




# misc-图片隐写

原创

0x7F.  于 2021-10-27 23:49:28 发布  53  收藏

文章标签: [安全](#)

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\\_51951386/article/details/121004720](https://blog.csdn.net/qq_51951386/article/details/121004720)

版权

## 题目描述

隐写2

MISC

未解决

题目作者: [harry](#)

一血: [好难的弗兰格](#)

一血奖励: 1金币

解 决: 1854

提 示:

描 述: f1@g{xxx}

其 他:

[↓ 下载](#)

CSDN @0x7F.

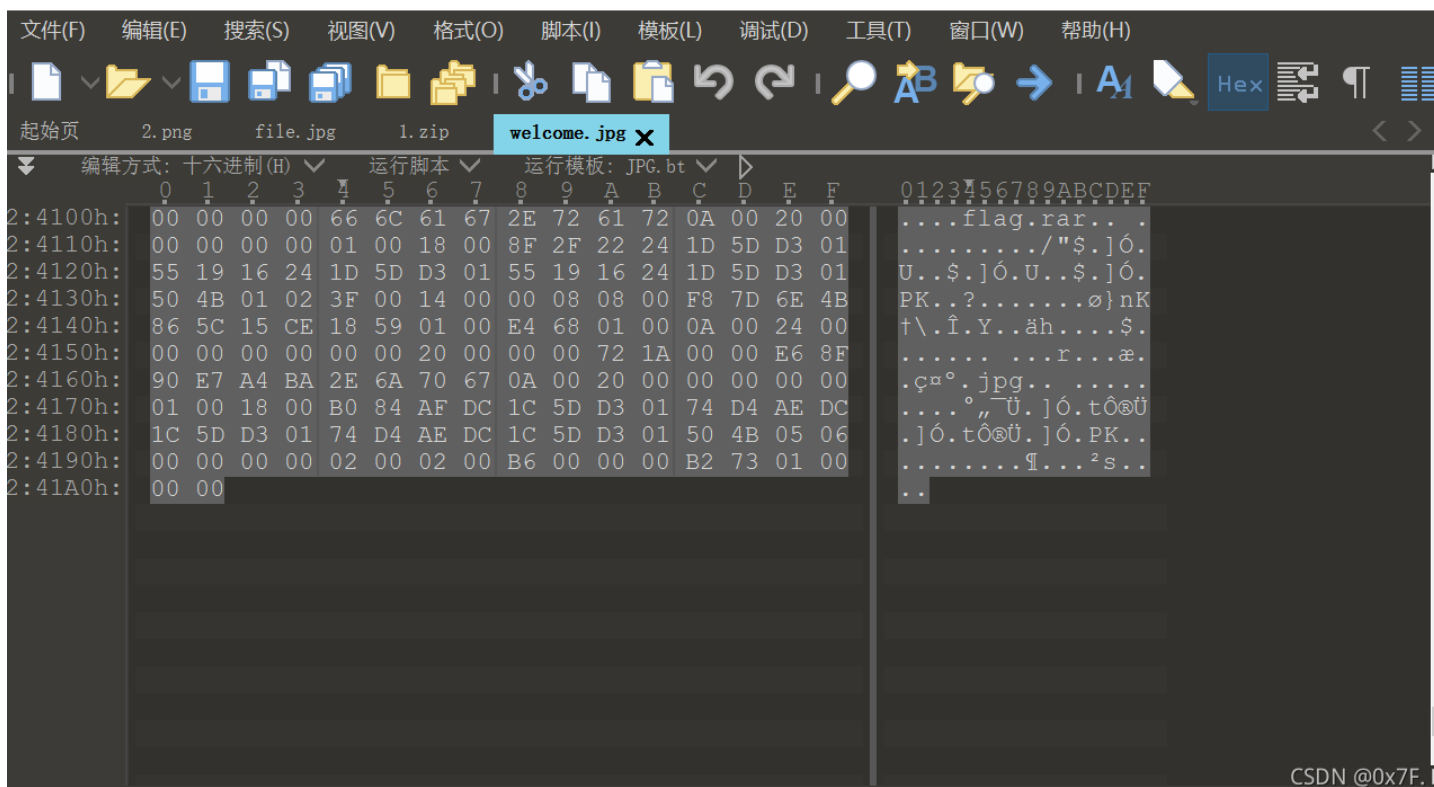
图片



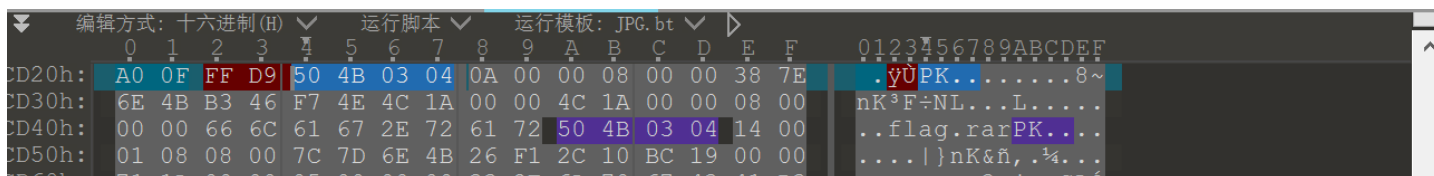
想拿到flag? 心中ないいくつかB数かの? CSDN @0x7F.

用010Editor打开，拉到尾部没有发现f1@g

010 Editor - C:\Users\lenovo\Downloads\welcome.jpg



搜索zip头文件，发现确实有



```

CD60h: 71 1A 00 00 03 00 00 00 33 2E 0A 70 87 43 41 D3
CD70h: 3A 6C B0 FB 54 2A E5 EC 61 7D 81 EB EF 34 F0 32
CD80h: 9C E7 16 3C C2 38 59 E7 4C 49 D2 7B 1E F3 2D F5
CD90h: 67 CD C2 25 95 73 94 5D 51 4F B2 AB A5 D1 86 9D
CDA0h: 41 92 C3 7F 91 17 3A 88 09 92 65 52 31 B2 5F BE
CDB0h: 0E 03 B7 83 CA E2 03 BA 1A 13 8A 27 49 DA 7E 4C
CDC0h: 3B F2 9C 15 14 2E F1 87 9D 25 2E 6C 00 85 99 7A
CDD0h: F7 48 C9 A8 3C 51 17 54 40 35 AB 54 D6 65 29 4E
CDE0h: 41 5F 6B 75 85 38 D3 6A 2B 2C 8B DA 3C 44 07 A1
CDF0h: 63 B8 3C 1A 2B 46 9B A9 BE 44 81 46 14 66 97 F1
CE00h: EA 06 C1 89 7C 07 73 D8 27 D5 E4 1B 8A 82 D6 8B
CE10h: F8 5B B1 C8 E9 29 7D 15 3A D9 DA 69 D5 75 99 7D
CE20h: 9F 6B C0 D3 5C 17 F1 22 E3 02 89 22 9A 1C 29 19
CE30h: BE EF 45 08 7E 38 65 D5 32 10 DD EE 0A 1E 96 AD
CE40h: E4 93 F6 E5 4D 68 C6 99 5F FF 34 25 2B 3B BB FF
CE50h: BD 5D 25 22 8D 4C 83 1E C0 DB 33 03 E9 EE 00 CE
CE60h: 71 2C 03 F0 CA 74 04 2F DD E8 FF 2B B4 13 1C 95
CE70h: 0C 00 41 02 16 1D F4 55 04 2D 4D 0A 21 74 27 40

```

查找结果

地址	值
已找到 3 个 '50 4B 03 04'.	
CD24h	50 4B 03 04
CD4Ah	50 4B 03 04
E796h	50 4B 03 04

CSDN @0x7F.

利用foremost分离图片，得到output目录

```

(root@kali)-[~/下载]
└─# foremost -i welcome.jpg
Processing: welcome.jpg
|foundat=flag.rarPK
foundat=提示.jpg
ECTZ(Ho
Bw]j]@D^Ha^wv36y9理在-1
a#g8F'bM:y;QzLG$Gq9
*|

```

发现里面有jpg目录和zip目录，jsp存放的之前的welcome.jpg图片，zip目录则有一个zip压缩包，压缩后发现一张jpg图片和一个需要密码的rar压缩包

```

(root@kali)-[~/下载/output/zip]
└─# ls
00000102.zip 提示.jpg  flag.rar

```

### 告诉你们一个秘密，密码是3个数哦。

查理曼：  
查理曼，法兰克王国国王，征服了西欧与中欧大部分土地，具有了至高无上的权威，下令全国人民信仰基督教，查理重振了西罗马帝国。

雅典娜：  
女神帕拉斯·雅典娜，是希腊神话中的女战神也是智慧女神，雅典是以她命名的。

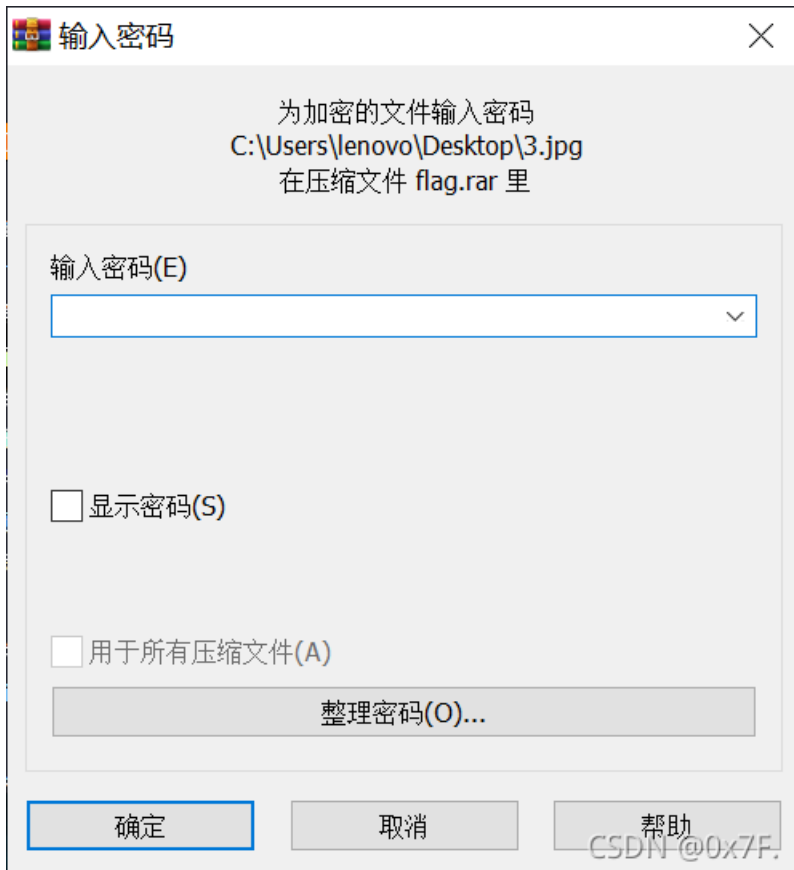
兰斯洛特，  
英格兰传说中的人物，是亚瑟王圆桌骑士团中的一员。看上去就是一个清秀年轻的帅小伙儿，由于传说中他是一名出色的箭手，因此梅花J手持箭支。兰斯洛特与王后的恋爱导致了他与亚瑟王之间的战争

物与正信的心及导致了它与正信上之间的例子。

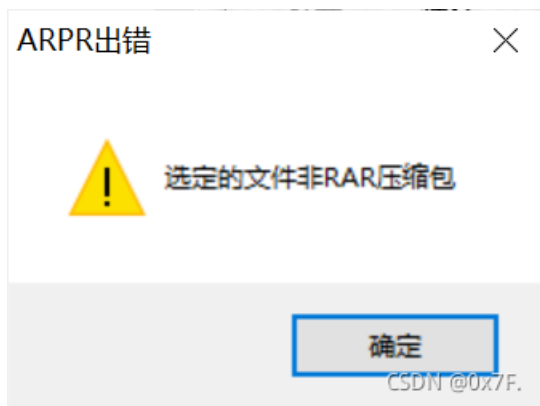
**Hint:**

其实斗地主挺好玩的。

CSDN @0x7F.



这里我们直接暴力破解



使用arpr报错,把后缀改成zip用ziperello爆破



输入解压得到一张图片, 010Editor打开拖到最后就是f1@g