CTF隐写术

原创

TristTeng 于 2019-07-30 17:06:31 发布 289 收藏 1

分类专栏： CTF复盘 文章标签： CTF 隐写术

本文链接：https://blog.csdn.net/qq_43145355/article/details/97795299

CTF复盘 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

CTF之隐写术：小苹果

首先熟悉一下题目：

flag格式: CTF{}

解题链接： http://ctf5.shiyanbar.com/stega/apple.png

下载后得到：

扫描中国结中的二维码得到

```
\u7f8a\u7531\u5927\u4e95\u592b\u5927
\u4eba\u738b\u4e2d\u5de5
```

可以看出这是经过Unicode编码得到的，解码后得到：

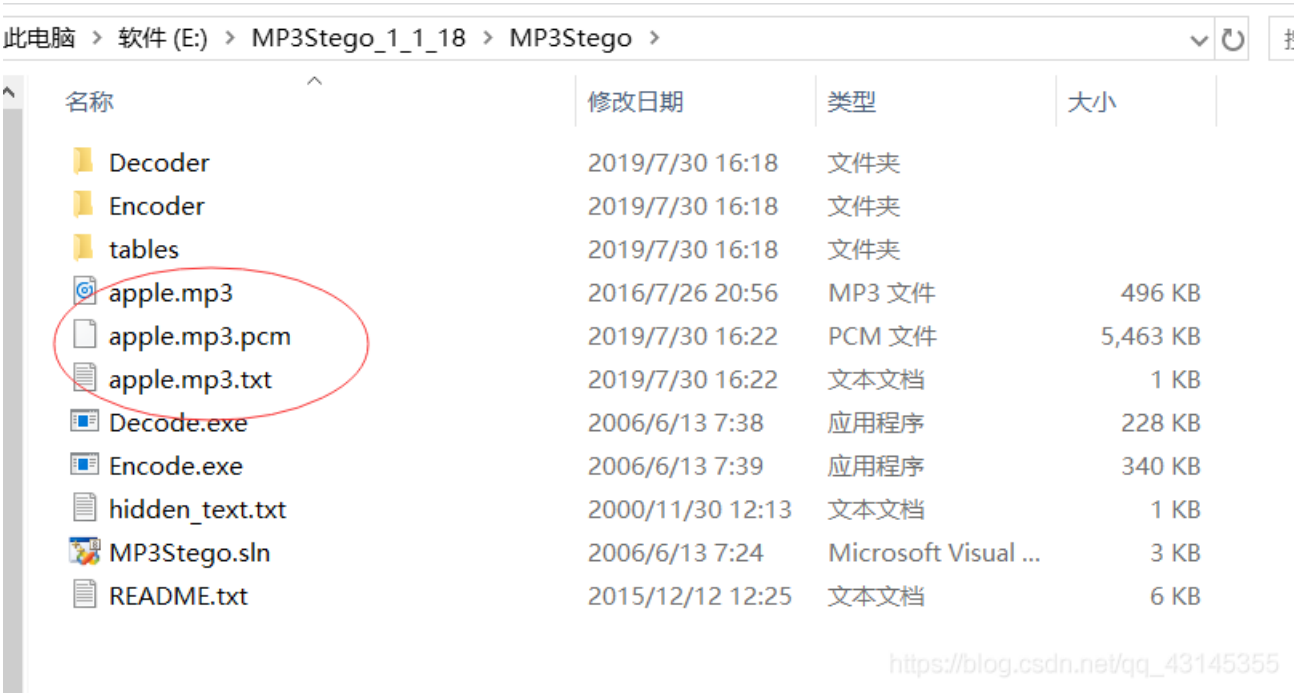
\u7f8a\u7531\u5927\u4e95\u592b\u5927\u4eba\u738b\u4e2d\u5de5

羊由大井夫大人王中工

说来惭愧，看到解码后的我是一脸懵逼的（这是啥东西？）经大神指点后掌握了一个新知识点（**划重点！**）
当铺密码：一种将中文和数字进行转化的密码，算法相当简单:当前汉字有多少笔画出头，就是转化成数字几（来源百度百科）
所以上面的文字经当铺解密后得到：9158753624。当解到这一步时并不清楚这个密码有什么作用，于是暂且放到一边。
把目光回到下载的png中，binwalk走一波发现里面包含一个压缩包（可以修改文件后缀名为zip),解压后得到apple.mp3，放到Audacity中没有发现什么特别之处（原本以为会出现摩斯电码）；
换一条路：使用MP3stego（一款专门提取音频中隐藏文件的工具），使用的时候发现需要知道该文件的密码（该工具 -p参数后要跟文件密码），尝试将上面我们解出的密码带入其中，发现**成功从apple.mp3中提取出了几个文件！**

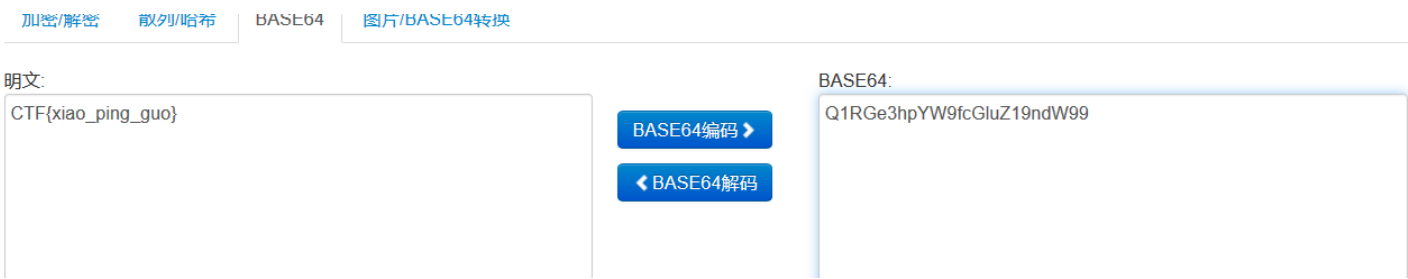
```
E:\MP3Stego_1_1_18\MP3Stego>E:\MP3Stego_1_1_18\MP3Stego\Decode.exe -X apple.mp3 -P 9158753624
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = 'apple.mp3'  output file = 'apple.mp3.pcm'
Will attempt to extract hidden information. Output: apple.mp3.txt
the bit stream file apple.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=stereo, sblim=32, jsbd=32, ch=2
[Frame 1213]Avg slots/frame = 417.617; b/smp = 2.90; br = 127.895 kbps
Decoding of "apple.mp3" is finished
The decoded PCM output file name is "apple.mp3.pcm"

E:\MP3Stego_1_1_18\MP3Stego>_
```

打开

apple.mp3.txt得到：Q1RGe3hpYW9fcGluZ19ndW99
尝试使用Base64解码：



成功得到flag!

总结：收获之处在于掌握了当铺密码以及当遇到音频隐写术时，audacity没有效果，可采用MP3Stego检验音频中是否隐藏了文件。

MP3stego使用方法传送门：https://blog.csdn.net/myloveprogrmming/article/details/52641916