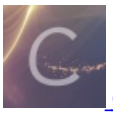
【MISC】从零开始学MISC

原创

兔兔包点吃机 于 2019-05-28 21:18:06 发布 12388 收藏 33

分类专栏： CTF MISC 文章标签： CTF

本文链接：https://blog.csdn.net/nineqblot/article/details/90647324


CTF 同时被 2 个专栏收录

3 篇文章 0 订阅

订阅专栏


MISC

1 篇文章 0 订阅

订阅专栏

1.了解ext3文件系统，熟练使用mount

将linux文件拽入虚拟机。

```
strings linux  //以字符串模式查看文件
strings linux | grep flag  //筛选flag字样
mount linux /mnt //使用mount挂载文件系统或使用binwalk提取文件
find /mnt -name "flag.*" -print  //寻找挂在之后的flag所在位置，得到地址 /mnt/O7avZhikgKgbF/flag.txt
cat O7avZhikgKgbF/flag.txt  //得到flag
base64 -d /mnt/O7avZhikgKgbF/flag.txt //base64转码（base64 balabala是加密，base64 -d balabala是解密）
```

2.修复二维码扫描得到flag

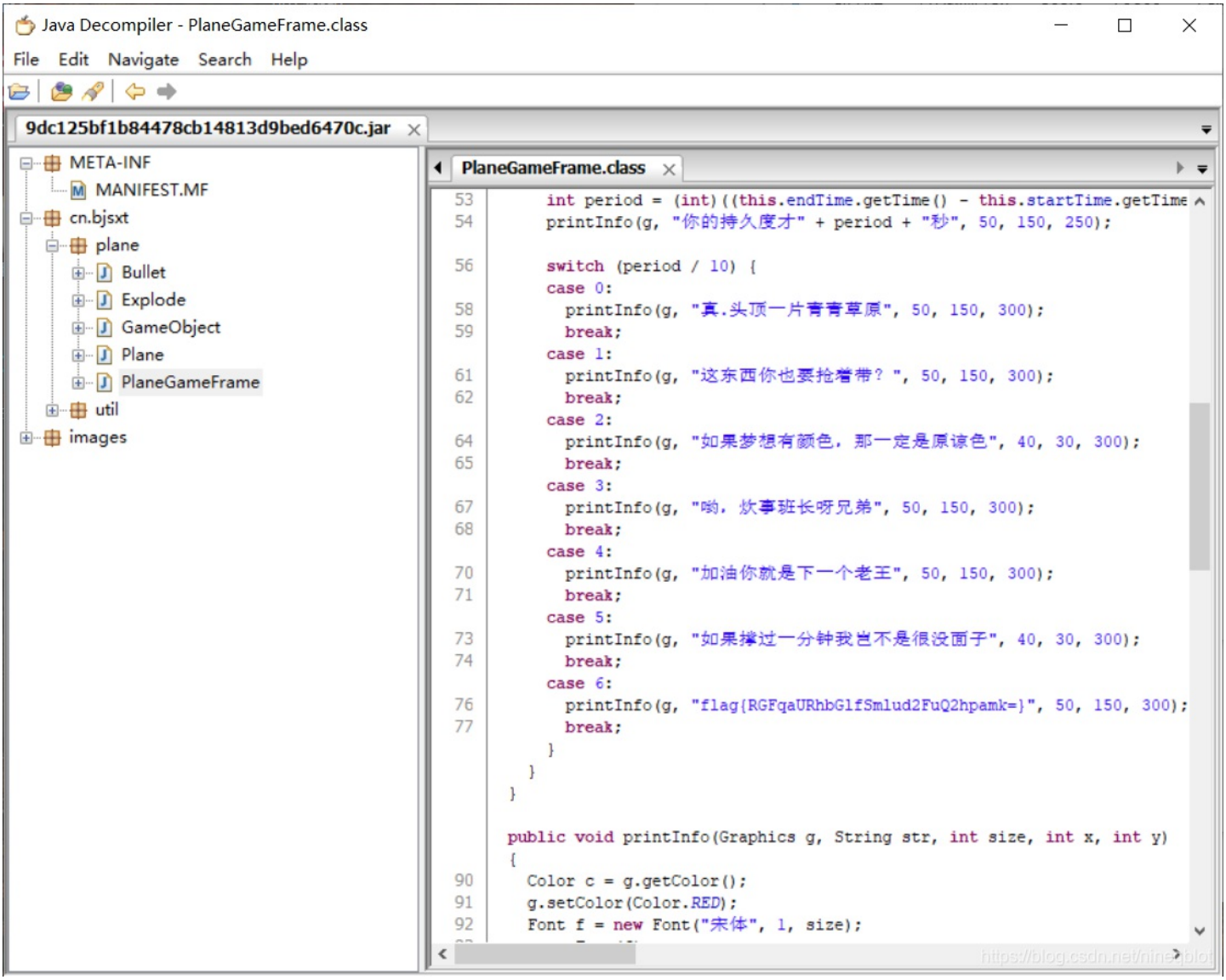
用fireworks打开gif图片，在第50帧找到二维码，发现三角残缺。
用photoshop找到完整二维码，截取三角补全二维码，扫描即得flag。

3.在pdf中找flag

题目提示在“图下面”。转换为word文档。

4.Java逆向，base64解码

java小游戏，坚持不到60s
选择反编译，使JD-GUI对这个java程序进行反编译。



得到flag，看后面带个=，考虑base64解码

5.Base64 ROT13 与佛论禅

夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三佷三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智佷諸若奢數菩奢集遠俱老竟寫明奢若梵等盧皤豆蒙密離怯婆皤礙他哆提哆多缽以南哆心曰姪罰蒙吶神。舍切真怯勝吶得俱沙罰娑是怯遠得吶數罰輸哆遠薩得槃漫夢盧皤亦醢吶娑皤瑟輸諳尼摩罰薩冥大倒參夢佷阿心罰等奢大度地冥毀皤沙蘇輸奢恐豆佷得罰提哆伽諳沙楞缽三死怯摩大蘇者數一遮。

与佛论禅？？？

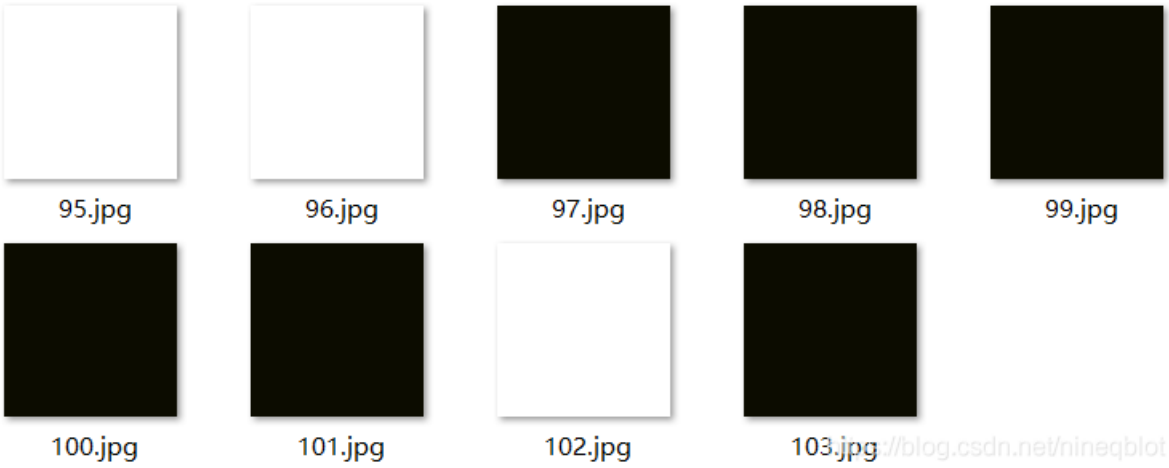
ROT13是它自己本身的逆反；也就是说，要还原ROT13，套用加密同样的演算法即可得，故同样的操作可用再加密与解密。ROT13=字符向后位移13位，但向前13与向后13结果相同？？

将ROT13解密后的结果进行base16解密？？

此题思路完全懵，想不到为什么要用ROT13。逐个尝试得到的？

6.二进制转换字符。

纯黑白的gif图，给出了gif文件夹，标了数字。



用ASCLL在线转换器转换前八位（二进制转字符），发现为f，方法正确。可通过python代码实现整个工作。

```
import os
#rb:r(只读)、w(只写)、a(追加)、b(二进制)
white = open("*/gif/0.jpg", "rb").read()
black = open("*/gif/1.jpg", "rb").read()
flag_binary = ""
for i in range(104):
    with open("*/gif/%d.jpg"%i,"rb") as f:
        if f.read() == white:
            flag_binary += "0"
        else:
            flag_binary += "1"
flag = ""
for i in range(int(len(flag_binary)/8)):
    flag += chr(int(flag_binary[i*8:(i+1)*8],2))
    #int(123,2)：将123转换为2进制的int值。int(x, [base])，其中base取值可为2~36。默认为10。
    print (flag)
```