

图片隐写分离

转载

[weixin_33704591](#) 于 2017-10-04 23:32:00 发布 394 收藏 1
提供下载:<https://files.cnblogs.com/files/xishaonian/yanhuo.rar>

工具:用

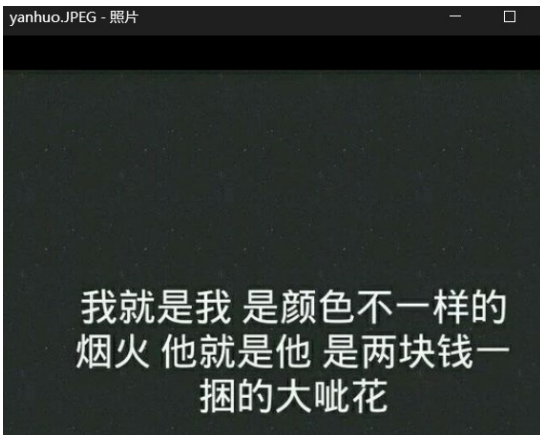
bindwalk

foremost

得到的时候是rar格式的,首先先判断一下其是否格式正确,直接丢Winhex查看发现是JFIF即为图片格式。



然后改为jpge之后图片显示正常

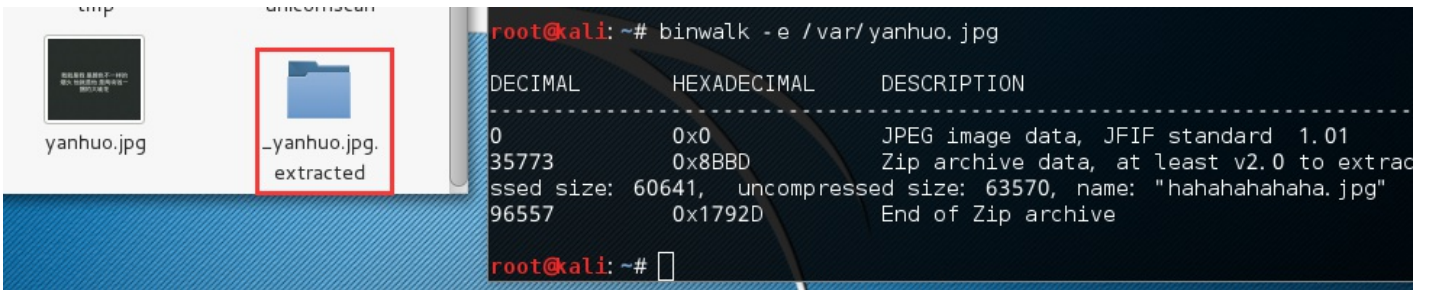


然后使用kali下的binwalk检测是否嵌入了数据（其实得到rar的时候直接打开里面就有一张hahaha.jpg的图片但是直接解压是失败的。心想就有多嵌入了数据）

```
root@kali: ~# binwalk /var/yanhuo.jpg
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          JPEG image data, JFIF standard 1.01
35773       0x8BBB      Zip archive data, at least v2.0 to extract, compressed size: 60641, uncompressed size: 63570, name: "hahahahaha.jpg"
96557       0x1792D     End of Zip archive
```

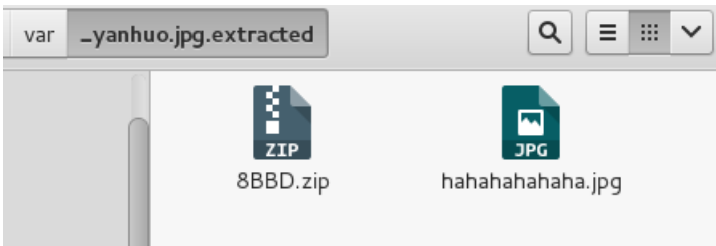
果不其然有一张hahahahaha.jpg的文件。

然后将其分离（-e参数）

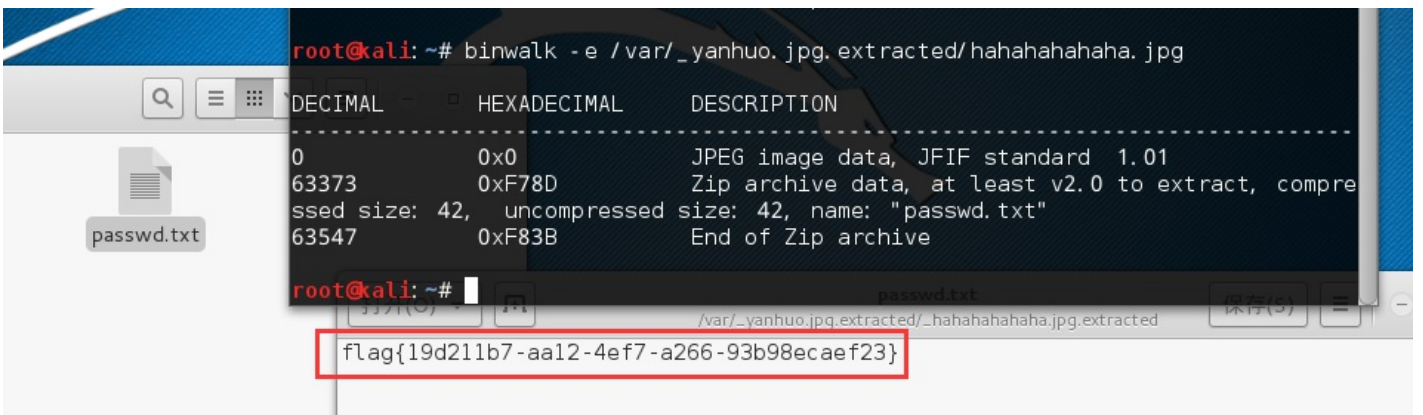


binwalk将分离出来的放在了生成出来的文件夹当中。

打开后发现还是图片。



然后又再分离hahahahaha.jpg得到flag.jpg



使用foremose分离

运行:foremost -v -i 图片路径 -o wzx

```
root@kali:~# foremost -v -i '/root/桌面/oddpic.jpg' -o wzx
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File
```

```
Foremost started at Wed Sep 21 16:40:06 2016
Invocation: foremost -v -i /root/桌面/oddpic.jpg -o wzx
Output directory: /root/wzx
Configuration file: /etc/foremost.conf
Processing: /root/桌面/oddpic.jpg
```

```
|-----|
File: /root/桌面/oddpic.jpg
Start: Wed Sep 21 16:40:06 2016
Length: 182 KB (186481 bytes)
```

Num	Name (bs=512)	Size	File Offset	Comment
0:	00000000.jpg	155 KB	0	
1:	00000310.jpg	27 KB	158792	

```
*|
Finish: Wed Sep 21 16:40:06 2016
```

```
2 FILES EXTRACTED
```