图片隐写分离

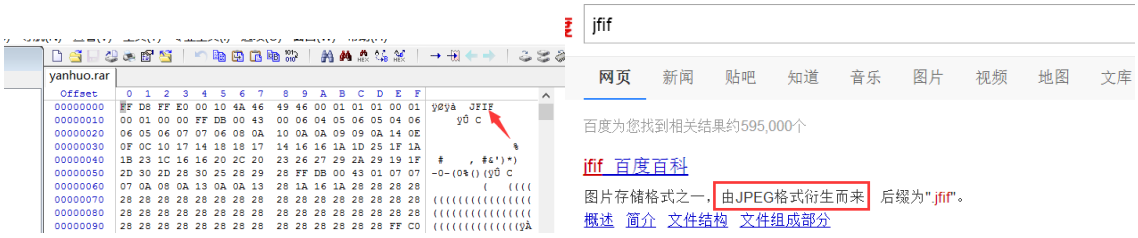
转载

aiquan9342 于 2017-10-04 23:32:00 发布 1536 收藏 1
原文链接：http://www.cnblogs.com/xishaonian/p/7628051.html
版权
提供下载:https://files.cnblogs.com/files/xishaonian/yanhuo.rar

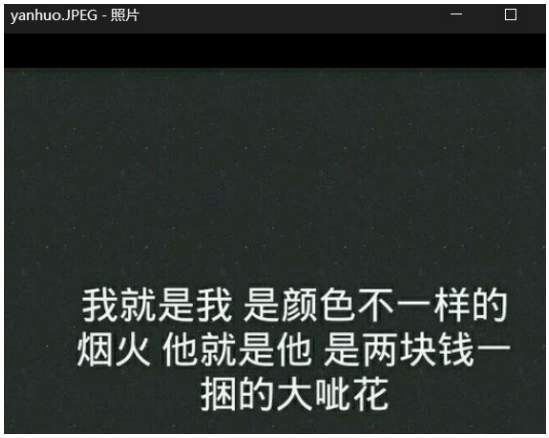
工具:用

> bindwalk
>
> foremost

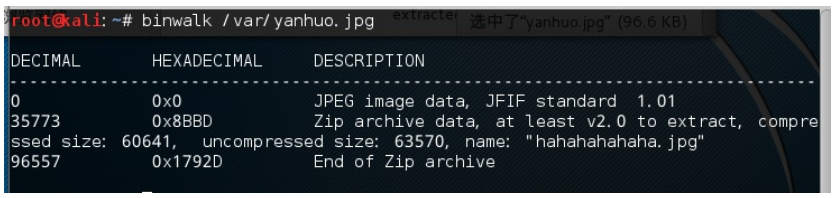
得到的时候是rar格式的,首先先判断一下其是否格式正确,直接丢Winhex查看发现是JFIF即为图片格式。



然后改为jpge之后图片显示正常

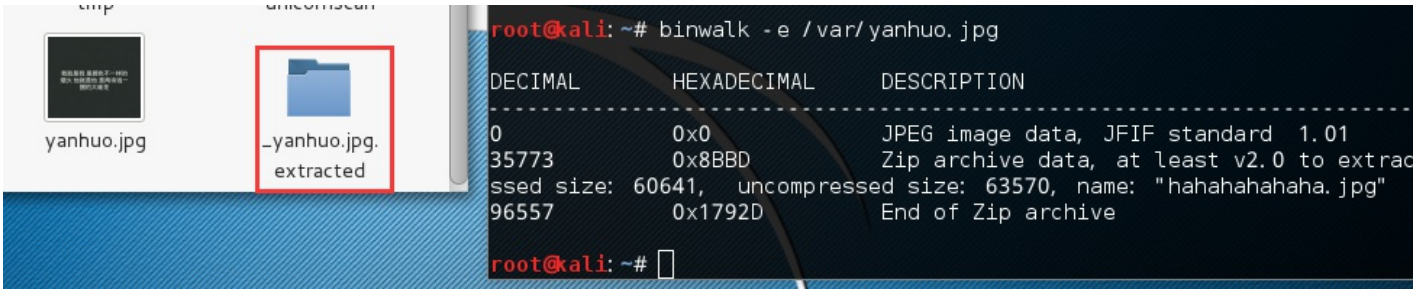


然后使用kali下的binwalk检测是否嵌入了数据（其实得到rar的时候直接打开里面就有一张hahaha.jpg的图片但是直接解压是失败的。心想就有多嵌入了数据）



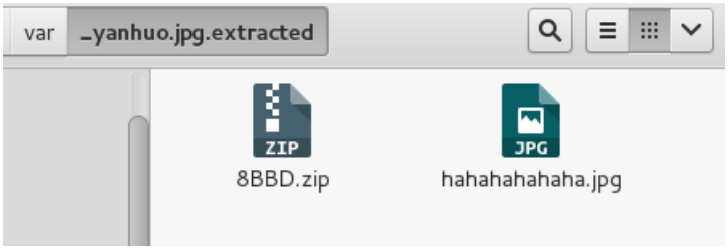
果不其然有一张hahahaha.jpg的文件。

然后将其分离（-e参数）

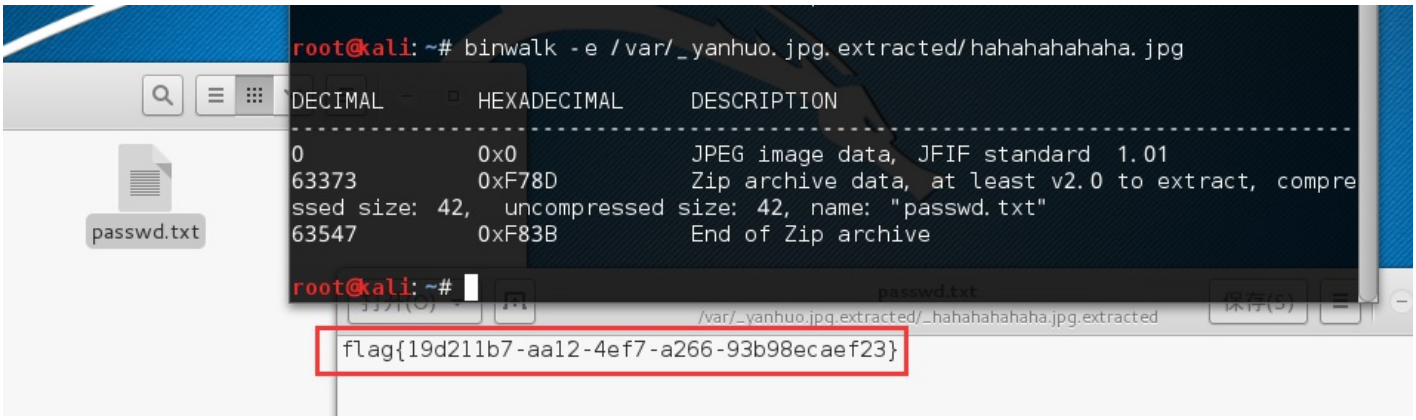


binwalk将分离出来的放在了生成出来的文件夹当中。

打开后发现还tmd是图片。

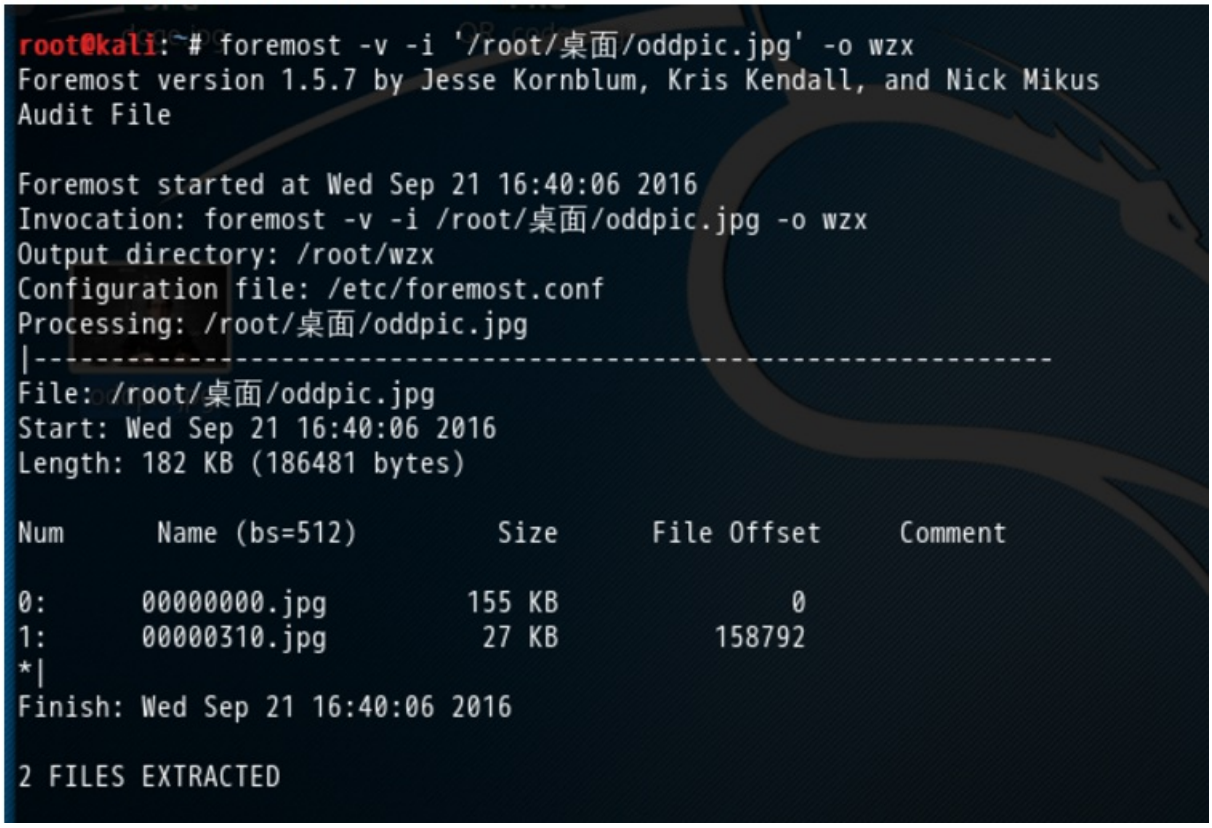


然后又再分离hahahahaha.jpg得到flag.jpg



使用foremose分离

运行:**foremost -v -i 图片路径 -o wzx**



转载于:https://www.cnblogs.com/xishaonian/p/7628051.html