

# 西邮网络科技协会ctf平台misc之真假迪迦writeup

原创

百里小羊 于 2019-11-16 14:10:27 发布 482 收藏 2

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\\_21538159/article/details/103096852](https://blog.csdn.net/qq_21538159/article/details/103096852)

版权

先来看题!!!

Challenge

0 Solves

×

## 真假迪迦 by ll

150

ll学长有一天心血来潮，想要重温童年的梦，就去看迪迦奥特曼了，然后他又保存了两张图片，这两张图片有一张是真的迪迦，另一张是假的迪迦，可是慌慌张张的他却分不清哪张是真，哪张是假，你能帮他找找吗？据说这两张图片可是大有猫腻哦，听说要用到几个神奇的工具哦！ll学长会为找到的人送出惊喜哦！所以，加油吧！

zip

Flag

Submit

[https://blog.csdn.net/qq\\_21538159](https://blog.csdn.net/qq_21538159)

这里划重点

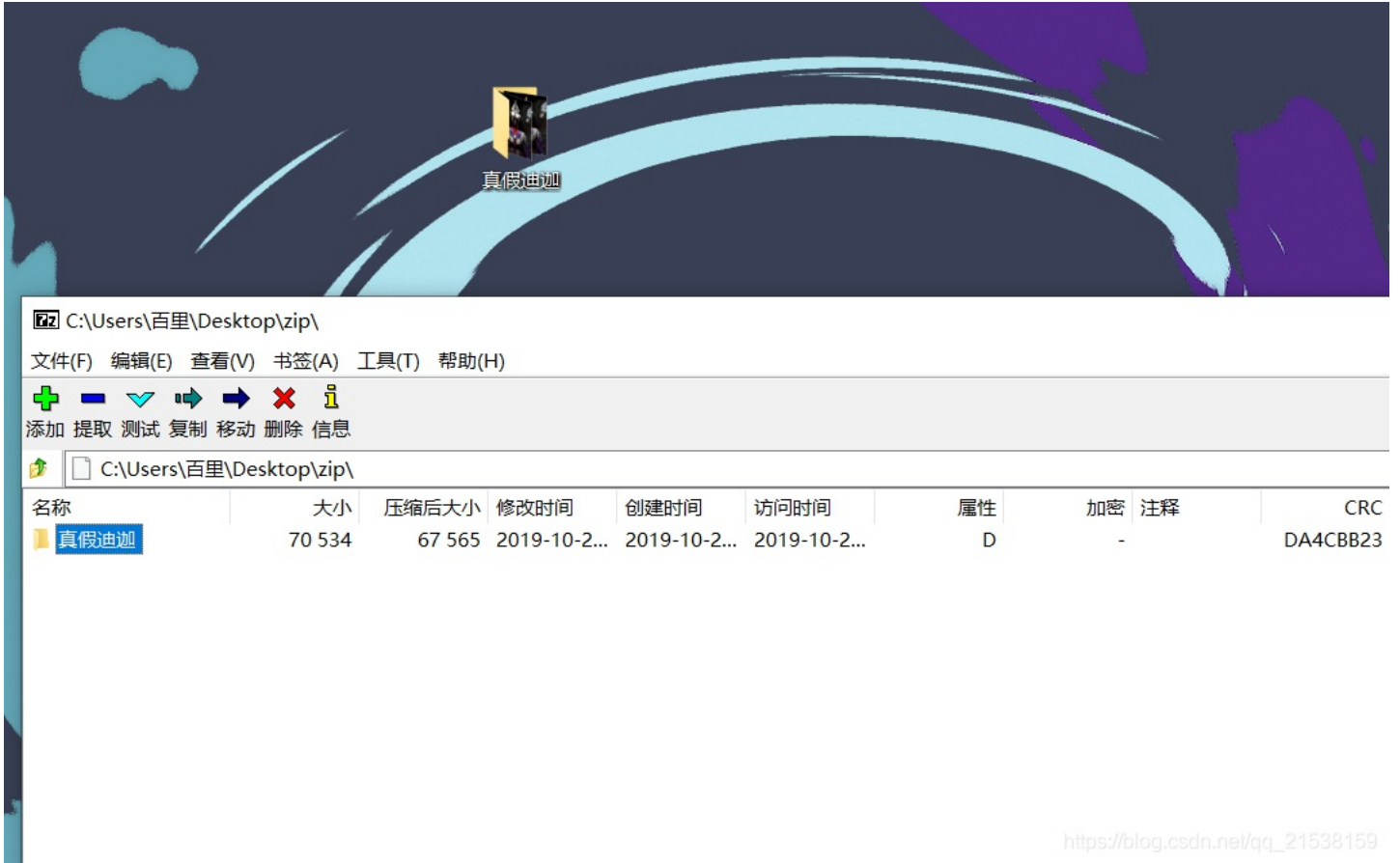
ll学长会为找到的人送出惊喜哦！

冲

下载压缩包



直接7z，拖拽解压



[https://blog.csdn.net/qq\\_21538159](https://blog.csdn.net/qq_21538159)

打开以后是两张图片



[https://blog.csdn.net/qq\\_21538159](https://blog.csdn.net/qq_21538159)

依次看下文件大小，再放winhex下看下，尝试搜索flag关键字字段未果，于是乎直接binwalk一下(这里为了方便直接改成1.jpg，和2.jpg)

```
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali:~# binwalk '/root/1.jpg' 文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
```

```

DECIMAL      HEXADECIMAL      DESCRIPTION
-----
0            0x0             JPEG image data, JFIF standard 1.01
32322       0x7E42          Zip archive data, at least v2.0 to extract, compressed size: 896, unc
ompressed size: 65536, name: flag1.txt
33348       0x8244          End of Zip archive, footer length: 22
root@kali:~#

```

```

root@kali:~# binwalk '/root/2.jpg'
DECIMAL      HEXADECIMAL      DESCRIPTION
-----
0            0x0             JPEG image data, JFIF standard 1.01
root@kali:~#

```

果然第一张图有东西，然后借助foremost工具分离一下

```

root@kali:~# foremost '/root/1.jpg'
Processing: /root/1.jpg
|foundat=flag1.txt00AR00D0+009vD0000nd0000|^      0\00g000000J0a0=000 0~0000000d700;00 0~00%000w\00
000 0~000 0|00000 tл/000>C00z0eZB?0gh00Ao0LK0wk00Uo0\b0A0000 0000q000Fio0LK`L00~:H{0eZc0G00A,0<00
00|000000t000 00冠 00|0maVK00w000000 00000mu5xDp0000m00G0 0kDp0000m00G0 0kDp000 0 00000m00 0~00000C
00C0000w00w000
.00000 0?d 000 C00\000mC00000 7J000D00 0~0000000000_00#L0~0000 000s?}
0F03t000000 0000K%0G0dG0 0Я
0~000000w0xG0000000=.000Я 0~0000h000000 000h0G00 0V0~0/0000000:Y00000 0~00 4C00o080 00000 000
0W00y 00^ 0 0~0000000000vW<x00[0 0~000000@00.03_000~00000 0~0'00E010j0
B0I 0~0+000S000 000y6I05x00w00h<00K{I05x00w00h<00K{I05x00w00h<00K{I05x00w00h<00K{I05x00w00h<00000E
y5000~00000
000000\00%0}0100000k0F

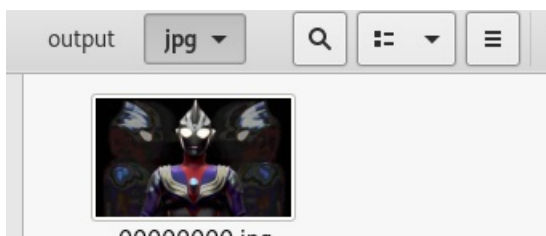
```

这里看到flag1.txt字段

同时当前文件夹下生成一个output文件夹，内容如下



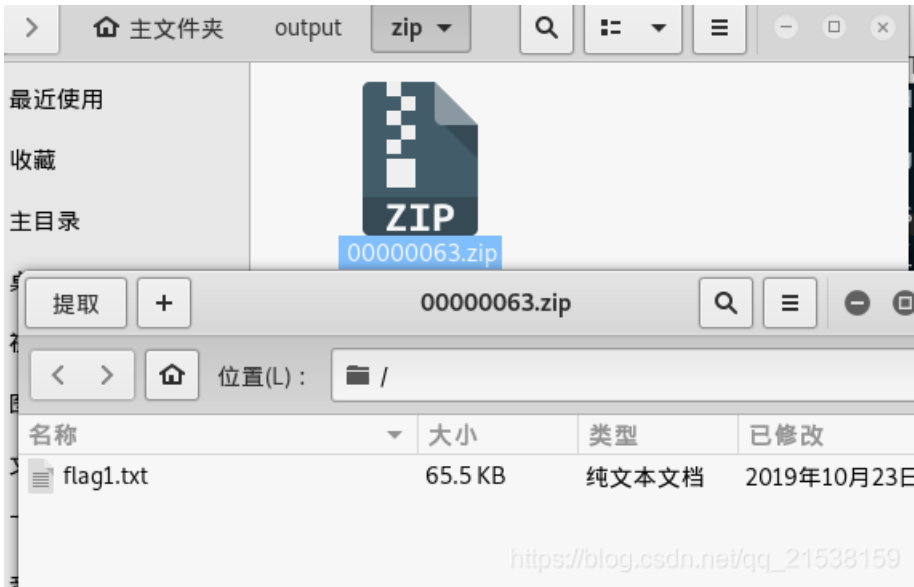
jpg里因该是迪迦的原图了



0000000.jpg

[https://blog.csdn.net/qq\\_21538159](https://blog.csdn.net/qq_21538159)

zip解压后发现flag1.txt



跟进flag1.txt





























扫描到以下内容

password:2333

以上内容非手机QQ提供，请谨慎使用。  
如需使用请复制。[csdn.net/qq\\_21538159](https://blog.csdn.net/qq_21538159)

好了，到此为止，迪迦1的戏份就结束了，为什么这样说呢。  
其一，

## 真假迪迦 by ll

### 150

ll学长有一天心血来潮，想要重温童年的梦，就去看迪迦奥特曼了，然后他又保存了两张图片，这两张图片有一张是真的迪迦，另一张是假的迪迦，可是慌慌张张的他却分不清哪张是真，哪张是假，你能帮他找找吗？据说这两张图片可是大有猫腻哦，听说要用到几个神奇的工具哦！ll学长会为找到的人送出惊喜哦！所以，加油吧！

zip

[https://blog.csdn.net/qq\\_21538159](https://blog.csdn.net/qq_21538159)

其二 还记得foremost出来的原图嘛  
我们来看一下几张图片的大小吧

迪迦一如下



迪迦二如下



foremost出来的原图



这里就很，明显了

迪迦2也是有东西的

但是binwalk并没有看到别的东西。再结合刚解出来的flag1是一个密码推断出这玩意因该是被加密的隐写，而不是简单的结合

这里就绕了很大的一个弯路

.....

先是stegsolve下研究了半天，未果

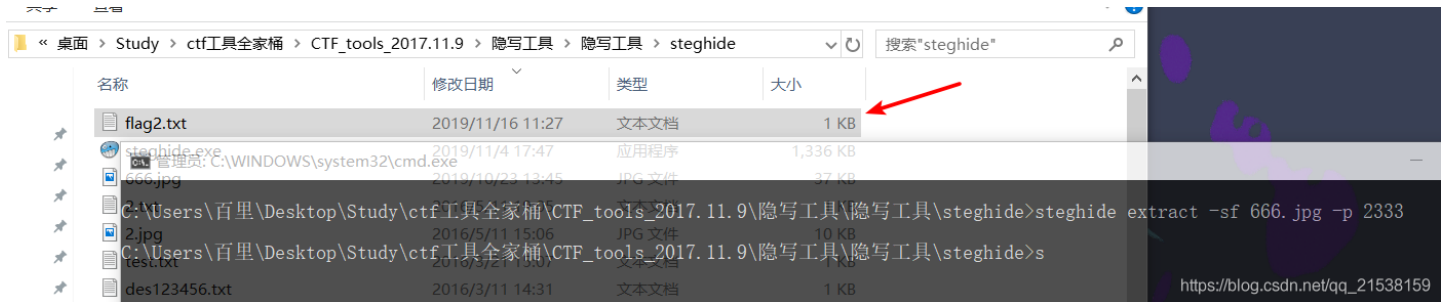
然后又走上了另一条弯路

以为是LSB加密隐写，然后又耽误了好长时间



[https://blog.csdn.net/qq\\_21538159](https://blog.csdn.net/qq_21538159)

就是没想到用Steghide去试一下  
然后这里



运行完后，在当前文件夹下跳出flag2.txt

flag2.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

flag is not here

那在哪儿呢?

试试这个吧:

链接: <https://pan.baidu.com/s/1kgb0rXgcaaQwv4->

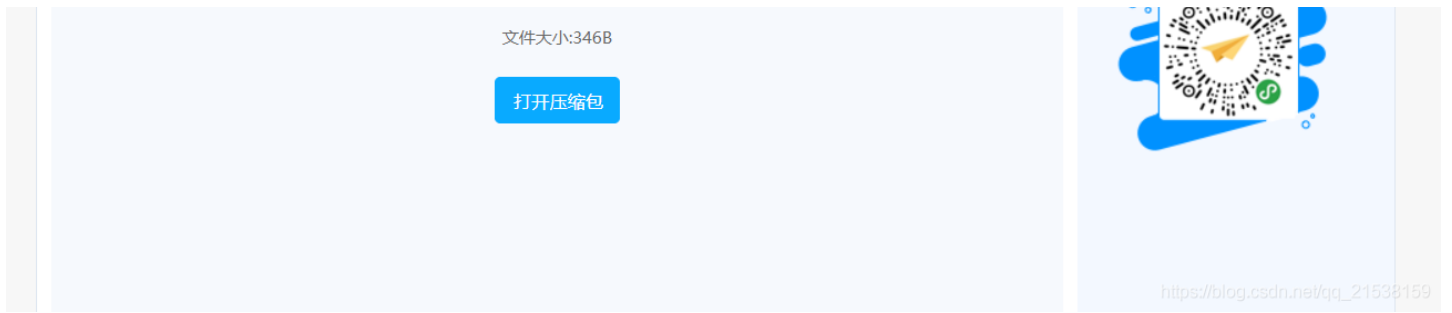
提取码: m4

复制这段内容后打开百度网盘手机App, 操作更方便哦

[https://blog.csdn.net/qq\\_21538159](https://blog.csdn.net/qq_21538159)

然后就到了这里





诶，这个头像好熟悉啊

嘻嘻

然后下载解压打开



出现flag3.txt

打开进去



还是打下马吧

至此，本题解析完毕

总结如下

题目本身并不是很难，更多考查的是熟练各种工具对不同文件的分析，而这需要在长期刷题的一个过程中不断去提炼，总结，反思，然后进步。

最后致敬出题人

