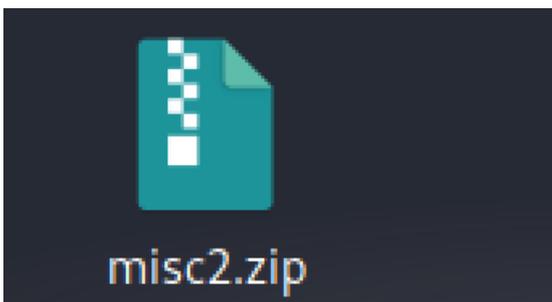
```
dd if=图片名 of=ZIP压缩包的名称（自己命名） skip=偏移量（本题是68019） bs=1
```

```
(kali㉿kali)-[~]
└─$ dd if=/home/kali/Desktop/misc2.jpg of=misc2.zip skip=68019 bs=1
233+0 records in
233+0 records out
233 bytes copied, 0.000892315 s, 261 kB/s
```

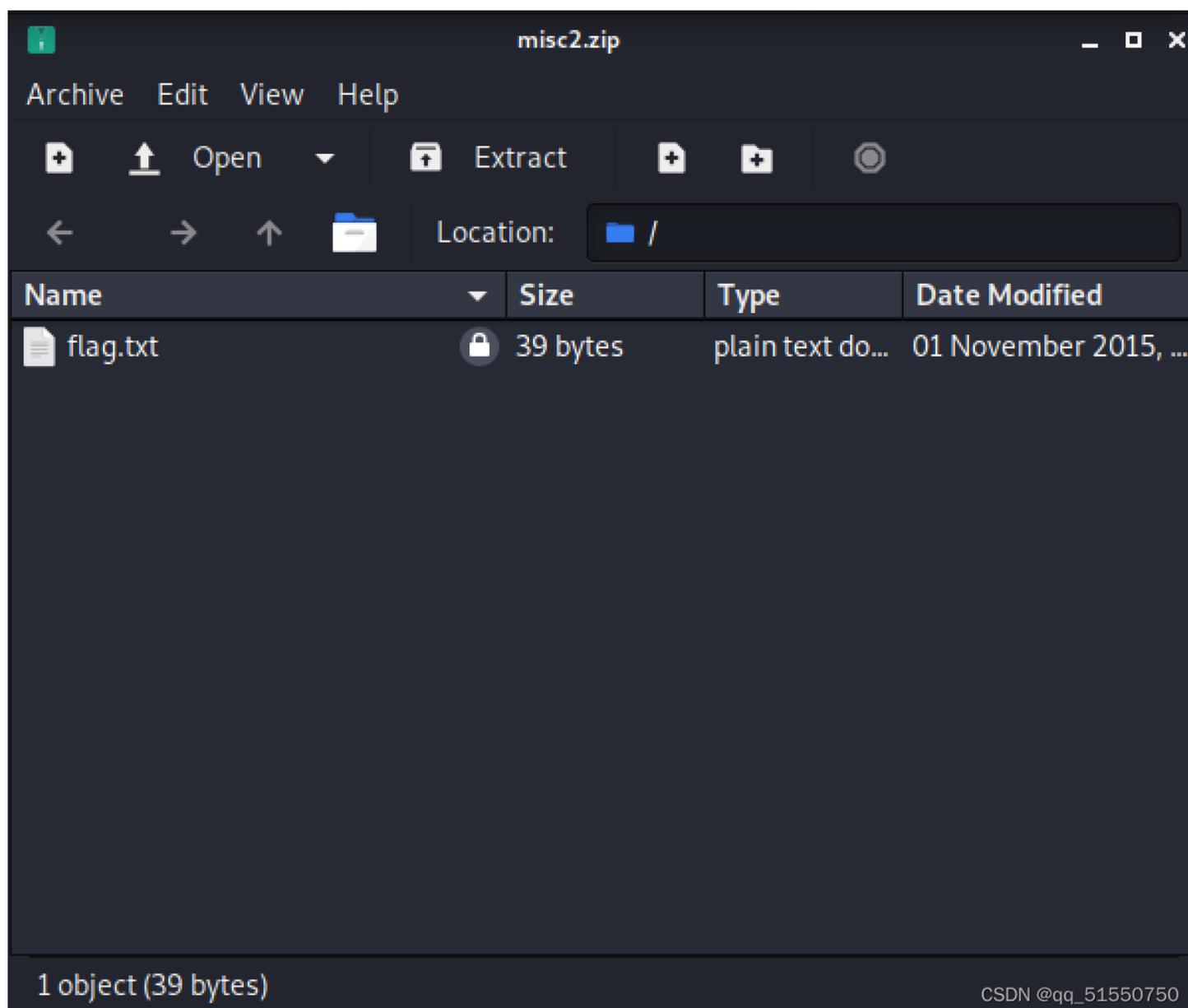
```
(kali㉿kali)-[~]
└─$
```

CSDN @qq_51550750

分离成功:

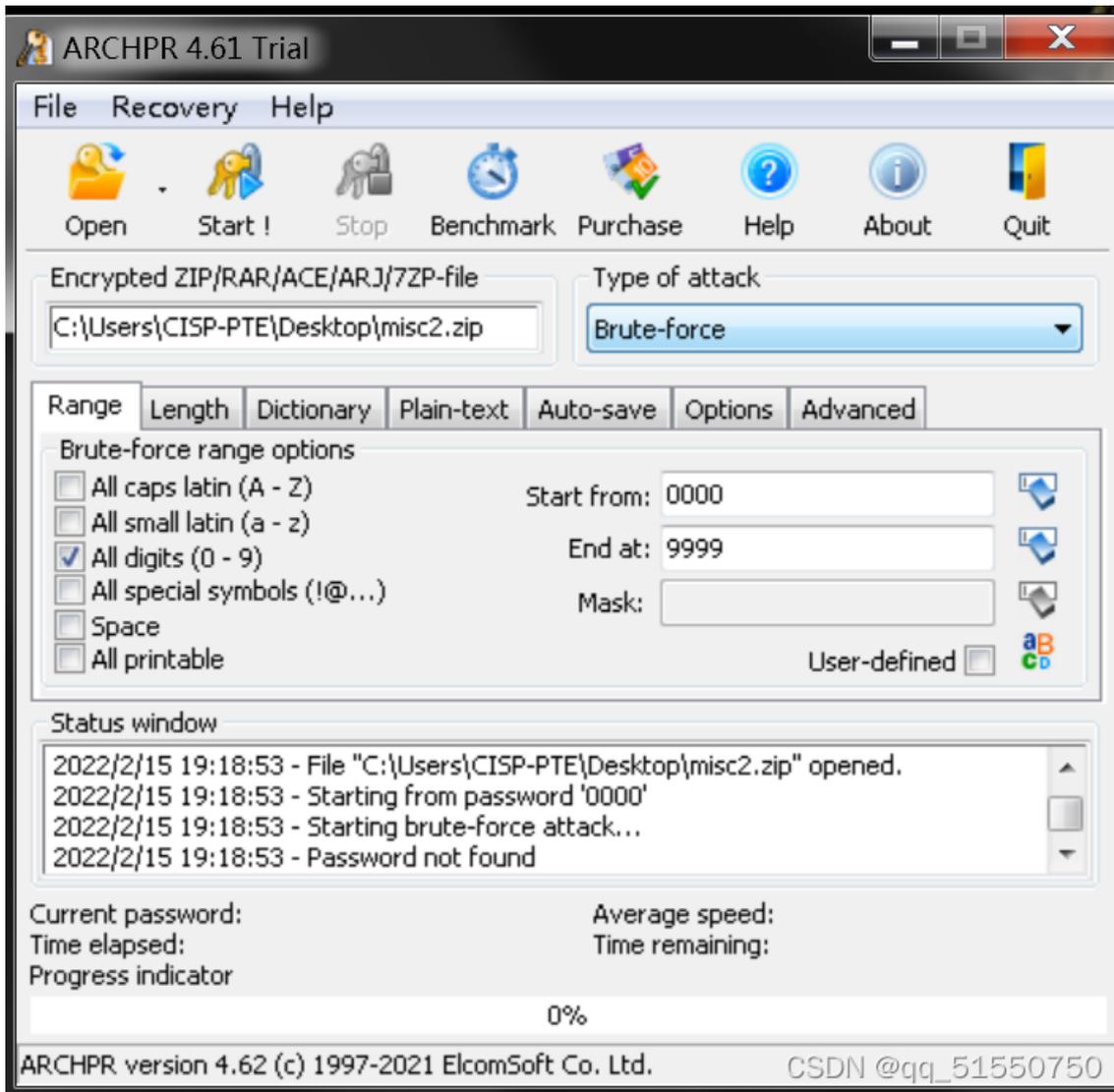


打开:



flag.txt上锁了

【4】ARCHPR尝试暴力破解:

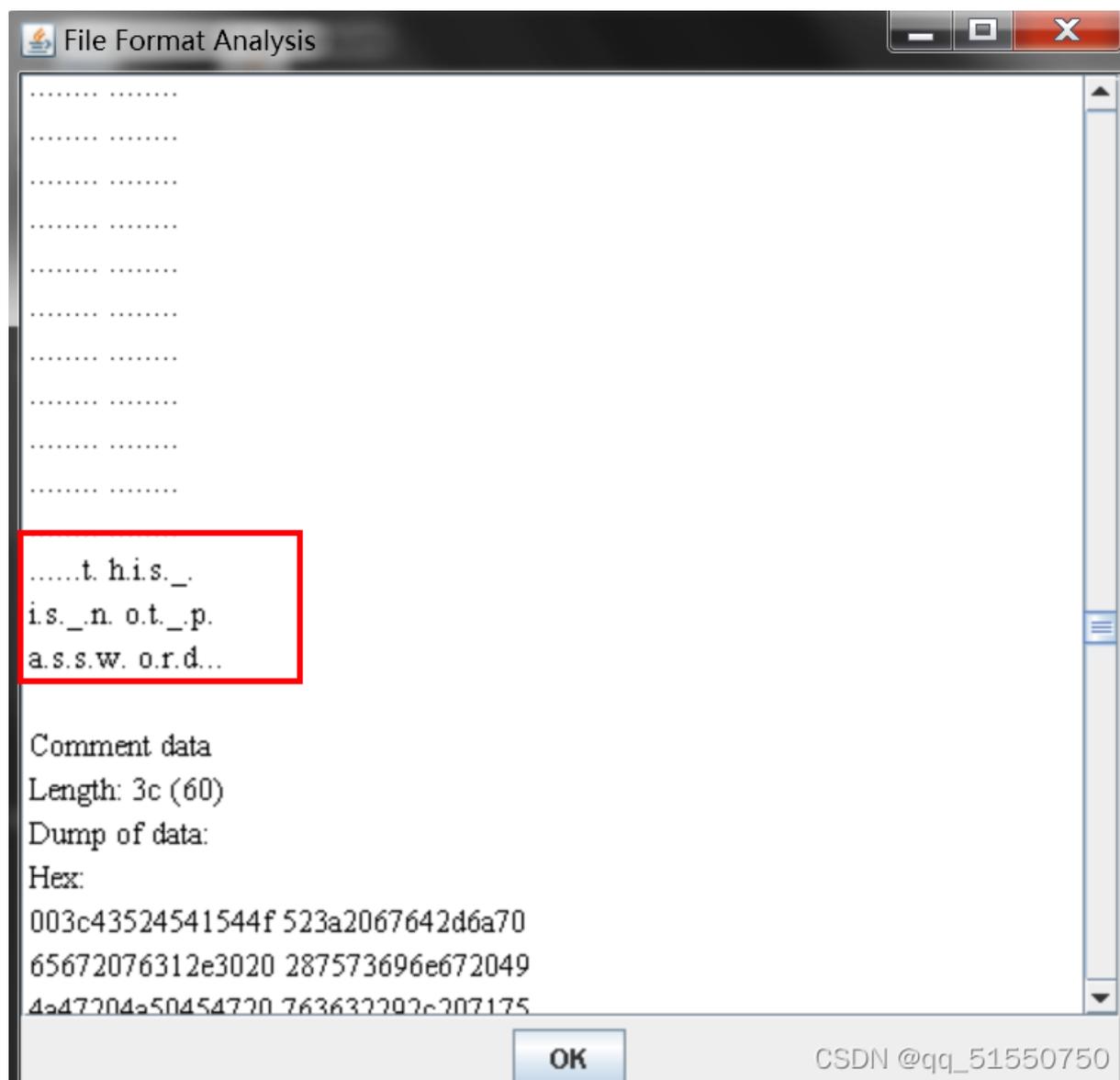


首先尝试了四位，无法破解:



题目也没有提示密码的信息，猜测不是采用破解的方法，需要再分析一下图片

【5】stegsolve分析图片（File Format）



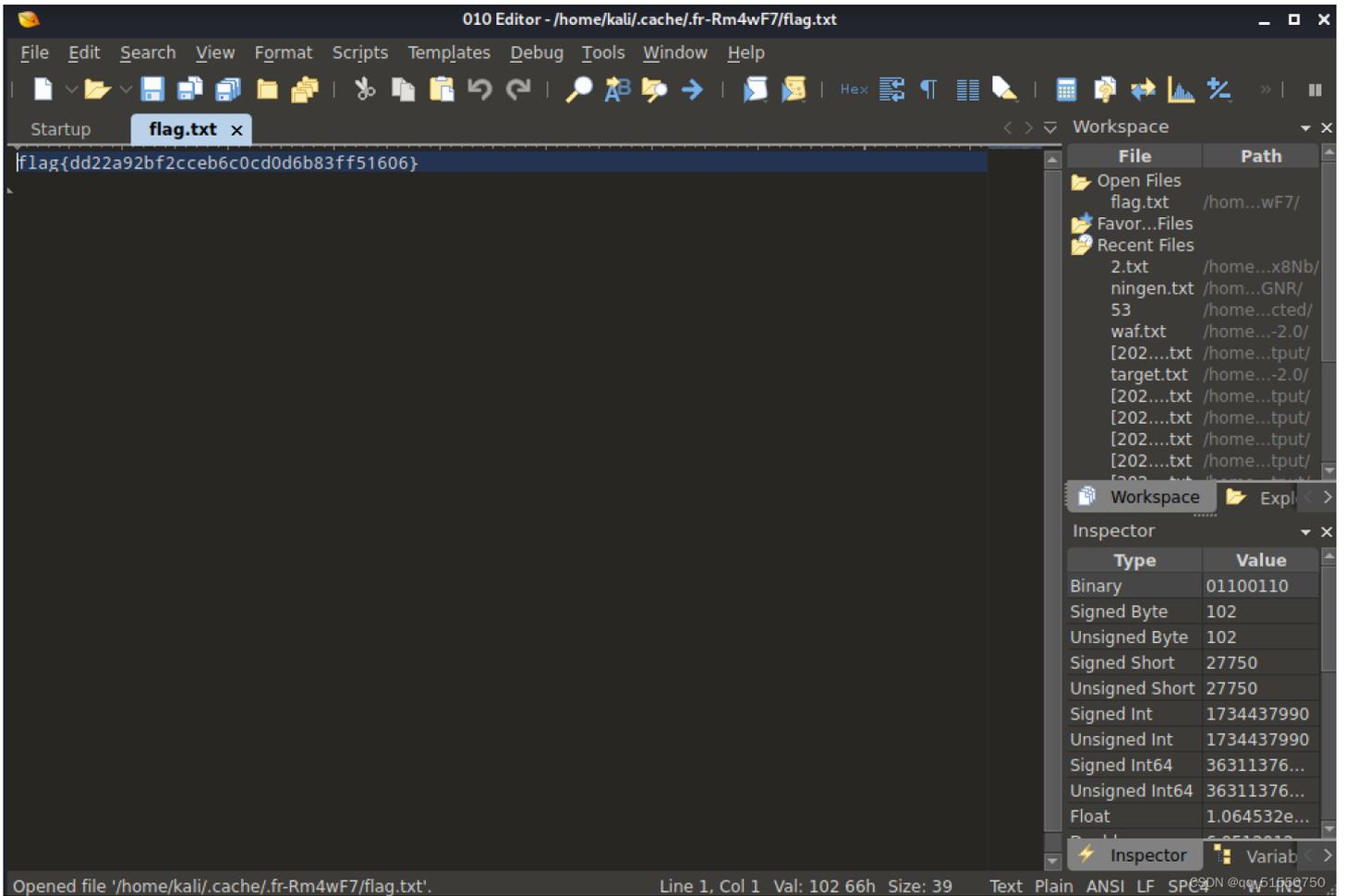
查看图片属性：





难道密码就是this_is_not_password ???

尝试发现密码就是this_is_not_password



成功打开flag.txt

【5】得到flag

flag{dd22a92bf2cceb6c0cd0d6b83ff51606}

题目

解题快手榜



爱因斯坦

1

注意：得到的 flag 请包上 flag{} 提交

 dafbd663-3...

Flag

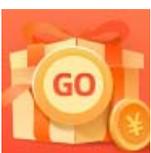
提交

正确

CSDN @qq_51550750

解题总结

- 【1】binwalk分析图片有一个ZIP文件
- 【2】dd命令分离该ZIP文件
- 【3】得到需要输入密码的flag.txt然后因为题目没有提示 如果暴力破解密码的话需要什么格式，就得从本来的图片中找密码
- 【4】图片的属性中就有密码
- 【5】得到flag



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)