

图片隐写及BinWalk识别隐藏数据

原创

平静愉悦 于 2021-03-31 17:06:17 发布 615 收藏 1

分类专栏: 笔记 文章标签: [python](#) [编程语言](#) [信息安全](#) [数据分析](#) [数据挖掘](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/aaahtml/article/details/115355122>

版权



[笔记 专栏收录该内容](#)

261 篇文章 5 订阅

订阅专栏

最近学习了图片隐写与音频隐写, 这次来一个组合拳练习练习。

首先对内嵌文件数据分析打开stego4.jpg文件, 图片里面显示了一段文字MUSTNOTHACK, 其他似乎没有什么有用的信息。

我们用binwalk看一下执行python binwalk命令来对stego4.jpg文件进行处理, 如图所示:

```
C:\ 命令提示符
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

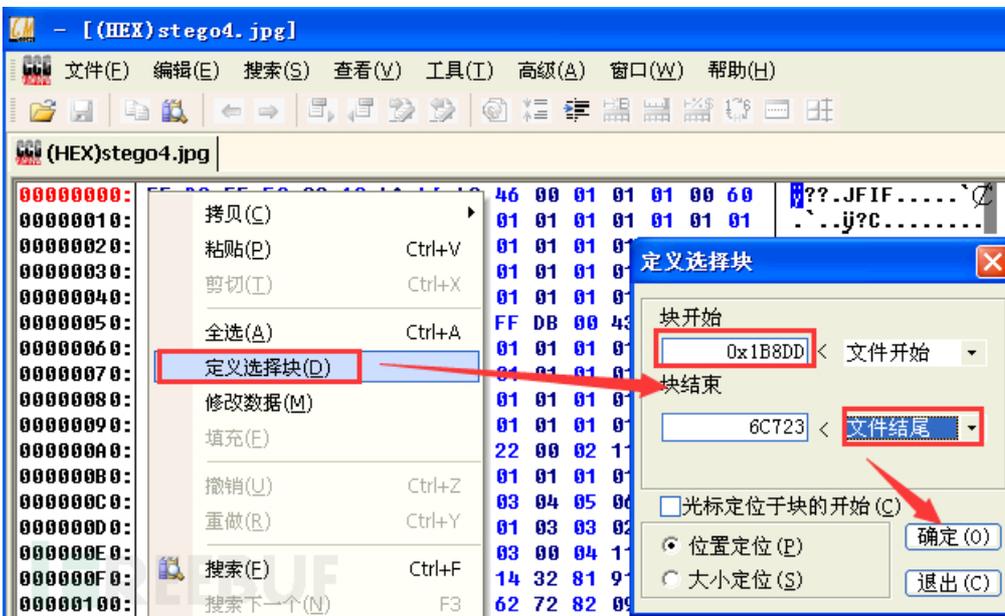
C:\Documents and Settings\Administrator>cd c:\Python27\Scripts\
C:\Python27\Scripts>python binwalk c:\Stegano\4\stego4.jpg

DECIMAL      HEXADECIMAL     DESCRIPTION
-----
112861       0x1B8DD         RAR archive data, first volume type: MAIN_HEAD
443990       0x6C656         7-zip archive data, version 0.3

C:\Python27\Scripts>
```

可以看到里面多了一个7-zip, 这说明软件分析出来这个图片里面还有一个压缩包。那我们怎么提取出来呢?

从BinWalk的分析结果可以看出, 其中RAR压缩包的文件偏移地址开始与0x1B8DD, 这里我们使用C32Asm将从0x1B8DD开始的所有数据提取出来。打开桌面上的C32Asm工具, 选择“文件”、“打开十六进制文件”载入C:\Stegano\4\stego4.jpg文件, 然后右键选择“定义选择块”, 填入数据块的起始地址为0x1B8DD, 结束地址选择“文件结尾”, 单击确定就选中数据块了, 右键复制数据, 然后新建一个十六进制文件, 将原有的数据替换为复制的数据, 保存即可得到压缩包文件。操作过程如图所示:



这样就得到了一个RAR压缩包文件了。

这个压缩包里面解压出来的flag.7z居然需要密码，p3文件也被隐藏起来了，在cmd中通过dir /AH命令就可以看到，使用attrib -H DO_NOT_LOOKING_HERE.mp3命令去除MP3文件的隐藏属性，如下图所示：

```

C:\> 命令提示符
C:\Stegano\4\stego>dir /AH
驱动器 C 中的卷没有标签。
卷的序列号是 5C2D-E95C

C:\Stegano\4\stego 的目录
2012-12-04  21:21          331,005 DO_NOT_LOOKING_HERE.mp3
             1 个文件          331,005 字节
             0 个目录 14,223,200,256 可用字节

C:\Stegano\4\stego>attrib -H DO_NOT_LOOKING_HERE.mp3
  
```

播放MP3文件并不能听到什么有用的信息，我们尝试使用MP3Stego检查文件中是否隐藏了数据，使用MP3Stego的时候需要指定一个密码，这里使用原始图片中显示的MUSTNOTHACK字符串。打开cmd命令提示符，首先切换到C:\tools\MP3Stego\目录，然后执行命令MP3StegoDecode.exe -P MUSTNOTHACK -X C:\Stegano\4\stego\DO_NOT_LOOKING_HERE.mp3，如图所示：

```

C:\> 命令提示符
C:\Stegano\4\stego>cd c:\tools\MP3Stego\
C:\tools\MP3Stego>MP3StegoDecode.exe -P MUSTNOTHACK -X C:\Stegano\4\stego\DO_NOT_LOOKING_HERE.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = 'C:\Stegano\4\stego\DO_NOT_LOOKING_HERE.mp3'  output file = 'C:\Stegano\4\stego\DO_NOT_LOOKING_HERE.mp3.pcm'
Will attempt to extract hidden information. Output: C:\Stegano\4\stego\DO_NOT_LOOKING_HERE.mp3.txt
the bit stream file C:\Stegano\4\stego\DO_NOT_LOOKING_HERE.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=3, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=single-ch, sblim=32, jsbd=32, ch=1
[Frame 791]Avg slots/frame = 417.434; b/smp = 2.90; br = 127.839 kbps
Decoding of "C:\Stegano\4\stego\DO_NOT_LOOKING_HERE.mp3" is finished
The decoded PCM output file name is "C:\Stegano\4\stego\DO_NOT_LOOKING_HERE.mp3.pcm"
  
```

之后我们提取出来一个txt文件，文件内容为INEVERASKEDABOUTTHIS!

把文本内容当成压缩密码输入，得到Flag为VERYEASYSSTEGO，即题目要求我们所要寻找的字符串。

在这里还是要推荐下我自己建的**Python学习Q群:705933274**，群里都是学Python的，如果你想学或者正在学习Python，欢迎你加入，大家都是软件开发党，不定期分享干货（只有Python软件开发相关的），包括我自己整理的一份2021最新的Python进阶资料和零基础教学，欢迎进阶中和对Python感兴趣的小伙伴加入！