CTF-MISC隐写总结

原创

Restart222 于 2021-08-23 10:35:08 发布 2600 收藏 22

分类专栏： CTF 文章标签： 网络安全

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/u011154053/article/details/119864063

版权


CTF 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

文章首发于freebuf 地址：https://www.freebuf.com/articles/others-articles/266884.html

本文仅就个人练习过的misc题目所涉及的知识点进行一定总结，如有错误或不足之处还请各位在评论处帮忙指出。

图片隐写

1.Exif信息隐藏

> **可交换图像文件格式**（英语：Exchangeable image file format，官方简称**Exif**），是专门为数码相机的照片设定的，可以记录数码照片的属性信息和拍摄数据。Exif信息是可以被任意编辑的，因此只有参考的功能。–《百度百科》

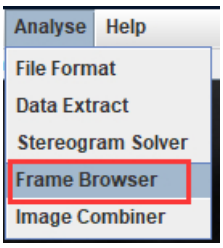
相关的exif查看器下载百度很多，这里就不贴链接了。

在linux下可以用**Exiftool**这个工具，相关教程请见https://blog.csdn.net/weixin_34393428/article/details/88679127

还有一种情况是直接在图片属性的**备注**里给出flag，这种情况可以用010editor或者winhex等工具打开图片搜索关键字如flag、ctf等查看。

2.Gif隐写

用神器Stegsolve可以一帧一帧查看，往往答案就隐藏在其中一帧



3.图片修复

1.文件头修复

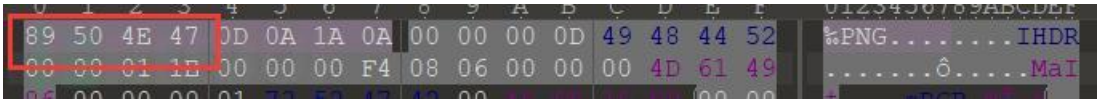
常见的图片格式文件头如下：

文件类型	文件头
JPEG(jpg)	FFD8FF
PNG(png)	89504E47
GIF(gif)	47494638
BMP	424DC001

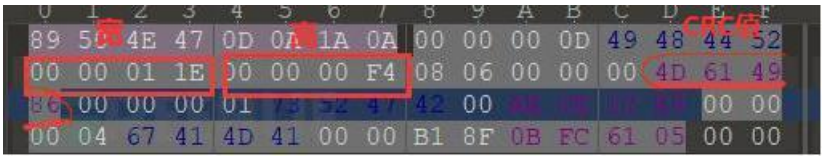
其他更多类型的文件头请看https://blog.csdn.net/qq_23100787/article/details/79040925

修复使用工具：010editor、winhex等

方法：以16进制的方式打开文件，在文件最开始添加相应的文件头

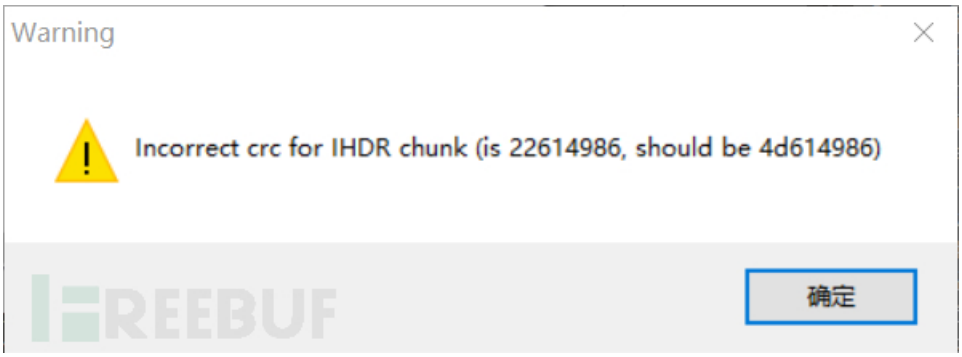


2.CRC校验修复



工具：tweakpng

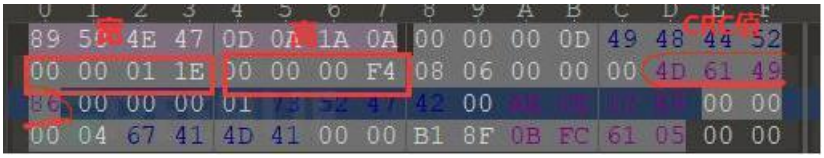
此时该图片的crc值未出错，用该工具打开该图片，不会报错，如果将crc值修改一下，这里我修改成22614986，再用tweakpng打开则会报错，并会提示该图片现有宽高应该得到的crc是多少



此时确保宽高是正确的情况下修改成正确的crc值即可。

3.宽高修复

对于png格式的图片，宽高的数据位置如图片所展示的那样



如果遇到简单一点的题目，可以直接尝试修改宽高，这里建议一般选择修改**高度**，一点点的改动即可。如果随意修改宽度一般都是会造成图像错误的。

> 一个简单的检测宽高是否有误的方法：在Windows下能打开的图片在linux下不能打开，就说明可能是宽高存在问题

最正确的方法则是通过crc值爆破宽高，给出大佬的脚本（记不得是哪里找到的了）

```
#!/usr/bin/env python
#-*- coding:UTF-8 -*-
import binascii
import struct
import os
crcbp = open("flag.png","rb").read()#填文件名
for i in range(1024):
    for j in range(1024):
        data = crcbp[12:16] + struct.pack('>i',i) + struct.pack('>i',j) + crcbp[24:29]
        crc32 = binascii.crc32(data) & 0xffffffff
        if crc32 == 0x4d614986 :#此处填CRC值
            print (i);
            print (j);
            print (hex(i),hex(j))
```

爆破出来后修改即可。

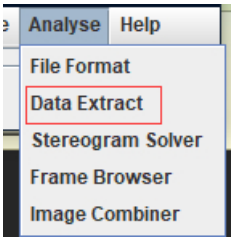
对于**jpg**格式的图片也存在宽高隐写，有师傅写的很详细了，此处不再赘述。有需要的朋友请移步：
https://blog.csdn.net/u010391191/article/details/80811813

4.LSB隐写

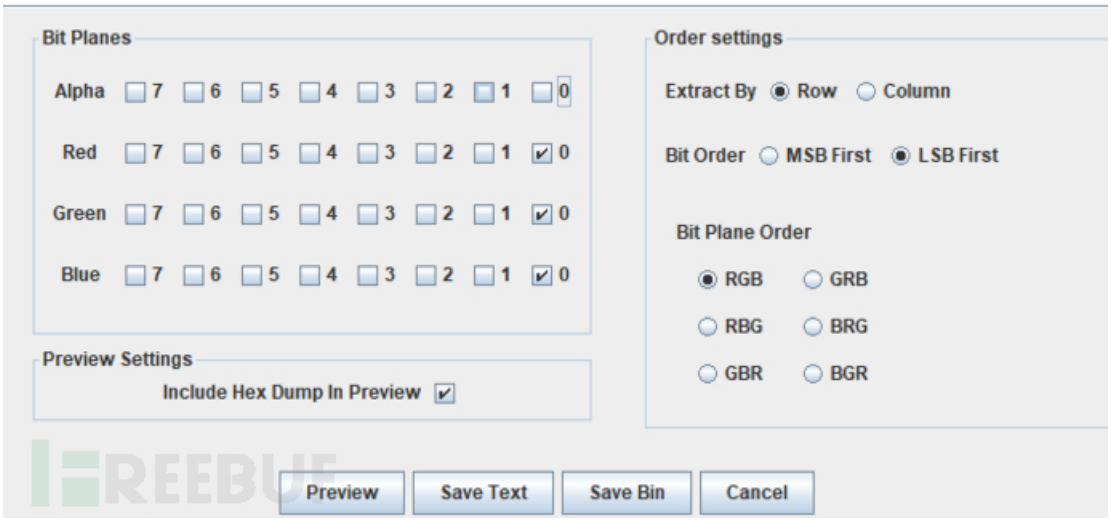
有关该隐写方式的原理网上已经有很多文章写过了，此处简单说一下做题方法。

工具：stegsolve（需要java环境）

用该工具打开图片后，点击



然后按照如下图片点击



最后点击preview。有时候点preview没用，需要点击最下面的save text或者save bin才能得出结果。这张图只是给出了示例，具体做题的时候可以多试一下和其他按键的组合。

还有一个比较简单的方法，用**zsteg**工具，需要kali里面在线安装：gem install zsteg

使用命令格式：zsteg filename

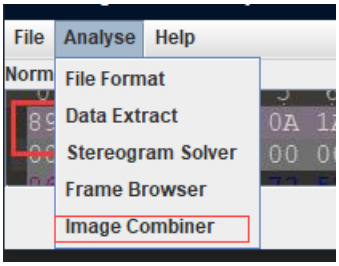
5.对于两张相同图片的隐写

1.盲水印

两张相同的图片首先考虑盲水印。使用方法及脚本移步https://github.com/chishaxie/BlindWaterMark

2.组合进行不同运算（and、or、xor等）

还是用stegsolve，点击



之后会再让你打开一张图片，此时需要注意两张图片的打开**顺序**不同，运算的结果也不同，实际操作中就需要各位来回试一下了

6.文件分离

常用工具：binwalk、formost、dd

binwalk：可快速分辨文件是否由多个文件合并而成，并将文件进行分离。如果分离成功会在目标文件的目录。

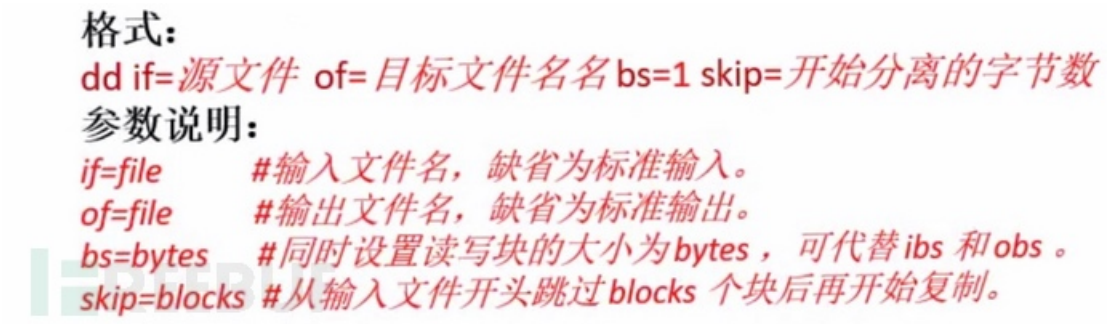
分析文件：binwalk filename

分离文件：binwalk -e filename

formost命令：formost filename -o 输出的目录名

因本人较懒，所以用了一个师傅说的方法，在用formost分离文件时很方便（不用敲命令）。参考链接：https://blog.csdn.net/qq_39368007/article/details/91129628

dd：当文件自动分离出错或者因为其他原因无法自动分离时使用



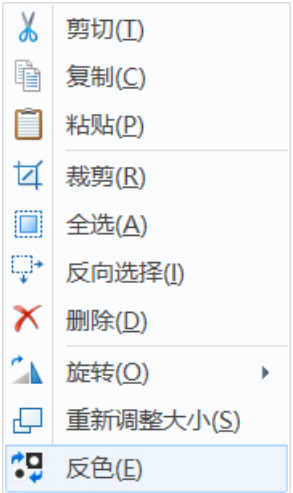
ps：如果一个工具分离不出来一定要多试几种，因为每种工具分离方法都有所差别，难免会出现分离不出来的情况。

7.二维码

取反色

有一道题就是将二维码颜色取反再扫描得出结果，记不得是哪里的了。具体操作可以用windows自带的画图工具，打开图片然后点击主页的选择

选中图片后右键选择反色



当你发现二维码的三个定位点是白色的时候，就说明需要进行反色操作了

8.一些其他常用工具介绍

针对jpg格式图片的隐写：

steghide

用法：

隐藏文件
steghide embed -cf [图片或wav文件载体] -ef [待隐藏文件]
steghide embed -cf 1.jpg -ef 1.txt

查看图片中嵌入的文件信息
steghide info 1.jpg

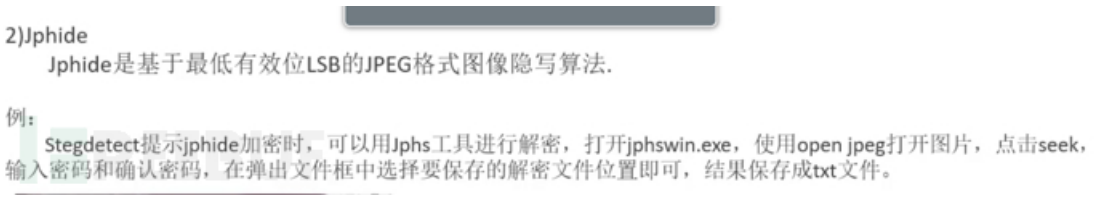
提取图片中隐藏的文件
steghide extract -sf 1.jpg

> stegdetect（可检测通过JSteg,JPHide,OutGuess,Invisible,F5,oppendX,Camouflage等隐写工具隐藏的信息）

用法：

> stegdetect xxx.jpg
> stegdetect -s 敏感度 xxx.jpgexi
> stegbreak（爆破密码）
> stegbreak.exe -r rules.ini -f password.txt p -c hide.jpg

jphide



silenteye（下面会有一定的介绍，用法基本一致)

音频隐写

1.针对mp3文件的隐写

将分别介绍以下工具：Audacity、MP3Stego

Audacity

一般得到题目文件，打开听到有杂音首选用这个工具打开。简单的题目就是在原音频中加入了一段摩斯密码，通过这个工具可以直接看出来

然后解密即可。

难一点的题目则是对音频进行频谱分析，比如这篇文章https://blog.csdn.net/vhkjhwbs/article/details/103036133谈到的lookme和用眼睛去倾听这两道题。

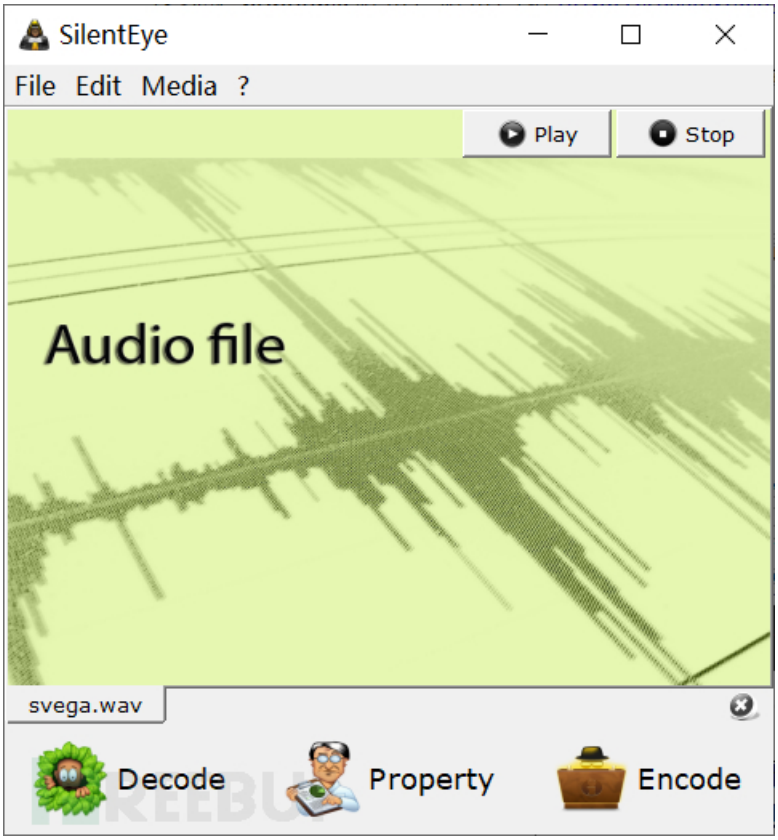
MP3Stego

如果mp3 文件听上去没有什么奇怪的地方，那么就试试用这个工具。教程：
https://blog.csdn.net/myloveprogrmming/article/details/52641916

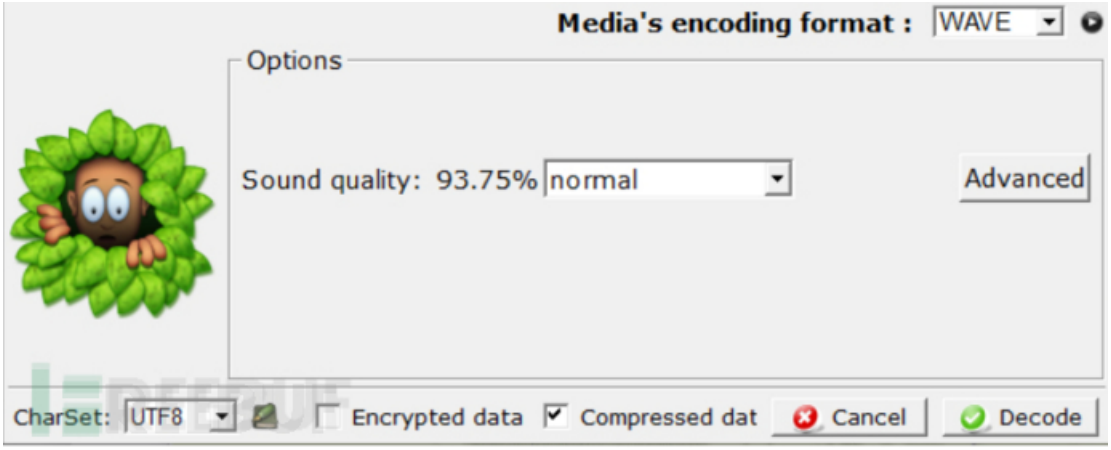
用这个工具会输入密码，有时候题目没有特别提示就可以试试弱口令，有时候甚至就是题目名字。

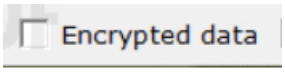
2.针对wav文件的隐写

工具：silenteye

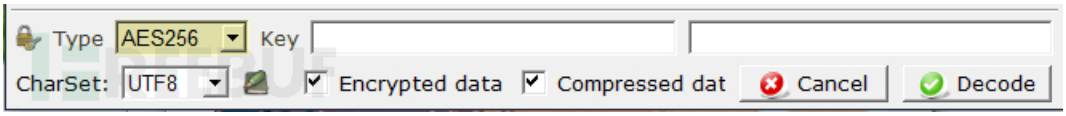


将文件拖到里面点击decode





简单的题目此时再点右下角的decode就能出结果，稍微绕点的就还需要 勾选这里输入密码，或者选择正确的type，看出题人的心思了~



当然，这个工具还能对**bmp**、**jpg**格式的隐写文件进行解密

视频隐写

1.针对mp4文件的隐写

工具：ffmpeg（一套可以用来记录、转换数字音频、视频，并能将其转化为流的开源计算机程序。）

详细使用教程介绍：https://blog.csdn.net/Allyli0022/article/details/78355248

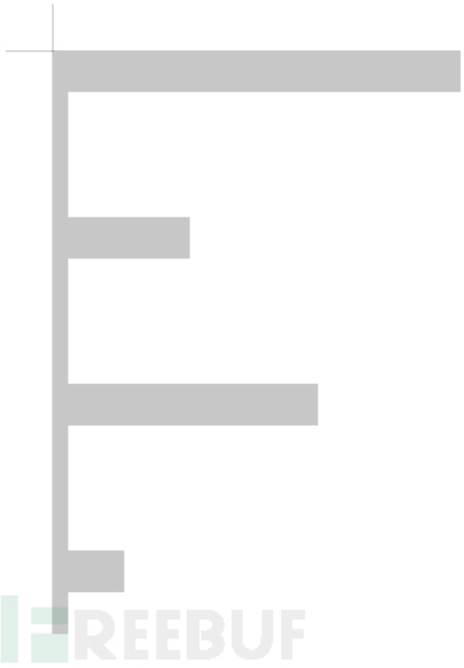
一般在题目中会插入一些图片，由于一下就闪过了所以需要用这个工具按帧提取出来，简单的题目往往这样就能做出来了。

文本隐写

1.word文档隐写

白色文字

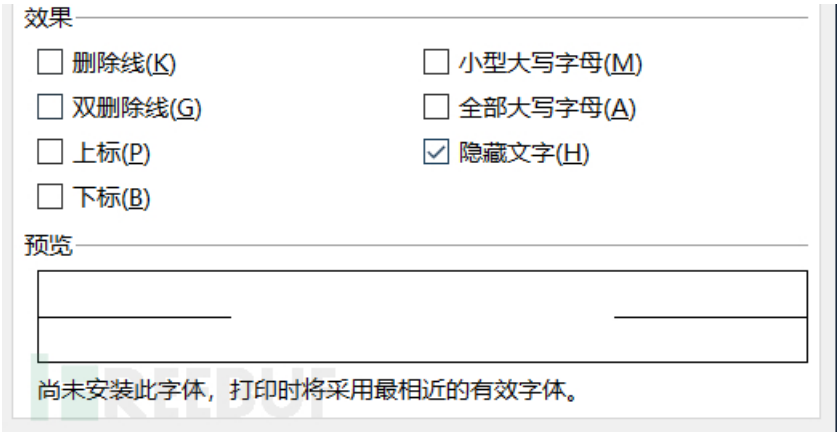
由于一般word文档都是白色为底色，所以如果文本字体设置的是白色，就看不出来有东西，这个时候可以试试**ctrl+a**，全选文字



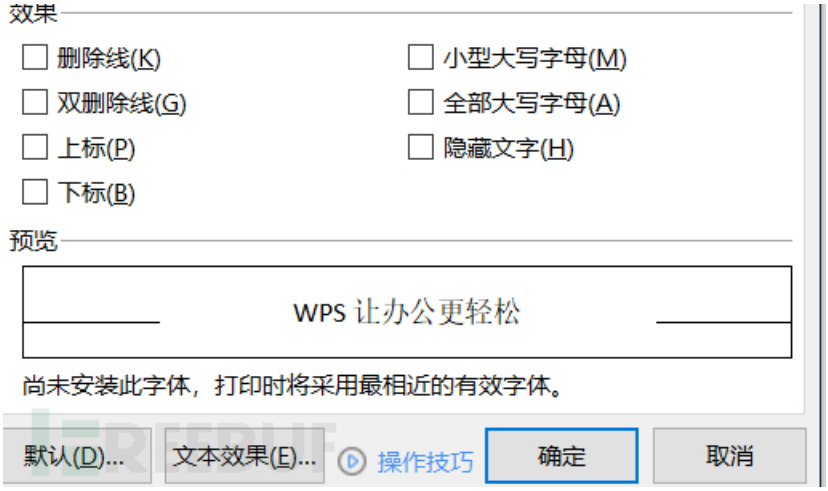
再把颜色改成其他颜色，就能看出来被隐藏的文字了

隐藏文字选项

在文本出右键鼠标，字体选项中有一处隐藏文字选项



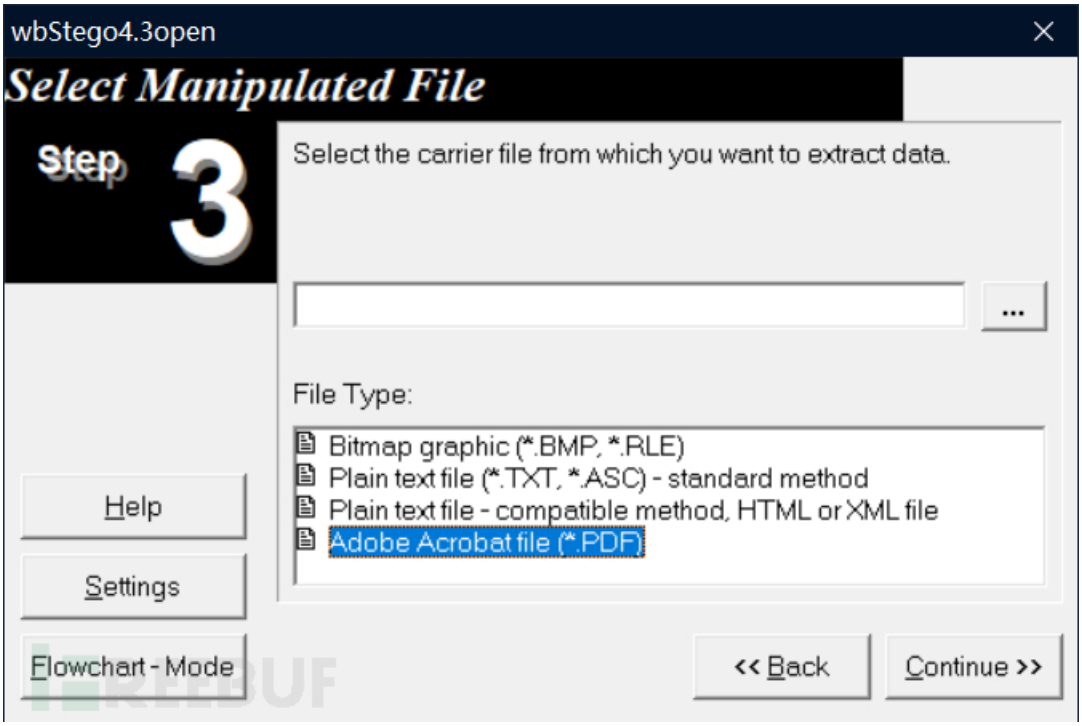
取消勾选后被隐藏的文字就出现了



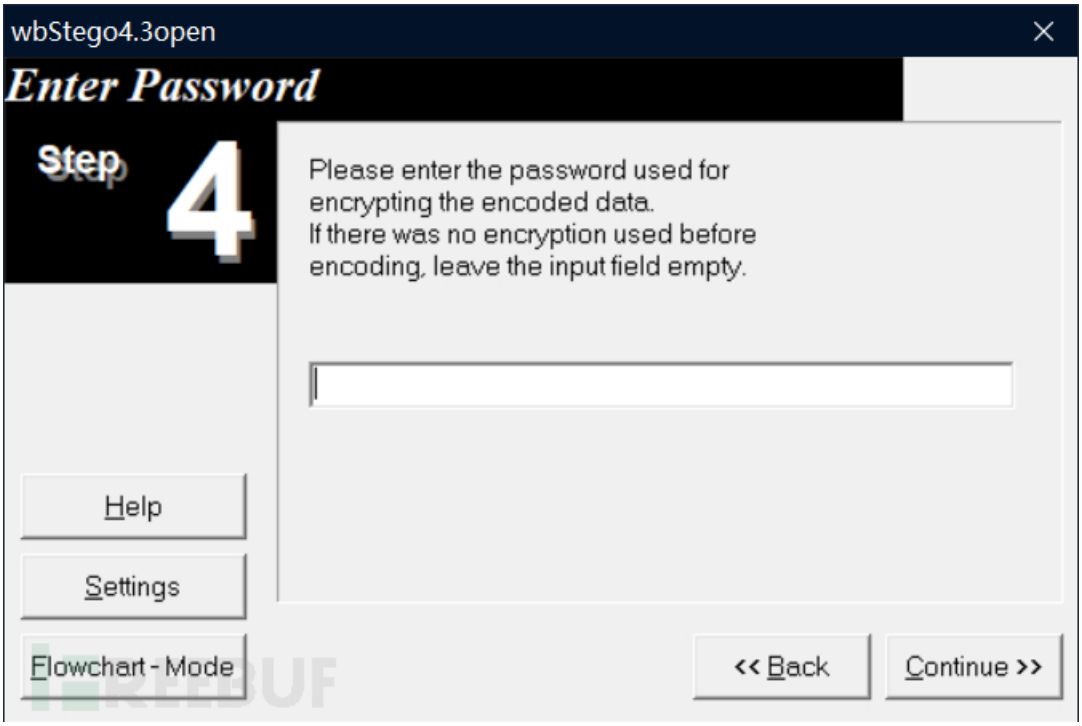
2.PDF隐写

wbs43open（可用于PDF、bmp等文件的隐写）

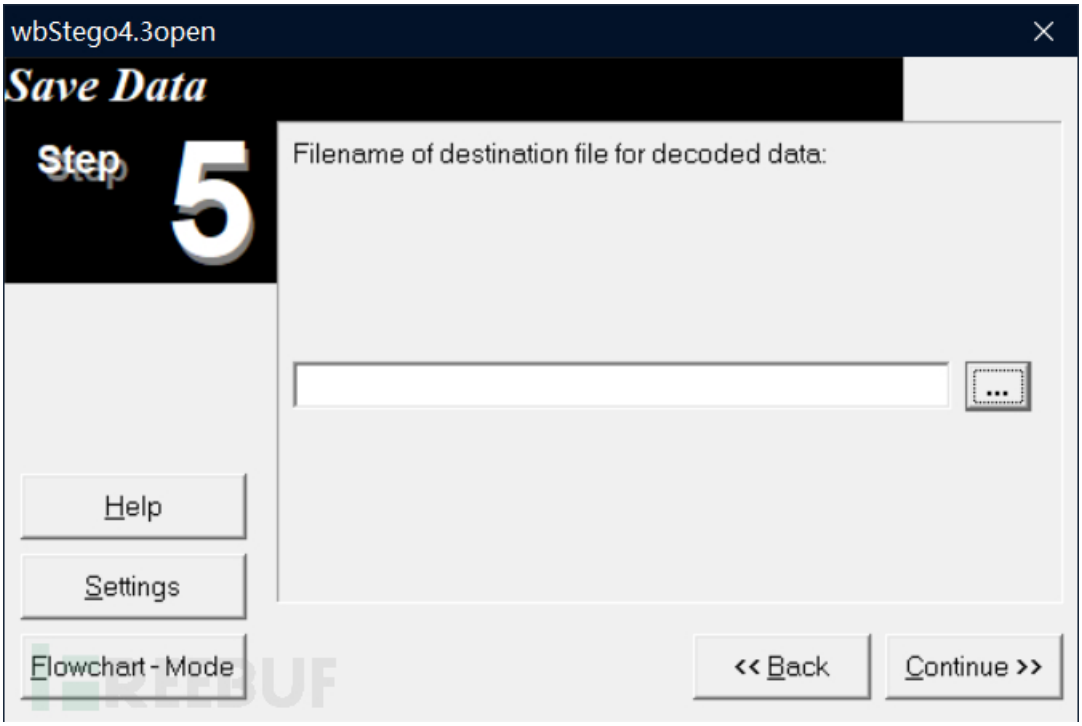
点击continue后会出现encode和decode，解密就选decode，然后第三步就选择文件类型和文件



第四步步设置密码，可以置空



第五步设置解密之后文件的存储路径及文件名



接下来第六步完成就行啦

要出这种类型的隐写题同样用这个工具也行。

3.html隐写

即snow隐写，需要告诉key，解密网站http://fog.misty.com/perry/ccs/snow/snow/snow.html

其他类型的隐写

1.base64隐写

Tr0y师傅的文章讲解的很详细，在这里就不过多介绍了，请移步https://www.tr0y.wang/2017/06/14/Base64steg/

2.零宽度字符隐写

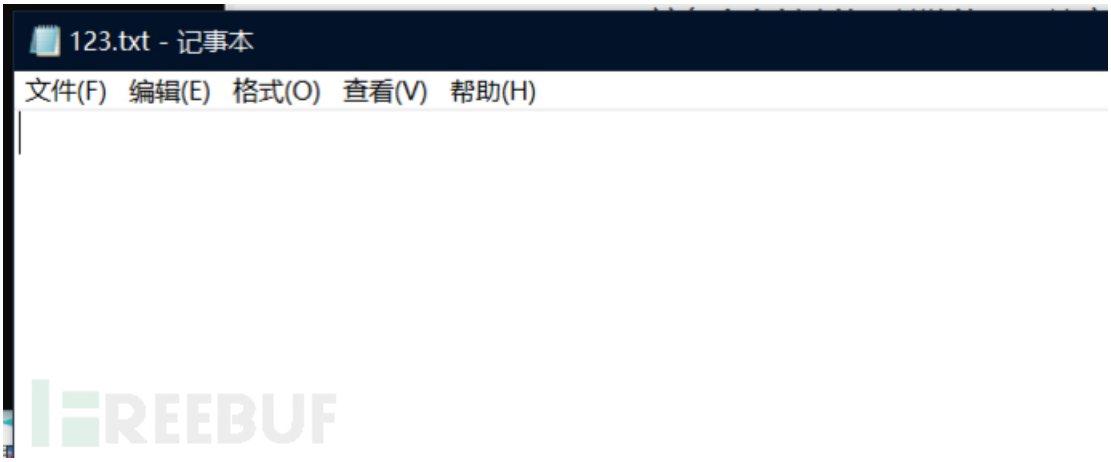
零宽度字符是一些不可见的，不可打印的字符。本文不做更多介绍，更详细的内容请移步http://www.ga1axy.top/index.php/archives/20/

3.ntfs数据流隐写

> NTFS（New Technology File System）是Windows NT内核的系列操作系统支持的、一个特别为网络和磁盘配额、文件加密等管理安全特性设计的磁盘格式，提供长文件名、数据保护和恢复，能通过目录和文件许可实现安全性，并支持跨越分区。 --《百度百科》

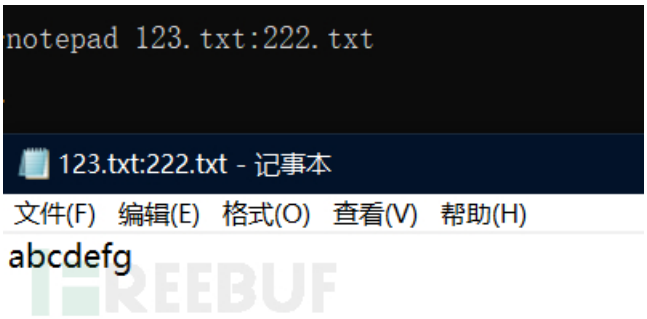
```
echo abcdefg>>123.txt:222.txt
```

该条命令创建的是单独的NTFS流文件，系统不可见的同时我们无法通过普通方法看到



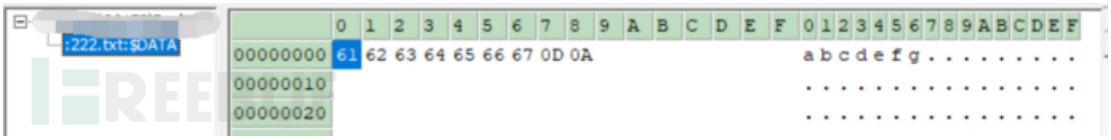
此时有两种方法，一种是命令：

```
notepad 123.txt:222.txt //这个命令只有自己已经知道NTFS流文件名的时候使用，局限性很大，同时失败几率大
```



另一种方法是用工具：NtfsStreamsEditor（右键以管理员身份运行）

点击快速查看



总结

有关隐写的内容非常非常多，本文内容主要针对misc新人，所以暂时先写这些，目的是为了让新手对一些常见的题目能够有一定思路去解决。很多时候misc做不出来（脑洞题除外）可能都是因为你不知道要用某某某工具，所以本文也针对一些题型介绍了一些工具。通过练习misc能对工具的使用有所了解，也能一定程度上学习各种文件类型的格式，但建议不要花过多时间在misc上，毕竟以后工作基本用不上，可以拿来放松的时候玩儿，有时候还是很有趣的！

如果本文有任何内容侵权，请及时联系我删除！

相关参考链接

> https://zhuanlan.zhihu.com/p/85825941
> https://www.jianshu.com/p/f5f0eb702dc3
> https://blog.csdn.net/qq_41079177/article/details/102964134