

# xctf攻防世界 MISC高手进阶区 hong

原创

18947943 已于 2022-01-25 15:31:28 修改 10900 收藏

分类专栏: [攻防世界misc之路](#) 文章标签: [安全](#) [web安全](#) [misc](#)

于 2022-01-25 15:30:42 首次发布

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/18947943/article/details/122686224>

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

给的是一个.mp3文件, 尝试打开后, 提示文件格式不对, 丢入winhex后, 对比文件头, 发现也没什么奇怪的点, 搜索关键词也无对应的字样

## 2. 问题分析

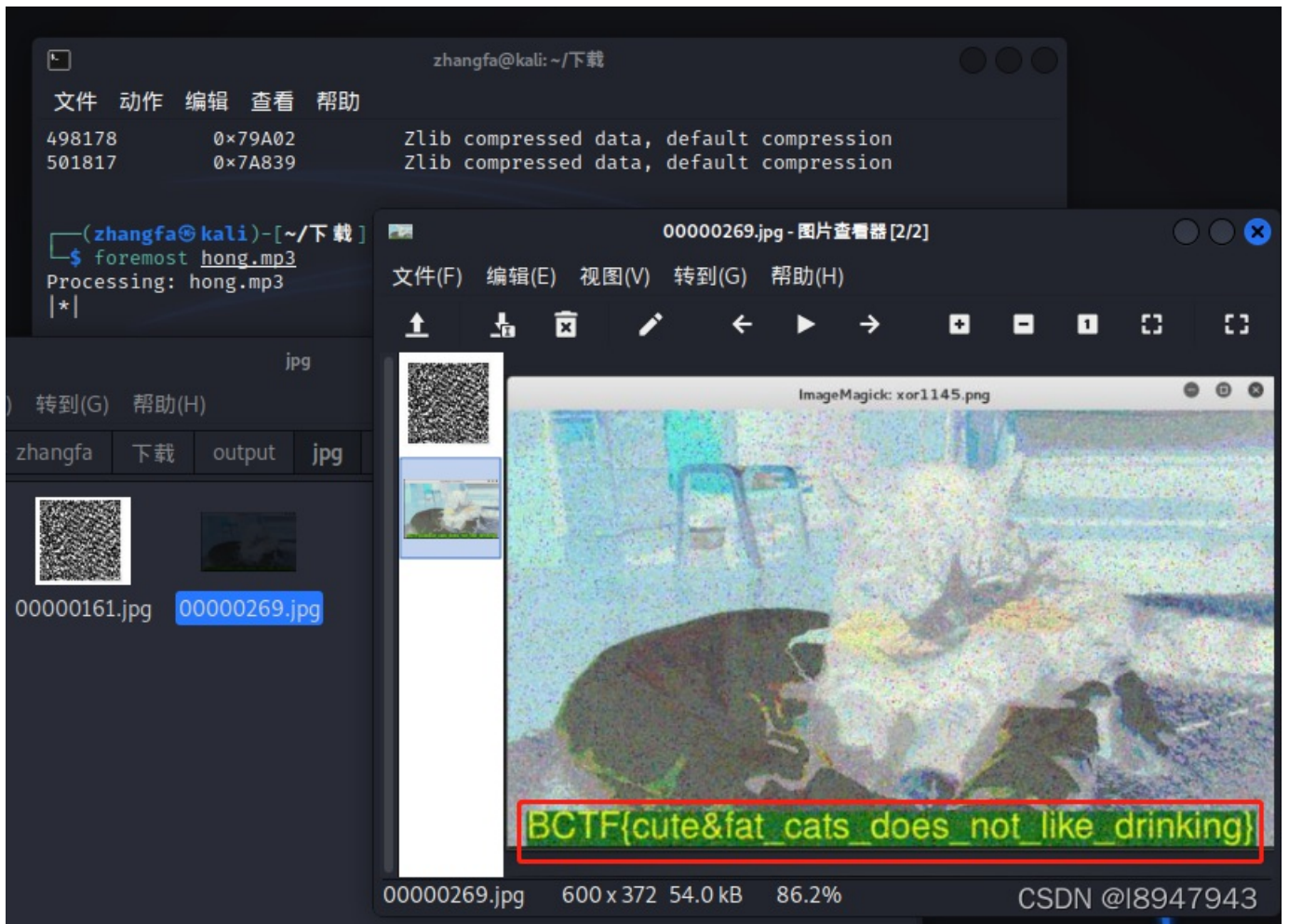
将文件丢入到kali中, binwalk查看一下有无隐写, 如图:

```
(zhangfa@kali) - [~/下载]
$ binwalk hong.mp3
```

DECIMAL	HEXADECIMAL	DESCRIPTION
55334	0xD826	Zlib compressed data, default compression
56734	0xDD9E	Zlib compressed data, default compression
82483	0x14233	JPEG image data, JFIF standard 1.01
82513	0x14251	TIFF image data, big-endian, offset of first image
directory: 8		
112115	0x1B5F3	Zlib compressed data, default compression
112861	0x1B8DD	Zlib compressed data, default compression
136938	0x216EA	Zlib compressed data, default compression
138170	0x21BBA	JPEG image data, JFIF standard 1.01
138200	0x21BD8	TIFF image data, big-endian, offset of first image
directory: 8		
192612	0x2F064	Zlib compressed data, default compression
194332	0x2F71C	Zlib compressed data, default compression
195518	0x2FBBE	Zlib compressed data, default compression
274685	0x430FD	Zlib compressed data, default compression
275977	0x43609	Zlib compressed data, default compression
276905	0x439A9	Zlib compressed data, default compression
277642	0x43C8A	Zlib compressed data, default compression
285855	0x45C9F	Zlib compressed data, default compression
294828	0x47FAC	Zlib compressed data, default compression
303158	0x4A036	Zlib compressed data, default compression
311823	0x4C20F	Zlib compressed data, default compression
320796	0x4E51C	Zlib compressed data, default compression
333060	0x51504	Zlib compressed data, default compression
335054	0x51CCE	Zlib compressed data, default compression
498178	0x79A02	Zlib compressed data, default compression
501817	0x7A839	Zlib compressed data, default compression

GSDN@18947943

有图片文件数据, 因此使用foremost进行分离, 如图:



最终答案为: `BCTF{cute&fat_cats_does_not_like_drinking}`