入门知识

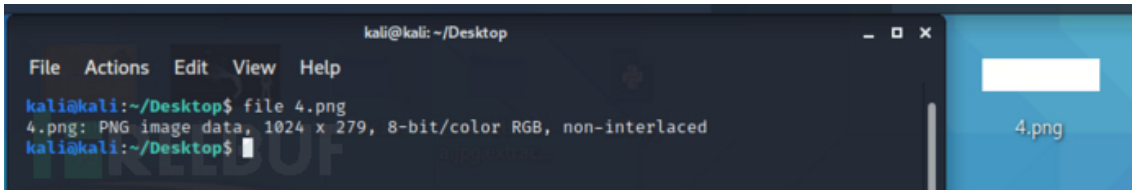
前言

有时候题目给的附件看起来是一个平平无奇的文件，但其有可能是若干个文件合并在一起或者是一个文件分离出来的文件。当对附件本身不好下手的时候，可以去检查一下它是否包含了其他含有线索的文件。

文件类型的识别

file命令

- file命令工具，是用来查看文件类型，能够得到一些没有后缀的文件。
- 命令：`file 4.png(得到的文件名字)`，根据情况判断可能的类型



可以看到该文件是.png格式的图，数据等信息，展现出来。

常见文件文件头和文件尾

常见的文件头（部分）：

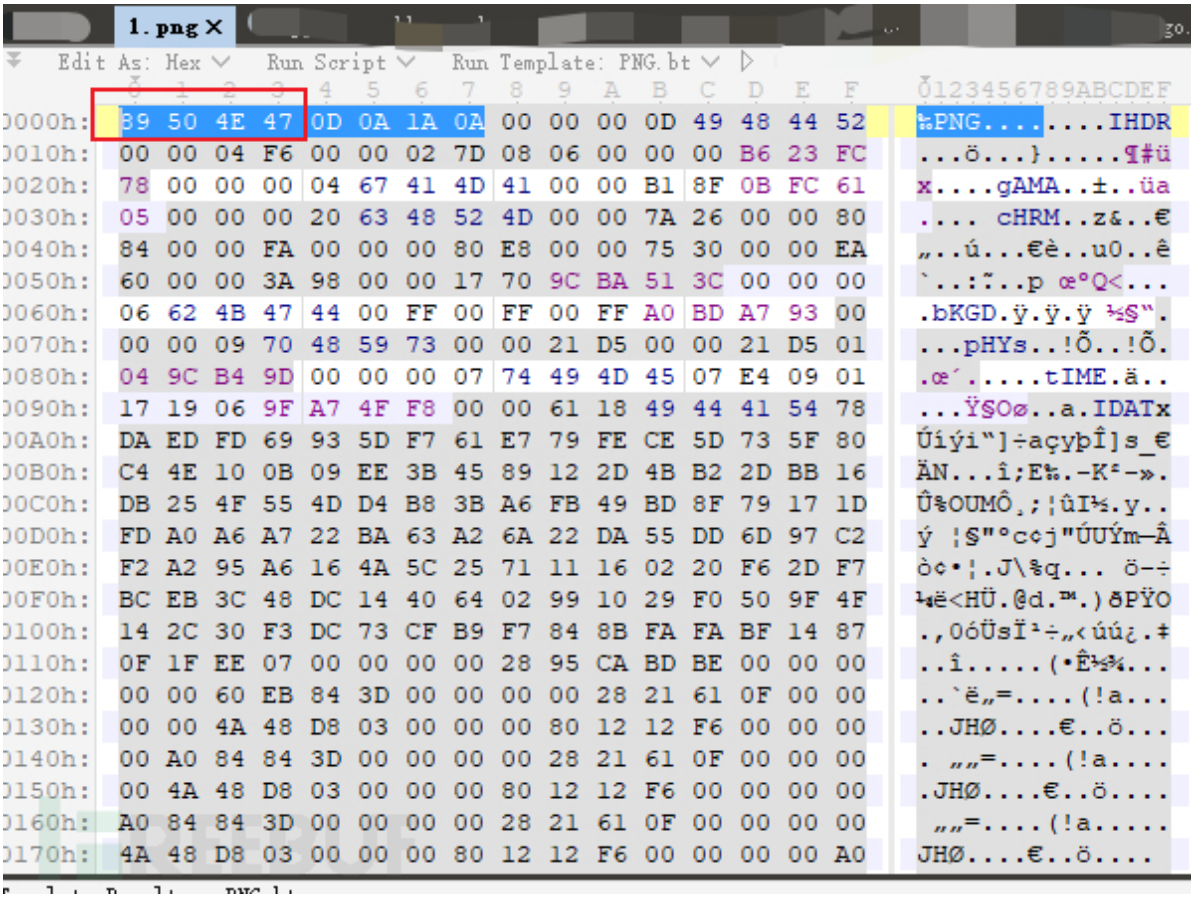
文件类型	文件头
JPEG(jpg)	FFD8FFE1
PNG(png)	89504E47
GIF (gif)	47494638
TIFF (tif)	49492A00
Windows Bitmap (bmp)	424DC001
ZIP Archive (zip)	504B0304
RAR Archive (rar)	52617221
Adobe Photoshop (psd)	38425053
Rich Text Format (rtf)	7B5C727466
XML (xml)	3C3F786D6C
Adobe Acrobat (pdf)	355044462D312E
Wave （wav)	57415645
pcap (pacp)	4D3C2B1A

没有后缀名的，可以查看文件尾部判断文件类型。

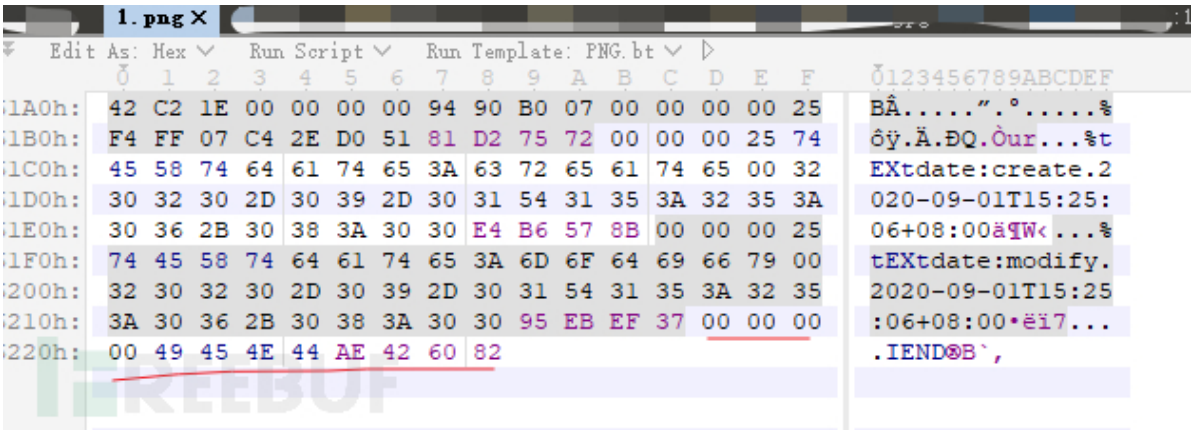
常见的文件尾部：

- zip文件尾部以一串504B0506开始
- rar文件以C 43DB00400700结尾
- JPG文件结尾的FFD9
- PNG文件 结尾为000049454E44AE426082
- Gif文件结尾为3B

例如1.png的图，用010打开，看一下文件头：



看一下文件尾部：



文件合并

linux环境文件合并

cat是linux系统下的一个能提取文件的内容的命令，使用cat命令将文件内容提取出来再导入目标文件。

命令如下：

```
# 将test1，test2，test3三个文件按从左到右顺序合并，输出book文件中
cat test1 test2 test3 > book
```

注意：cat是需要遵循顺序来获取文件内容的，所以再cat之前需要判断一下文件的先后顺序。

windows环境文件合并

copy命令。同上，从左到右的顺序合并，输出book.txt。

```
copy /B test1.txt+test2.txt+test3.txt book.txt
```

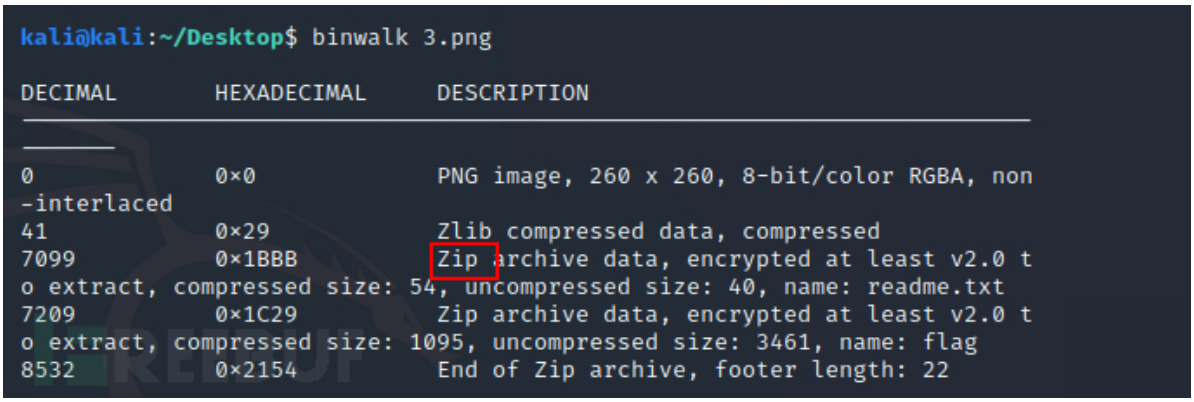
文件分离

binwalk

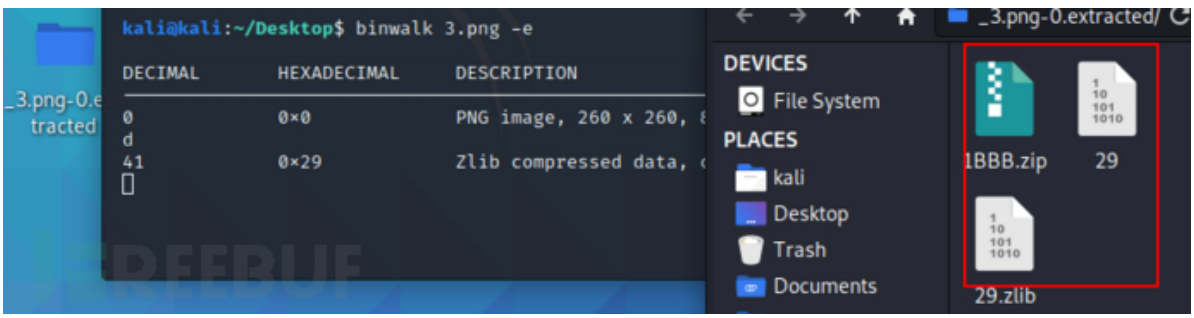
是一个自动提取文件系统，该工具可以自动完成指定文件的扫描，发现潜藏在文件中中所有可疑的文件类型以及文件系统。

```
# 命令
binwalk +file 扫描发现目标文件中包含的所有可识别的文件类型
binwalk +file -e 提取文件
```

提取成功的话则会生成一个文件名extracted目录，目录中存放的就是提取的文件。



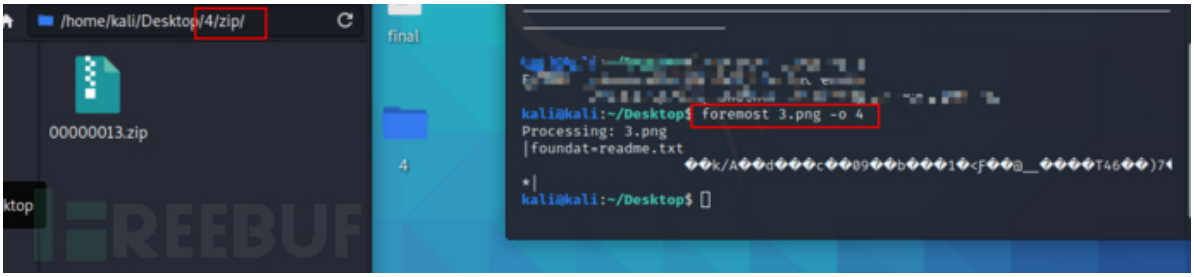
可以看到，3.png图片中存在一个压缩包，分离出来。

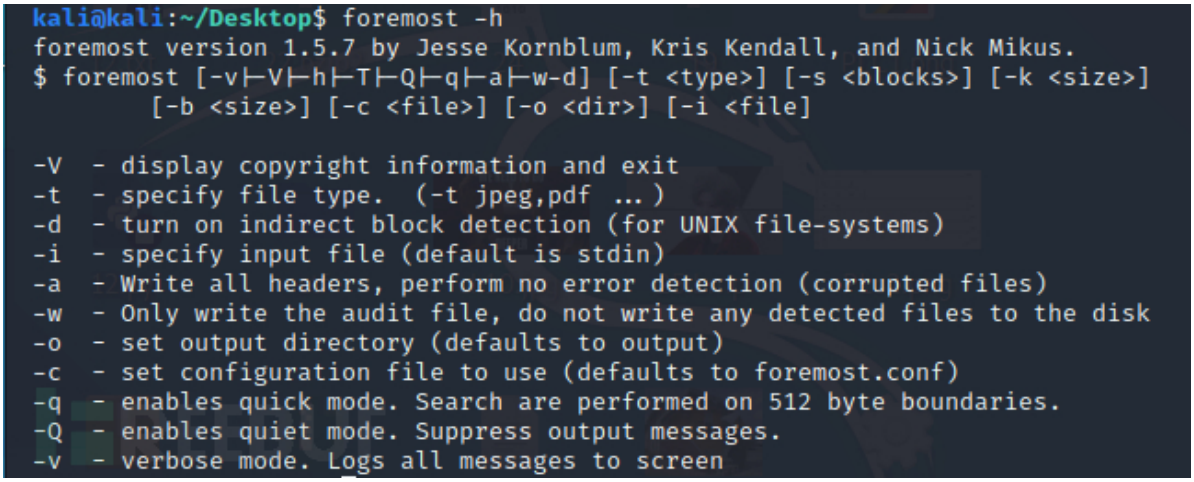


foremost

该工具通过分析不同类型的头、尾和内部数据结构，同镜像文件的数据进行比对，来还原文件。支持19中类型文件的恢复。用户还可以通过配置文件扩展支持其他文件类型。

```
# 命令
foremost +file -o 输出目录名
```





- -V --- 显示版权信息并退出
- -t --- 指定文件类型. (-t jpeg,pdf ...)
- -d --- 打开间接块检测 (针对UNIX文件系统)
- -i --- 指定输入文件 (默认为标准输入)
- -a --- 写入所有的文件头部, 不执行错误检测(损坏文件)
- -w --- 向磁盘写入审计文件，不写入任何检测到的文件
- -o --- 设置输出目录 (默认为./output)
- -c --- 设置配置文件 (默认为foremost.conf)
- -q --- 启用快速模式. 在512字节边界执行搜索
- -Q --- 启用安静模式. 禁用输出消息
- -v --- 详细模式. 向屏幕上记录所有消息

dd

该工具是自动化分离工具，用在当题目文件包含其他文件时，可以把其他文件分离出来的一款工具。

```
# 命令
dd if=源文件名 bs=1 skip=开始分离的字节数 of=目标文件名
```

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，缺省为标准输出
- bs=bytes #同时设置读写块的大小为bytes，可代替ibs和obs
- skip=blocks #从输入文件开头跳过blocks个块后再开始复制

常用工具

- 010 Editor
- WinHex
- cat
- copy
- binwalk
- foremost
- dd

实战案例

CTF中的文件分离 & 文件合并*coderge*的*51CTO*博客的技术博客51CTO博客

参考资料

CTFer成长之路-Nu1L战队-Misc部分