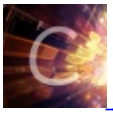
图片隐写及BinWalk识别隐藏数据

原创

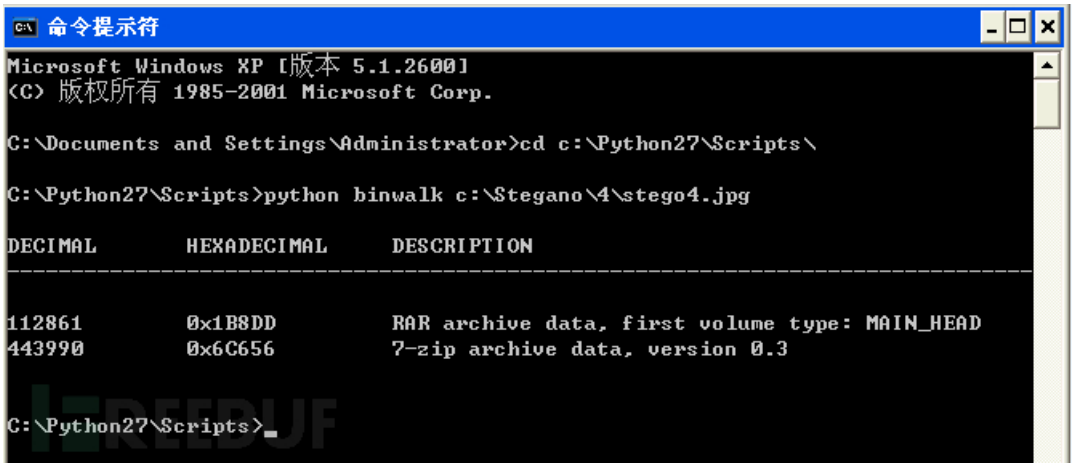
平静愉悦 于 2021-03-31 17:06:17 发布 615 收藏 1
分类专栏： 笔记 文章标签： python 编程语言 信息安全 数据分析 数据挖掘



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。

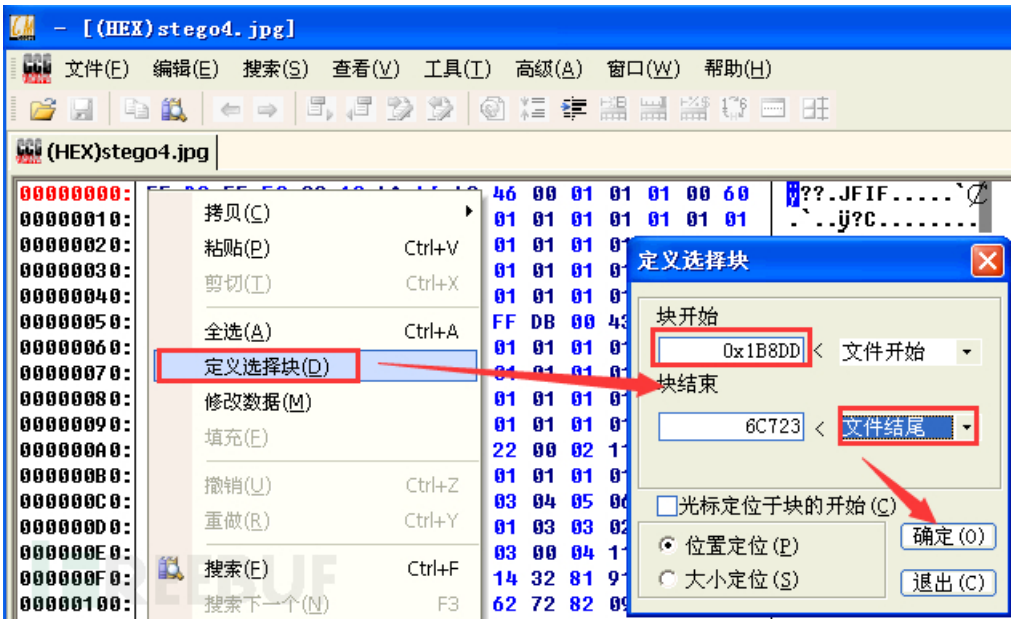
首先对内嵌文件数据分析打开stego4.jpg文件，图片里面显示了一段文字MUSTNOTHACK，其他似乎没有什么有用的信息。

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：



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？

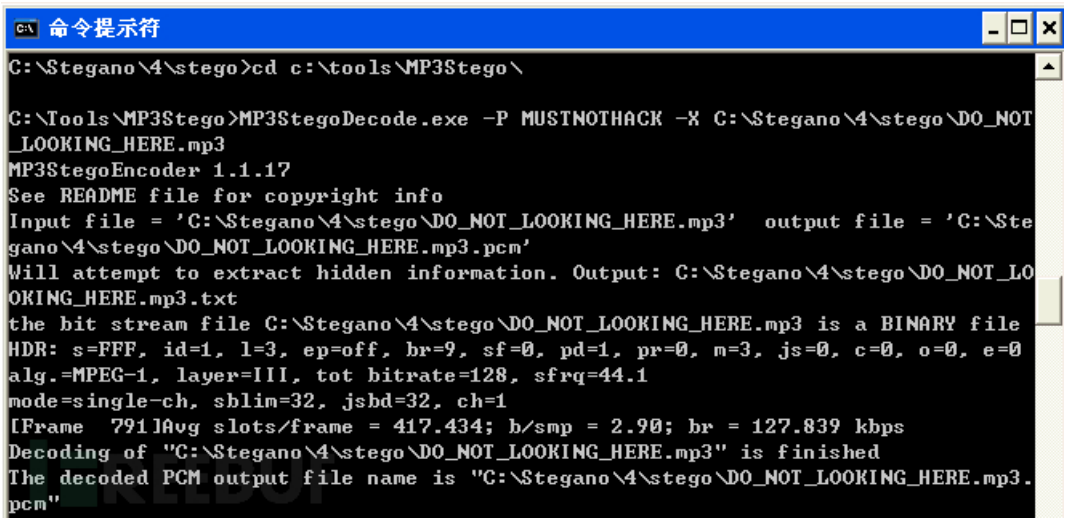
从BinWalk的分析结果可以看出，J其中RAR压缩包的文件偏移地址开始与0x1B8DD，这里我们使用C32Asm将从0x1B8DD开始的所有数据提取出来。打开桌面上的C32Asm工具，选择“文件”、“打开十六进制文件”载入C:\Stegano\4\stego4.jpg文件，然后右键选择“定义选择块”，填入数据块的起始地址为0x1B8DD，结束地址选择“文件结尾”，单击确定就选中数据块了，右键复制数据，然后新建一个十六进制文件，将原有的数据替换为复制的数据，保存即可得到压缩包文件。操作过程如图所示：



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：

播放MP3文件并不能听到什么有用的信息，我们尝试使用MP3Stego检查文件中使用隐藏了数据，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：



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VERYEASYSTEGO，即题目要求我们所要寻找的字符串。