

xctf攻防世界 MISC高手进阶区 3-11

原创

[18947943](#) 于 2022-01-19 10:55:47 发布 3729 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/18947943/article/details/122575855>

版权



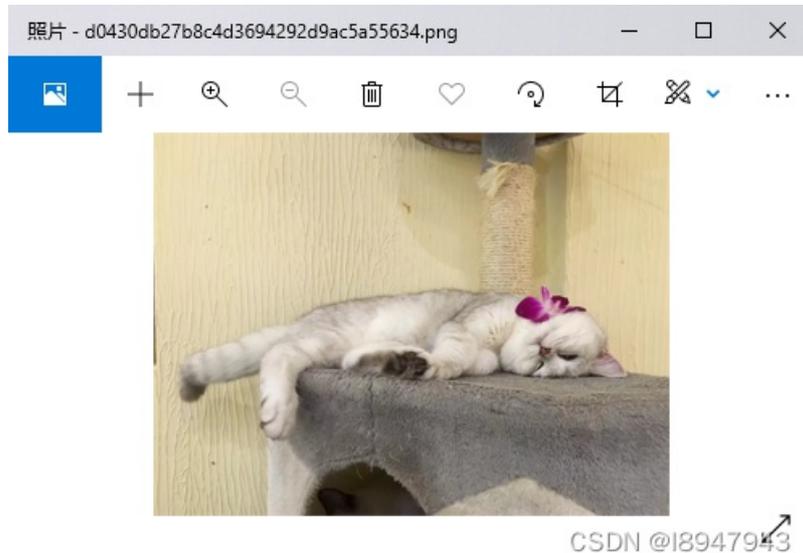
[攻防世界misc之路](#) 专栏收录该内容

68 篇文章 2 订阅

订阅专栏

1. 进入环境, 下载附件

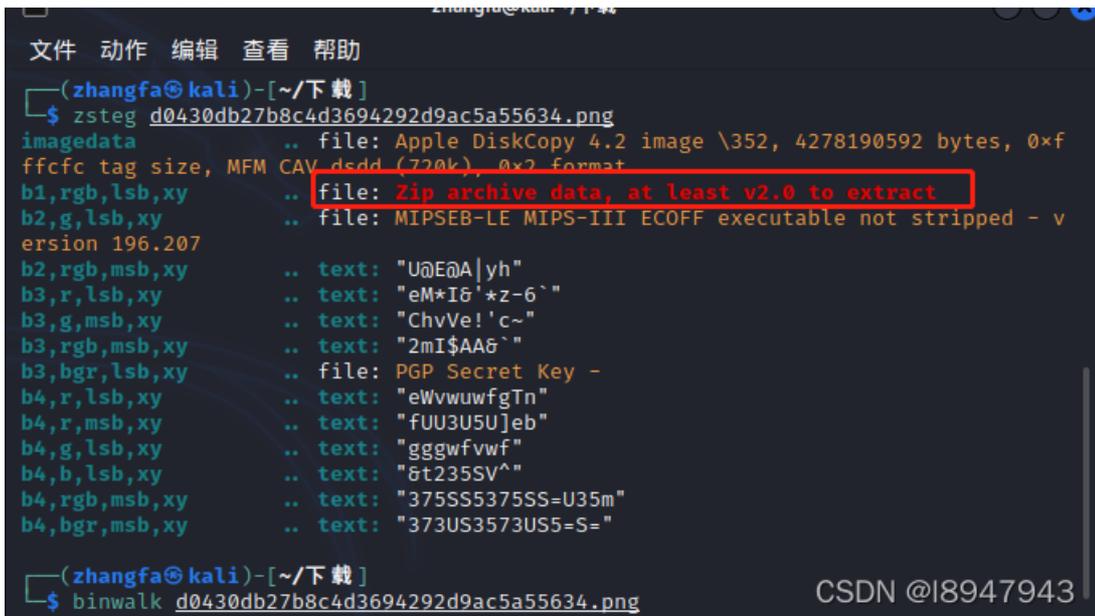
题目给的是一张猫猫png图片, 如图:



2. 问题分析

kali中zsteg

我发现这个工具真的好用，如图：



```
(zhangfa@kali)-[~/下载]
└─$ zsteg d0430db27b8c4d3694292d9ac5a55634.png
imagedata .. file: Apple DiskCopy 4.2 image \352, 4278190592 bytes, 0xffcfc tag size, MFM CAV dsdd (720k), 0x2 format
b1,rgb,lsb,xy .. file: Zip archive data, at least v2.0 to extract
b2,g,lsb,xy .. file: MIPS-EB-LE MIPS-III ECOFF executable not stripped - version 196.207
b2,rgb,msb,xy .. text: "U@EQ@A|yh"
b3,r,lsb,xy .. text: "eM*I@' *z-6`"
b3,g,msb,xy .. text: "ChvVe!'c~"
b3,rgb,msb,xy .. text: "2mI$AA@`"
b3,bgr,lsb,xy .. file: PGP Secret Key -
b4,r,lsb,xy .. text: "eWvwuwfgTn"
b4,r,msb,xy .. text: "fUU3U5U]eb"
b4,g,lsb,xy .. text: "gggwfvwf"
b4,b,lsb,xy .. text: "6t235SV^"
b4,rgb,msb,xy .. text: "375SS5375SS=U35m"
b4,bgr,msb,xy .. text: "373US3573US5=S="

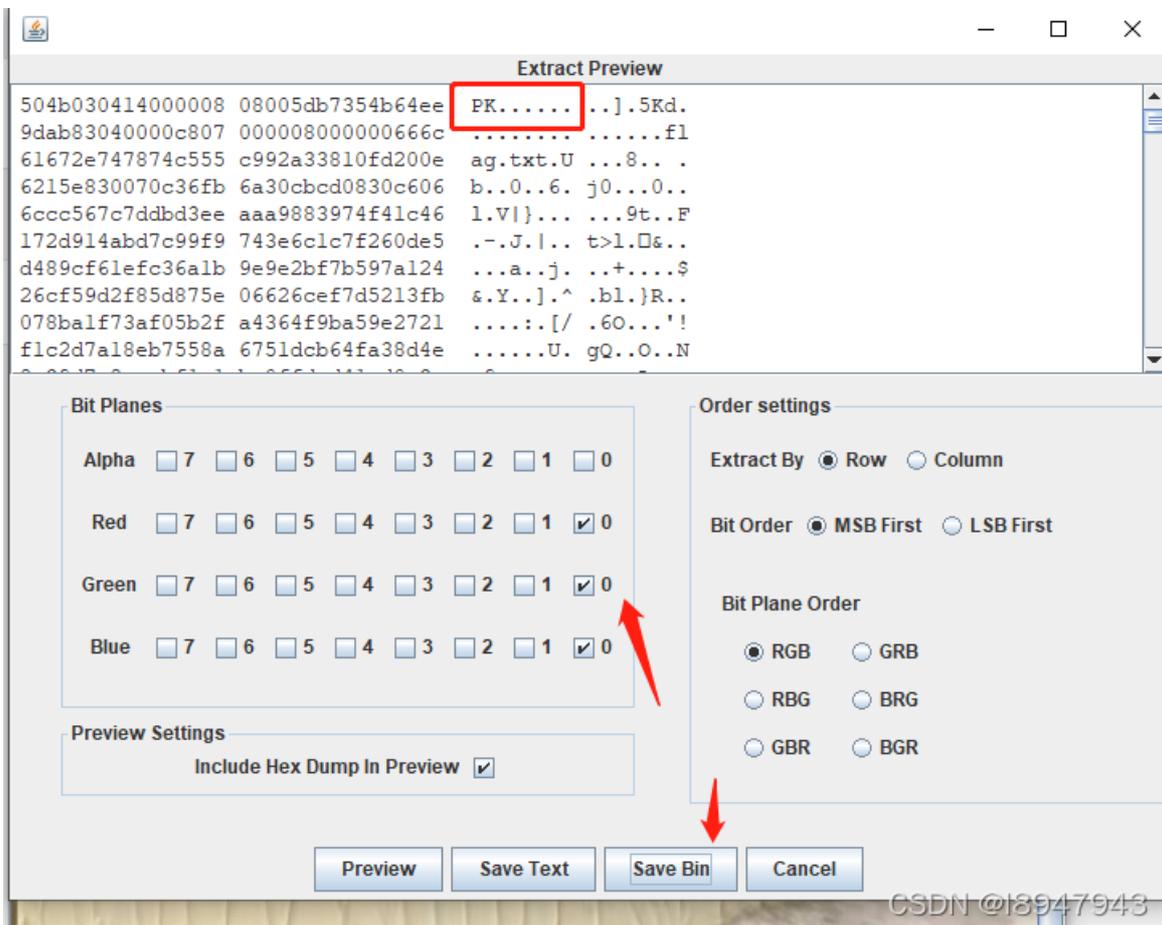
(zhangfa@kali)-[~/下载]
└─$ binwalk d0430db27b8c4d3694292d9ac5a55634.png
```

如图，第一通道，rgb三色的lsb（least significant bit）的读模式是个Zip数据文件，好的，搞出来

StegSolve提取

如图，可以看到位通道的数据是504B0304（ZIP Archive (zip)文件），对照地址：

<https://blog.csdn.net/holandstone/article/details/7624343>



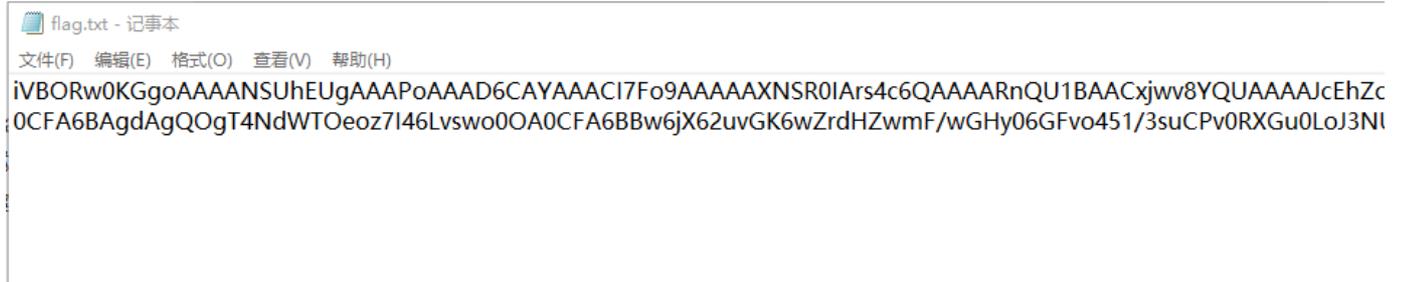
我们存储文件并保存为Zip格式。

3. base64转图片

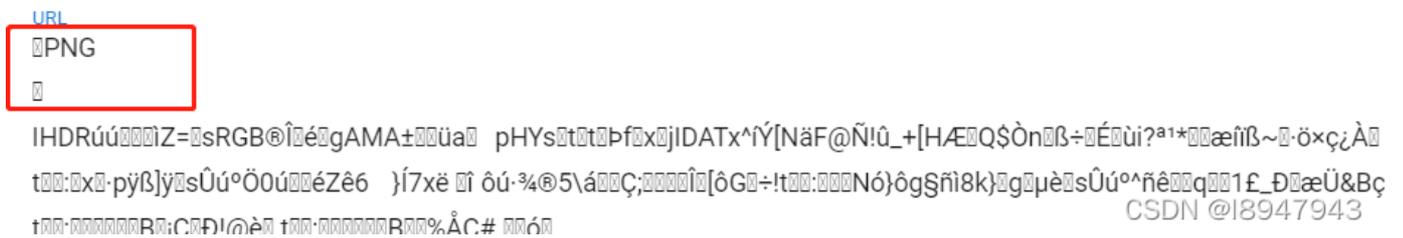
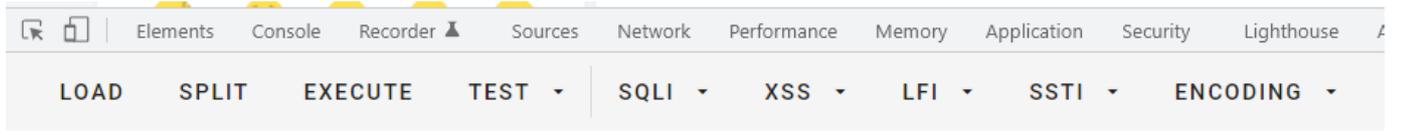
部分软件可能存在win环境中打不开压缩包的问题，要么尝试修复，要么在kali中打开，如图：



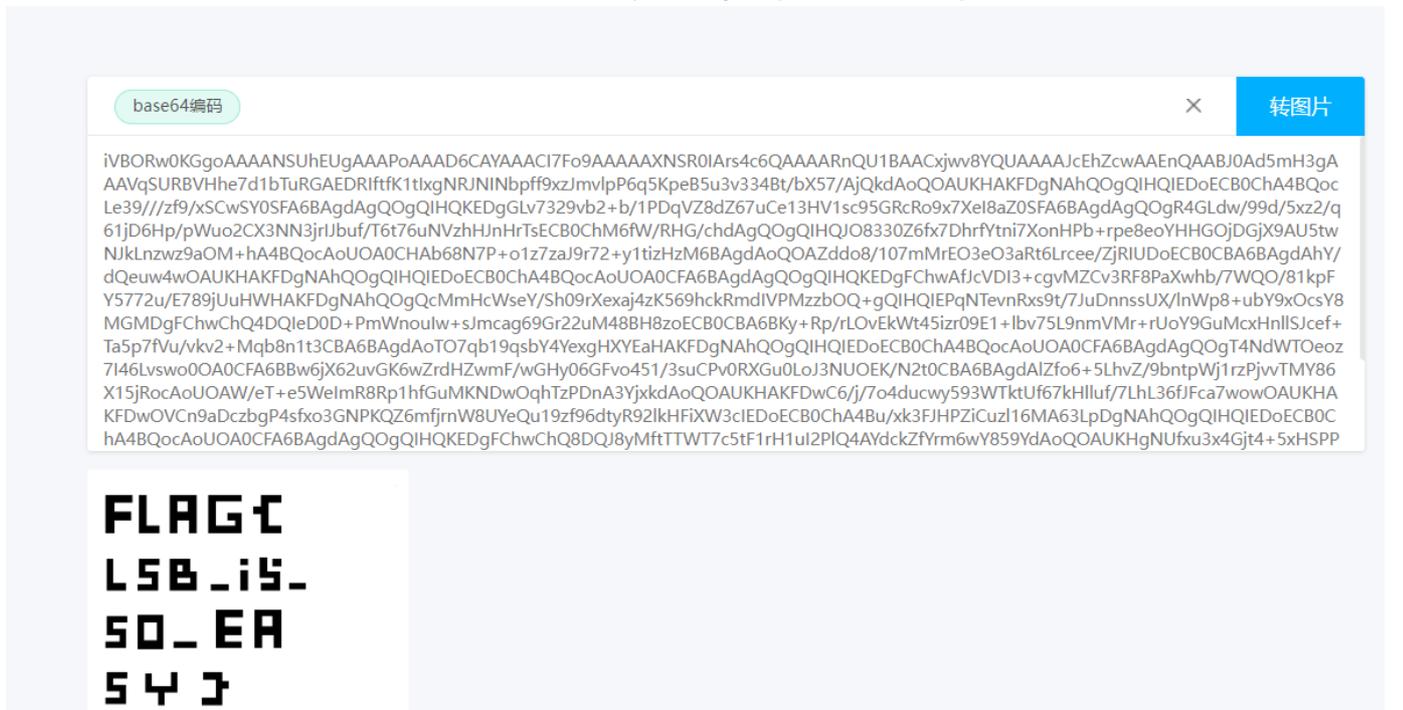
给了一堆字符：



后面有=号，很像base64，使用hackbar解码，发现有png字样，如图：



猜测是base64需要转成图片文件，找到在线小工具：<https://tool.jsuapi.com/base642pic.html>，结果如图：



最终答案为: `FLAG{LSB_i5_S0_EASY}`