xctf攻防世界 MISC高手进阶区 something_in_image

l8947943 　于 2022-01-11 13:52:01 发布 　124 　收藏

分类专栏： 攻防世界misc之路 文章标签： misc

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/l8947943/article/details/122430846

版权

攻防世界misc之路 专栏收录该内容

68 篇文章 2 订阅

订阅专栏

1. 进入环境，下载附件

是个压缩文件，如图：

2. 问题分析

解法一

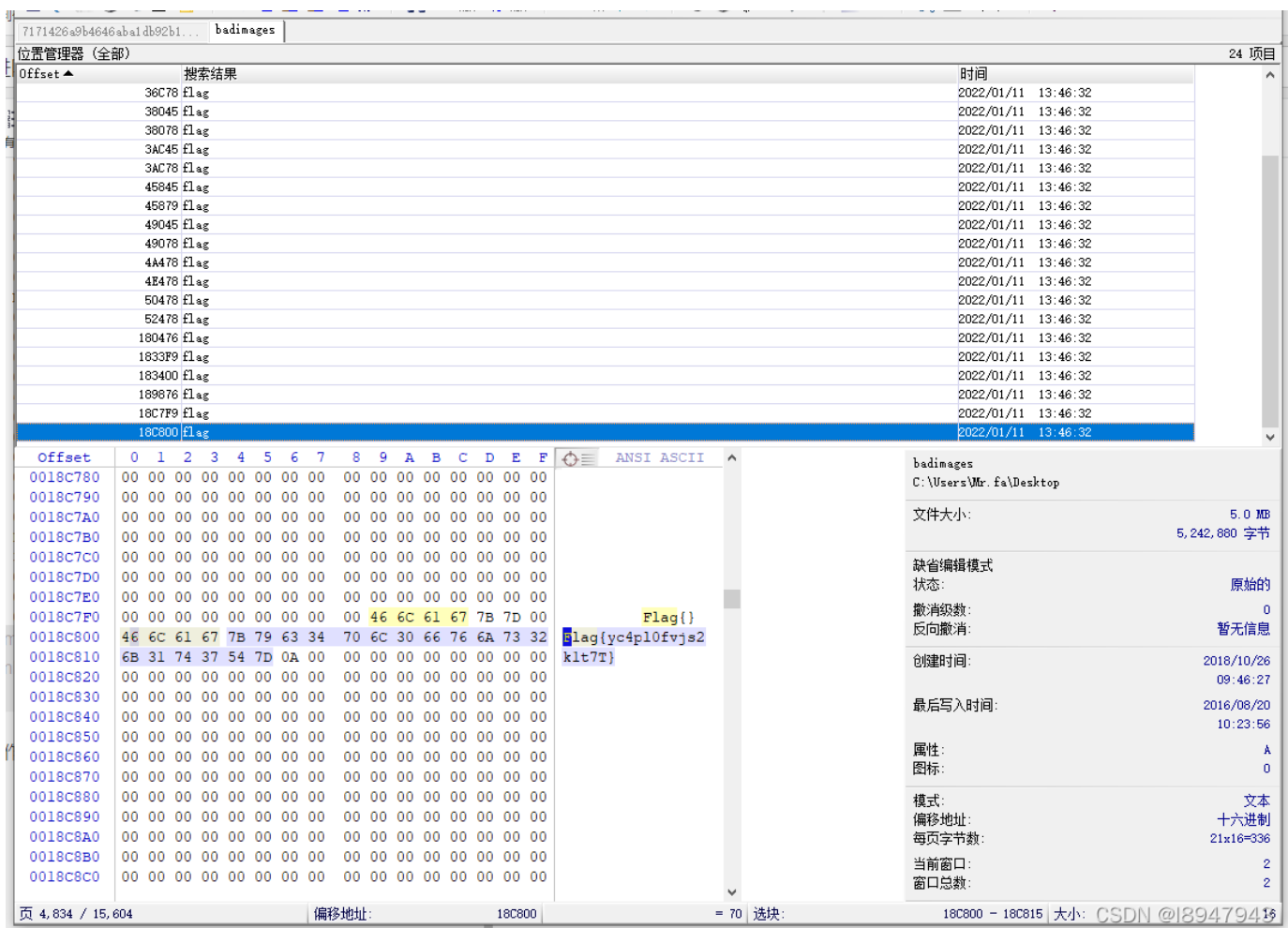题目是something_in_image（图片中有一些东西），而本身又是非图片文件，那么我么用winhex打开，看看有什么有用的信息，如图：

```
000003A0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
000003B0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
000003C0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
000003D0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
000003E0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
000003F0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000400  00 05 00 00 00 14 00 00   00 01 00 00 27 0F 00 00            '
00000410  F1 04 00 00 01 00 00 00   00 00 00 00 00 00 00 00   ñ
00000420  00 20 00 00 00 20 00 00   00 05 00 00 00 BF B7 57    ¿·W
00000430  3B BF B7 57 05 00 24 00   53 EF 01 00 01 00 00 00   ;¿·W  $ Sï
00000440  BF 36 F4 52 00 4E ED 00   00 00 00 00 01 00 00 00   ¿6ôR Ní
00000450  00 00 00 00 00 0B 00 00   80 00 00 00 3C 00 00 00   €    <
00000460  02 00 00 00 01 00 00 00   CA 01 46 91 C6 EA 4A 5A   Ê F'ÆêJZ
00000470  8D A4 74 A1 AA 1C 9A 80   00 00 00 00 00 00 00 00    ¤t¡ª š€
00000480  00 00 00 00 00 00 00 00   2F 6D 6E 74 2F 74 65 73           /mnt/tes
00000490  74 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   t
000004A0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
000004B0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
000004C0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 13 00
000004D0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
000004E0  08 00 00 00 00 00 00 00   00 00 00 00 2C 3D 7A 0F           ,=z
000004F0  8E 5A 43 2F BF E9 40 D7   D4 FB AD 16 01 01 00 00   ŽZC/¿é@×Ôû
00000500  00 00 00 00 00 00 00 00   BF 36 F4 52 C6 00 00 00           ¿6ôRÆ
00000510  C7 00 00 00 C8 00 00 00   C9 00 00 00 CA 00 00 00   Ç   È   É   Ê
00000520  CB 00 00 00 CC 00 00 00   CD 00 00 00 CE 00 00 00   Ë   Ì   Í   Î
00000530  CF 00 00 00 D0 00 00 00   D1 00 00 00 D2 00 00 00   Ï   Ð   Ñ   Ò
```

我们尝试在右侧ascii字符栏搜索flag，一通操作还真有，如图：

```
7171426a9b4646aba1db92b1...   badimages
位置管理器（全部）                                                                        24 项目
Offset ▲        搜索结果                                                        时间
   36C78 flag                                                         2022/01/11  13:46:32
   38045 flag                                                         2022/01/11  13:46:32
   38078 flag                                                         2022/01/11  13:46:32
   3AC45 flag                                                         2022/01/11  13:46:32
   3AC78 flag                                                         2022/01/11  13:46:32
   45845 flag                                                         2022/01/11  13:46:32
   45879 flag                                                         2022/01/11  13:46:32
   49045 flag                                                         2022/01/11  13:46:32
   49078 flag                                                         2022/01/11  13:46:32
   4A478 flag                                                         2022/01/11  13:46:32
   4E478 flag                                                         2022/01/11  13:46:32
   50478 flag                                                         2022/01/11  13:46:32
   52478 flag                                                         2022/01/11  13:46:32
  180476 flag                                                         2022/01/11  13:46:32
  1833F9 flag                                                         2022/01/11  13:46:32
  183400 flag                                                         2022/01/11  13:46:32
  189876 flag                                                         2022/01/11  13:46:32
  18C7F9 flag                                                         2022/01/11  13:46:32
  18C800 flag                                                         2022/01/11  13:46:32
```

```
Offset      0 1 2 3 4 5 6 7  8 9 A B C D E F      ANSI ASCII         badimages
0018C780   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00      C:\Users\Mr.fa\Desktop
0018C790   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0018C7A0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00      文件大小:              5.0 MB
0018C7B0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00                      5,242,880 字节
0018C7C0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0018C7D0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00      缺省编辑模式
0018C7E0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00      状态:                  原始的
0018C7F0   00 00 00 00 00 00 00 00  00 46 6C 61 67 7B 7D 00          Flag{}     撤消级数:              0
0018C800   46 6C 61 67 7B 79 63 34  70 6C 30 66 76 6A 73 32   Flag{yc4pl0fvjs2   反向撤消:           暂无信息
0018C810   6B 31 74 37 54 7D 0A 00  00 00 00 00 00 00 00 00   k1t7T}
0018C820   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00      创建时间:           2018/10/26
0018C830   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00                           09:46:27
0018C840   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0018C850   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00      最后写入时间:        2016/08/20
0018C860   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00                           10:23:56
0018C870   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0018C880   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00      属性:                    A
0018C890   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00      图标:                    0
0018C8A0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0018C8B0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00      模式:                   文本
0018C8C0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00      偏移地址:             十六进制
                                                                每页字节数:         21x16=336
页  4,834 / 15,604        偏移地址:        18C800    = 70  选块:      18C800 - 18C815  大小:     16   当前窗口:              2
                                                                窗口总数:                2
```

最终结果为： `Flag{yc4pl0fvjs2k1t7T}`

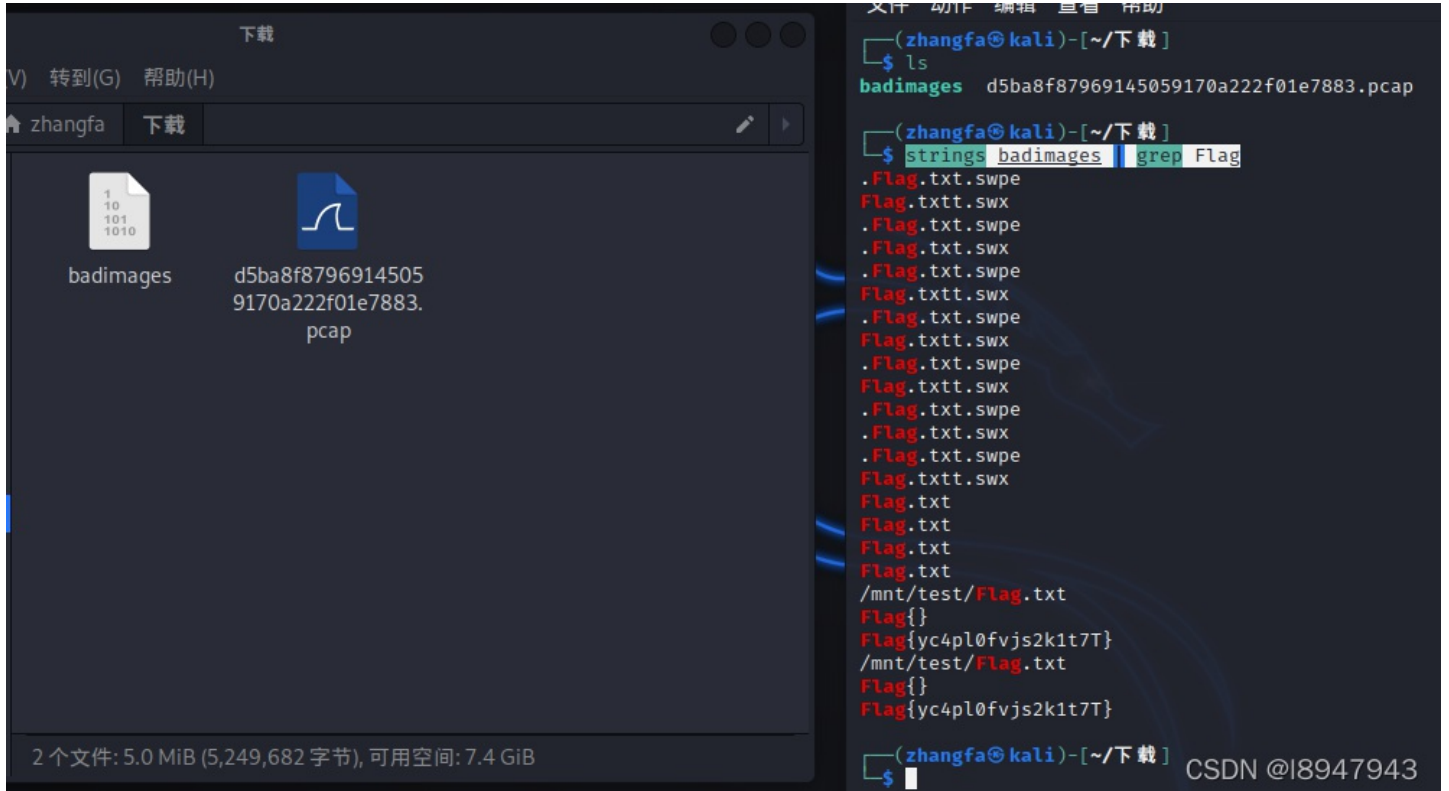## 解法二

参考网上的wp，在kali操作系统中使用strings命令，

```
strings badimages | grep Flag
```

效果如图：

3. **解法三**

   文件改成txt后缀，然后直接搜flag完事。