linux隐写文件剥离,杂项的基本解题思路(1)——文件操作隐写、图片隐写

转载

weixin_39997443 于 2021-04-30 10:20:15 发布 122 收藏 1
文章标签： linux隐写文件剥离

文件操作隐写

图片隐写

压缩文件处理

流量取证技术

文章本来是分成4部分的，但是前两部分何在一起写了也就没有分开，所以干脆就只分了两部分

文件基本类型的识别

一、kail 下

file 文件名

```
root@kali:~/Desktop# file 倒立屋
倒立屋: PNG image data, 649 x 487, 8-bit/color RGB, non-interlaced
root@kali:~/Desktop#
```

原理就是识别文件文件头

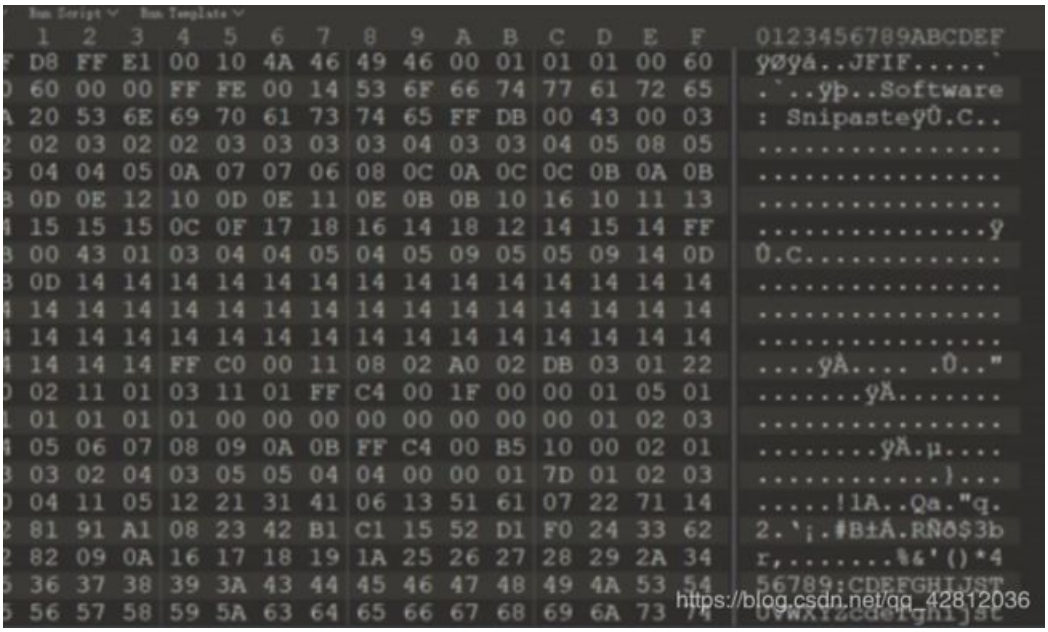
比如这个软件：

二、WinHex

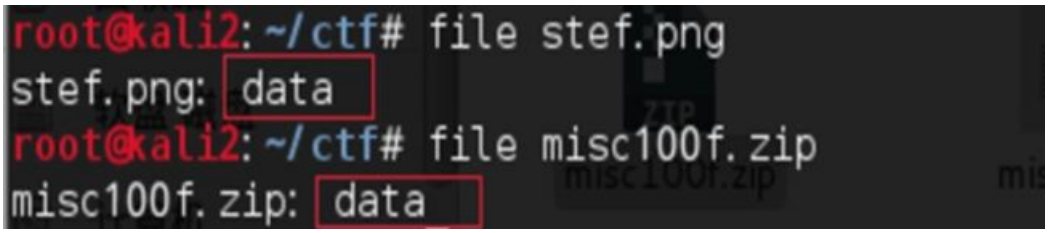
常见的文件头类型如图所示

文件类型	文件头
JPEG (jpg)	FFD8FFE1
PNG (png)	89504E47
GIF (gif)	47494638
TIFF (tif)	49492A00
Windows Bitmap (bmp)	424DC001
ZIP Archive (zip)	504B0304
RAR Archive (rar)	52617221
Adobe Photoshop (psd)	38425053

通过winhex分析能得到16进制和ascii, flag可能就在右边ascii区头部或尾部。



三、文件头残缺、错误



只告诉说是一个data文件；

这时要进行修复：编辑文件头区域修改为正确的方式 。

文件分离操作

一、Binwalk 工具

用法：

分析文件：binwalk filename

分离文件: binwalk -e filename

：分离出的压缩包，通常会自动解压出来。

二、foremost

有时候binwalk -e 分离不出，则用 foremost

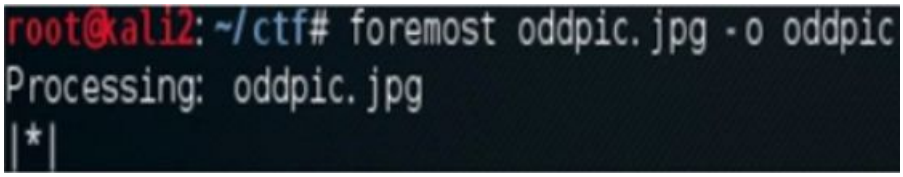
我一直都是binwalk查看，然后foremost分离

方法

foremost 文件名 -o 输出目录名

直接 foremost 文件名

也会自动生成文件夹输出到当前目录下

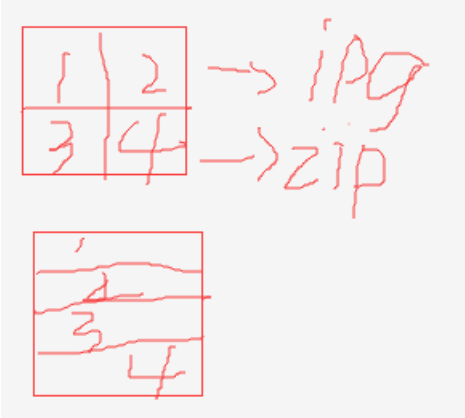


三、dd

前两个工具都是自动分离，有些题目复杂，如果都分离不出，可以使用dd实现文件手动分离。

单纯的题目：文件一部分是jpg,一部分是zip

复杂的题目：文件混杂，jpg和zip混合



图二上 1324的文件排列顺序，两种文件混合

假设有个 1.txt 文件内容123456789abcdefg。

格式：

dd if=源文件 of=目标文件名 bs=1 skip=开始分离的字节数

参数说明：

if=file #输入文件名，缺省为标准输入

of=file #输出文件名，缺省为标准输入

bs=bytes #同时设置读写快的大小为bytes，可代替ibs和obs

skip=blocks #从输入文件开头跳过blocks个块后再开始辅助。

四、winhex

除了dd，还可以使用winhex手动分离，将目标文件拖入winhex中，找到要分离的部分，点击复制

五、010Editor

选中-右键选择selection–save selectionb.

有的题目给了一个txt文件 打开是16进制文段，010Editor打开查看文件头，找出文件类型，另存为正确文件类型即可。

文件合并

一、Linux下的文件合并

使用场景：Linux下，通常对文件名相似的文件要进行批量合并

格式 ：cat 合并的文件 > 输出的文件

有md5可以进行完整性校验的话

>> md5sum 文件名

二、windows下的文件合并

格式：copy /B 合并的文件(用加号连接，Linux空格即可) 合并后的文件名

copy /B gif01+gif02 2.gif

完整性校验：

certutil -hashfile 2.gif md5

：这些步骤大都只是一个解题步骤，文件合并了还打不开，可以查看文件头是否错误。

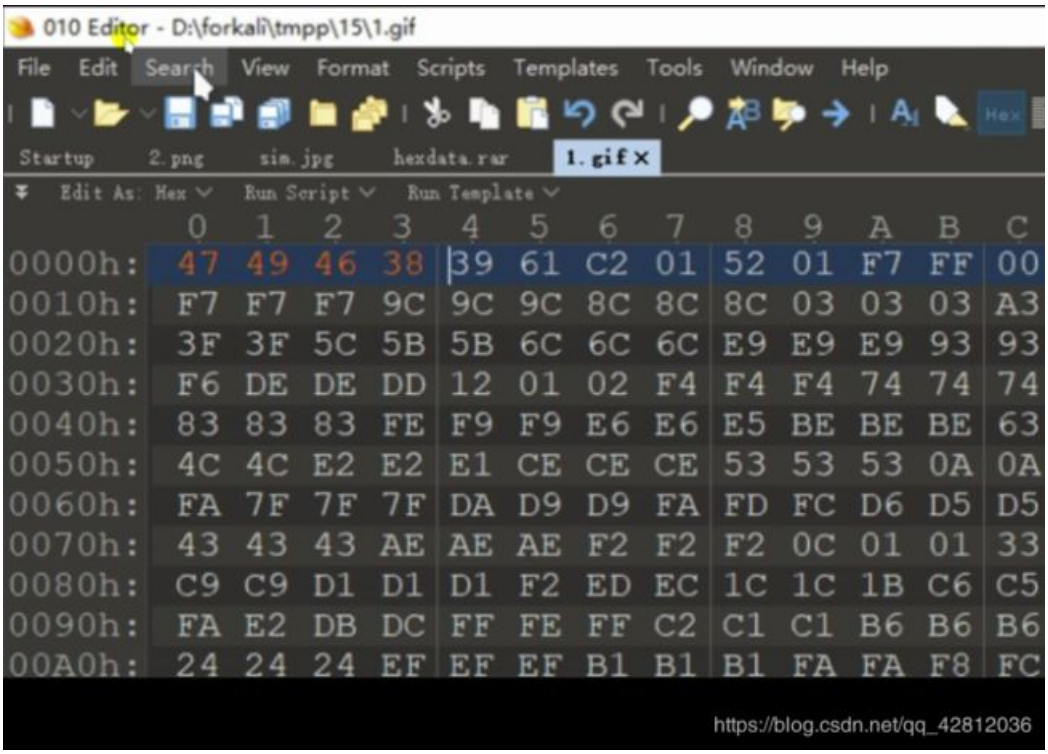
文件内容隐写

通常KEY以十六进制的形式写在文件中，通常在文件的开头和结尾部分如果在文件中间部分，通常搜索关键字KEY或者flag来查找隐藏内容。

window下

一、Winhex/010editor

二、Notepad++


010 Editor - D:\forkali\tmpp\15\1.gif
File Edit Search View Format Scripts Templates Tools Window Help
Startup 2.png sim.jpg hexdata.rar 1.gif
Edit As: Hex Run Script Run Template
0 1 2 3 4 5 6 7 8 9 A B C
0000h: 47 49 46 38 39 61 C2 01 52 01 F7 FF 00
0010h: F7 F7 F7 9C 9C 9C 8C 8C 8C 03 03 03 A3
0020h: 3F 3F 5C 5B 5B 6C 6C 6C E9 E9 E9 93 93
0030h: F6 DE DE DD 12 01 02 F4 F4 F4 74 74 74
0040h: 83 83 83 FE F9 F9 E6 E6 E5 BE BE BE 63
0050h: 4C 4C E2 E2 E1 CE CE CE 53 53 53 0A 0A
0060h: FA 7F 7F 7F DA D9 D9 FA FD FC D6 D5 D5
0070h: 43 43 43 AE AE AE F2 F2 F2 0C 01 01 33
0080h: C9 C9 D1 D1 D1 F2 ED EC 1C 1C 1B C6 C5
0090h: FA E2 DB DC FF FE FF C2 C1 C1 B6 B6 B6
00A0h: 24 24 24 EF EF EF B1 B1 B1 FA FA F8 FC
https://blog.csdn.net/qq_42812036


Search View Format Scripts Templates Tools
Find... Ctrl+F
Find Next F3
Find Previous Ctrl+F3
Replace... Ctrl+R
Replace Next F4
Replace Previous Ctrl+F4
Find Strings...
Find in Files... Ctrl+Shift+F
Replace in Files... Ctrl+Shift+R
Goto... Ctrl+G
Goto Again Ctrl+Shift+G
Add/Edit Bookmark Ctrl+B
Toggle Bookmark Ctrl+F2

010Editor最下方的查找。

使用的工具Linux下的 kail有自带

window下的自行下载

Winhex

010editor

Notepad++