论剑-writeup

因为很少人做出来，导致网上很少这个wp（找不到），所以我在这里记录下解题思路

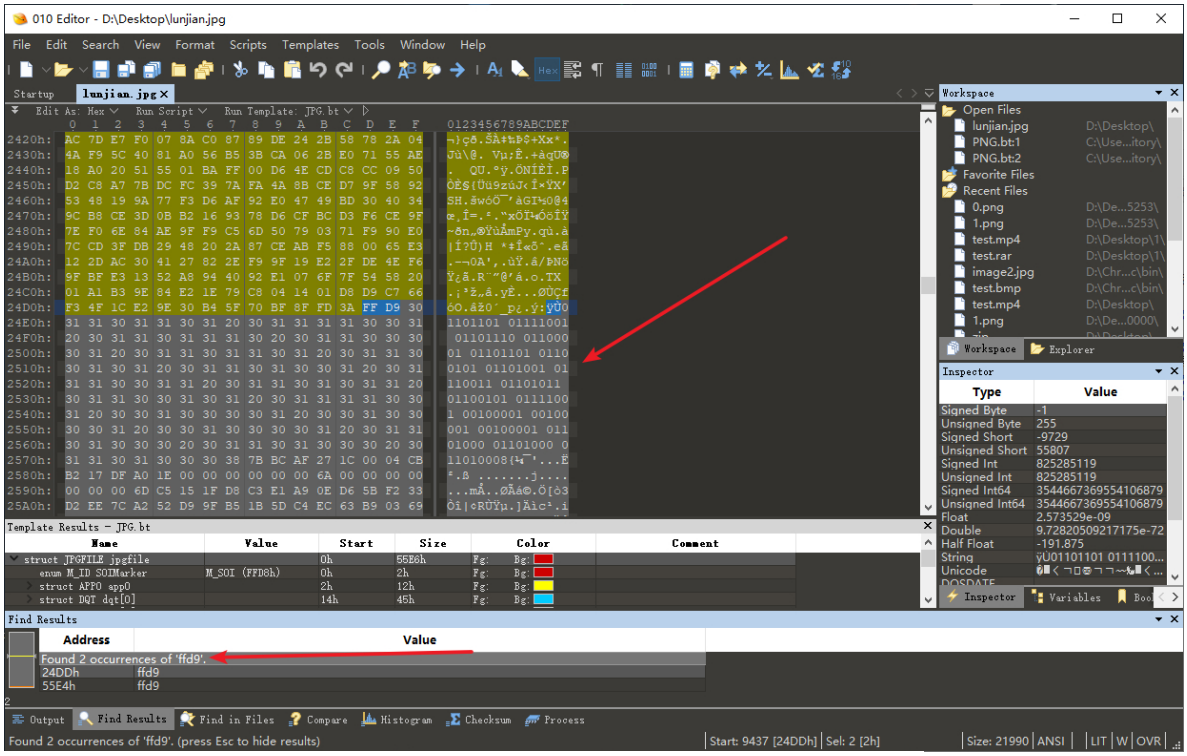
打开题目

访问链接，把图片下载下来另存为

先把它丢进kali上binwalk扫描以下，发现有隐藏文件，foremost直接分离出来，得到两张图片

把图片都拿去二进制编辑工具查看下，在原图上搜索下FFD9（jpg的结束标识），发现有两个，以及一段二进制文件，很可疑

这段二进制拿去转ASCII码，得到mynameiskey!!!hhh 折腾了下，暂时先放着。



ASCII在线转换器-十六进制，十进制、二进制

ASCII转换到 ASCII (例: a b c)

```
m y n a m e i s k e y ! ! ! h h h
```

添加空格 删除空格 将空白字符转换

十六进制转换到16进制(例:0x61或61或61/62) 删除 0x

```
0x6d 0x79 0x6e 0x61 0x6d 0x65 0x69 0x73 0x6b 0x65 0x79
0x21 0x21 0x21 0x68 0x68 0x68
```

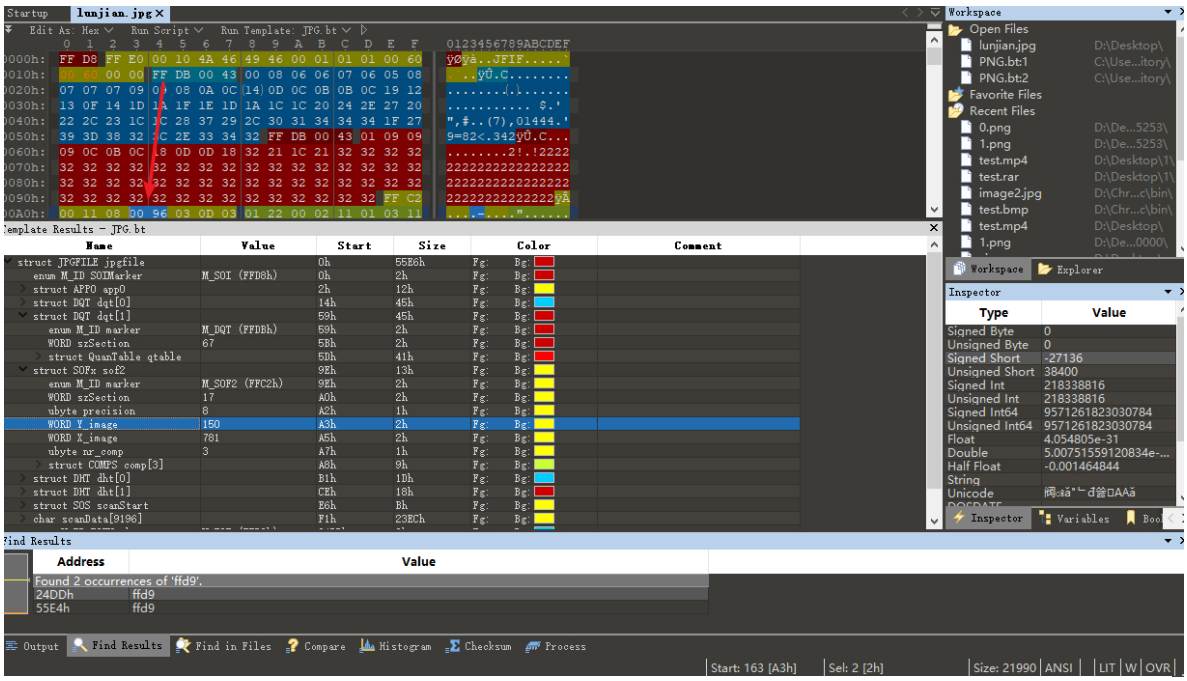
十进制转换到 10进制 (例: 97 98 99)

```
109 121 110 97 109 101 105 115 107 101 121 33 33 33 104
104 104
```

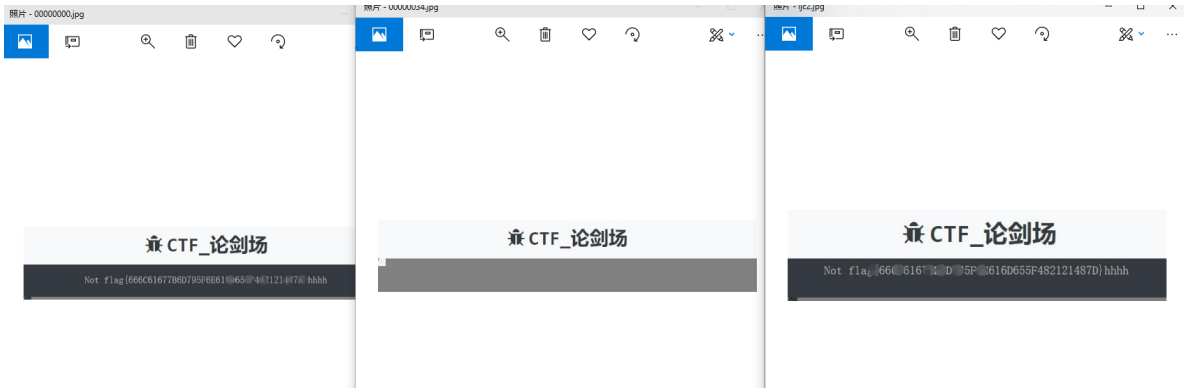
二进制转换到 2进制(例:01100001 01100010 01100011)

```
01101101 01111001 01101110 01100001 01101101 01100101
01101001 01110011 01101011 01100101 01111001 00100001
00100001 00100001 01101000 01101000 01101000
```

什么详细信息、备注都毫无hint，想着修改图片高度看下，发现新大陆，但是隐藏了一部分-_-!

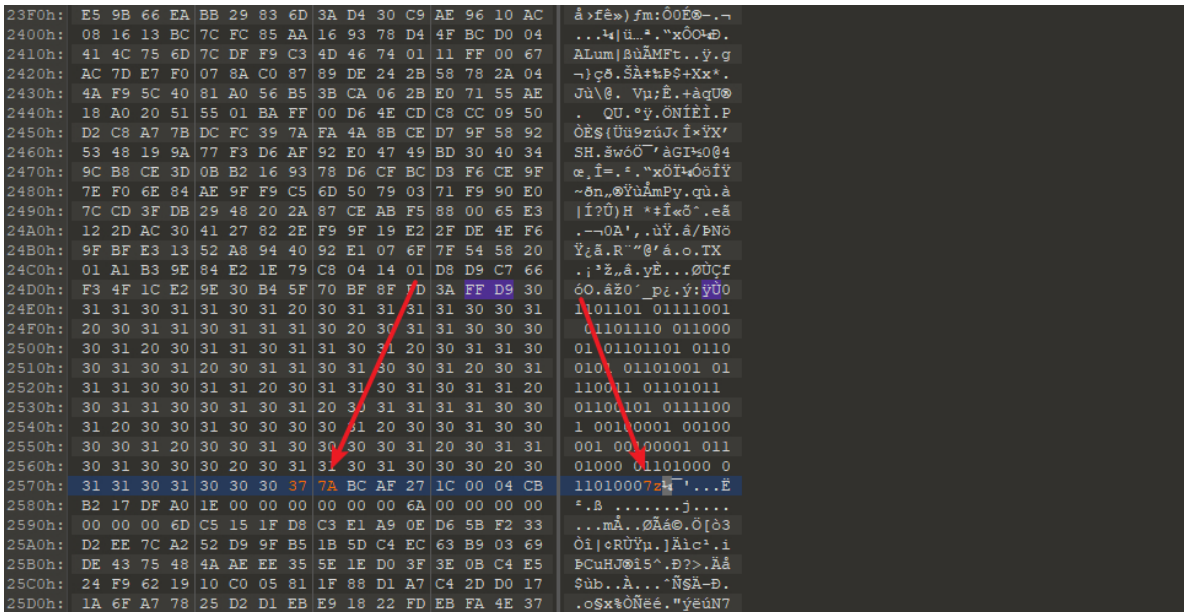


把分离出来的图片都修改高度，发现跟原图一样，无果



天坑，这里想打si作者的环节，在分离出来的两张图片，以及这段这段二进制狂下功夫，xor、盲水印、色道分析..折腾了一段时间并没有什么用

查看二进制那段信息发现，看到BC AF 27 1C好熟悉，好像特征码给改过，尝试修改,修复文件头



常见的文件头：

7z

文件头标识：37 7A BC AF 27 1C

JPEG/JPG

文件头标识：ff, d8 (SOI) (JPEG 文件标识)

文件结束标识：ff, d9 (EOI)

PNG

文件头标识：89 50 4E 47 0D 0A 1A 0A

GIF

文件头标识：47 49 46 38 39(37) 61--- GIF89(7)a

BMP

文件头标识：42 4D--- BM

HTML (html)

文件头标识：68746D6C3E

ZIP Archive (zip)

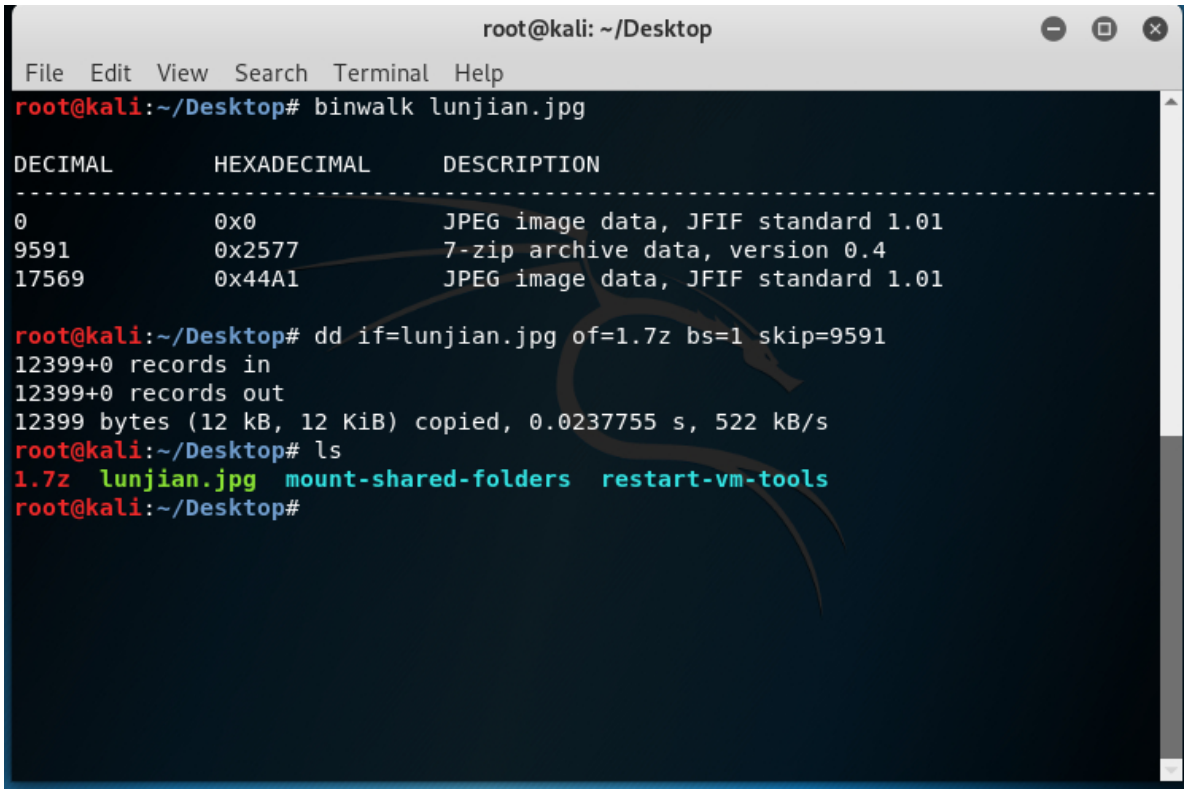
文件头标识：504B0304 --- PK

RAR Archive (rar)

文件头标识：52617221

等等..

丢回kali用binwalk分析，发现多了一个压缩包，分离，注意使用foremost分离不出来，利用dd分离出来



使用dd命令分离文件，如：
dd if=hehe.jpg of=hehe1.zip bs=1 skip=54163
if=file（源文件）
of=file（输出文件）
bs=bytes（一次性转换bytes个字节，及转换缓冲区大小）
skip=blocks（输入文件开头跳过blocks个块再开始复制--通俗点讲就是从哪开始）

进行解压，需要密码，用二进制转的ASCII码进行解密，得到一张图片，修改高度，得到另一部分的flag，进行拼接
最终得到一个的密文

这个不是md5，是一个base16密文，进行base16解密，得到flag

666C61677B6D795F6E616D655F482121487D

编码 解码

flag{my_name_H!!H}