ctf中MISC之MP3等音频隐写

原创

最后d轻语 于 2017-08-25 12:56:14 发布 34310 收藏 42
分类专栏： ctf笔记 文章标签： mp3stego隐写 ctf音频文件常用解决方式 CTF中音频隐写总结 音频隐写binwalk ctf音频例题writeup

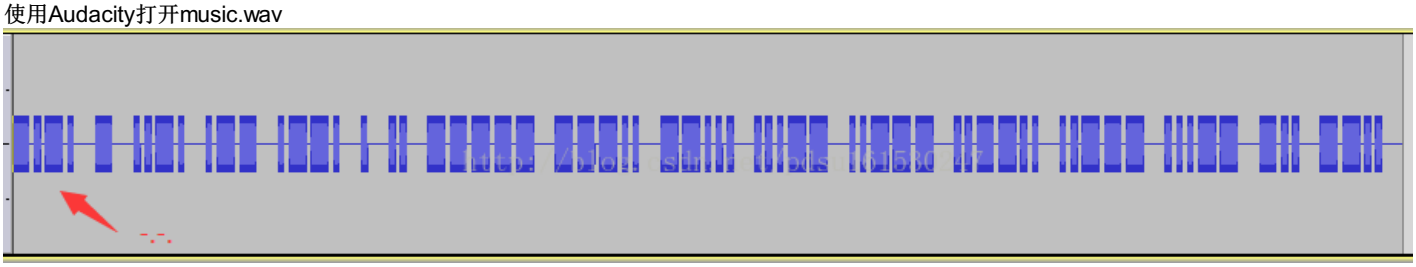

ctf笔记 专栏收录该内容
3 篇文章 1 订阅
订阅专栏

0x00音频隐写二进制或者莫斯密码

音频中隐写摩斯电码

例题：flag在音乐中123（例题链接）
打开压缩包里面有一张图片和一个加密的压缩包（压缩包里面有被加密的music.wav音频文件）

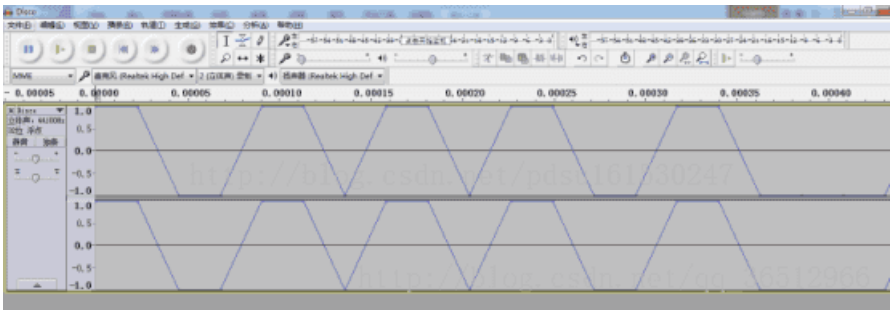
图片上面有盲文（盲文介绍链接）对应明文是：kmdonowg
应该是压缩包密码
使用Audacity打开music.wav

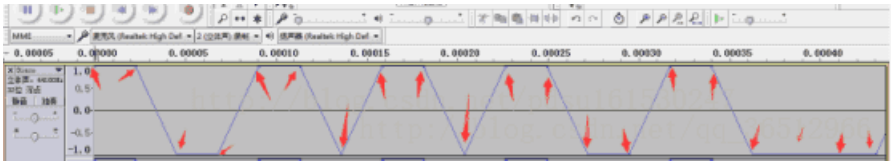


粗的代表杠（-） 细的代表点（.），同时要注意格式：可用空格或者单斜杠/来分割摩斯电码，单只可用一种，不可混用
最后就可以拿到flag

音频中隐写二进制

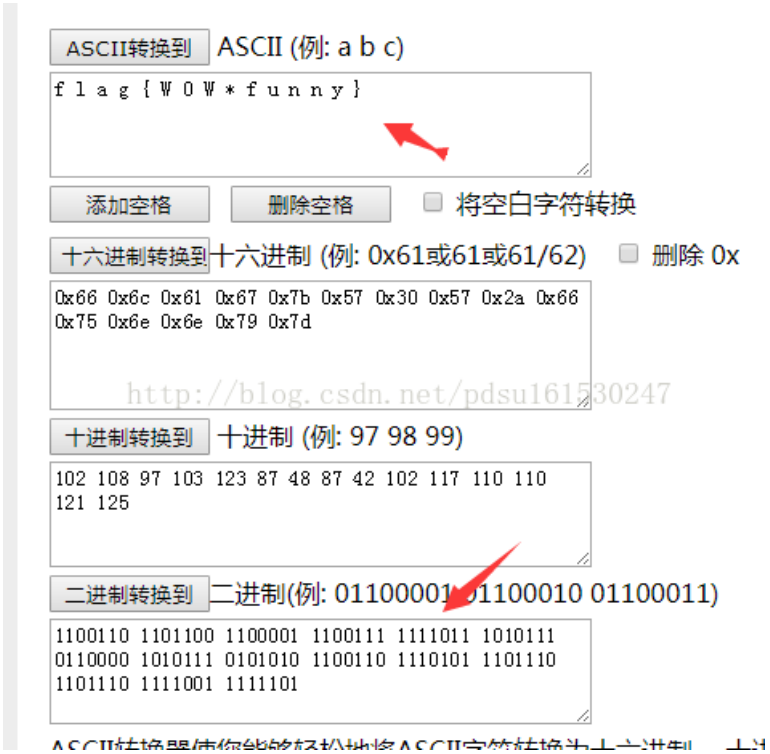
例题：ISCC2017 MISC 很普通的Disco（250分）





我们以高的为1，低的为0得到flag的二进制：1100110110110011000011100111111110111010111011000010101110101010110011011101011101110111011011101110011111101

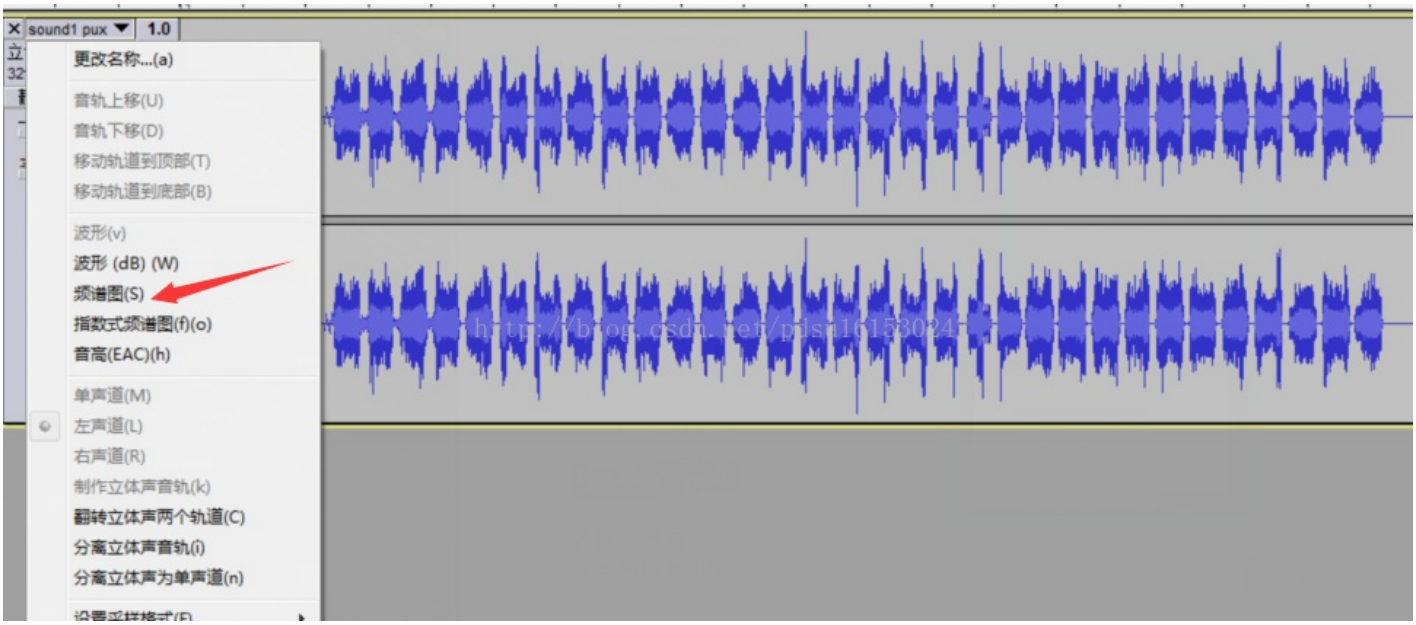
因为ASCII码的二进制是7个字节，所以转换的时候要七位转换一个ASCII码

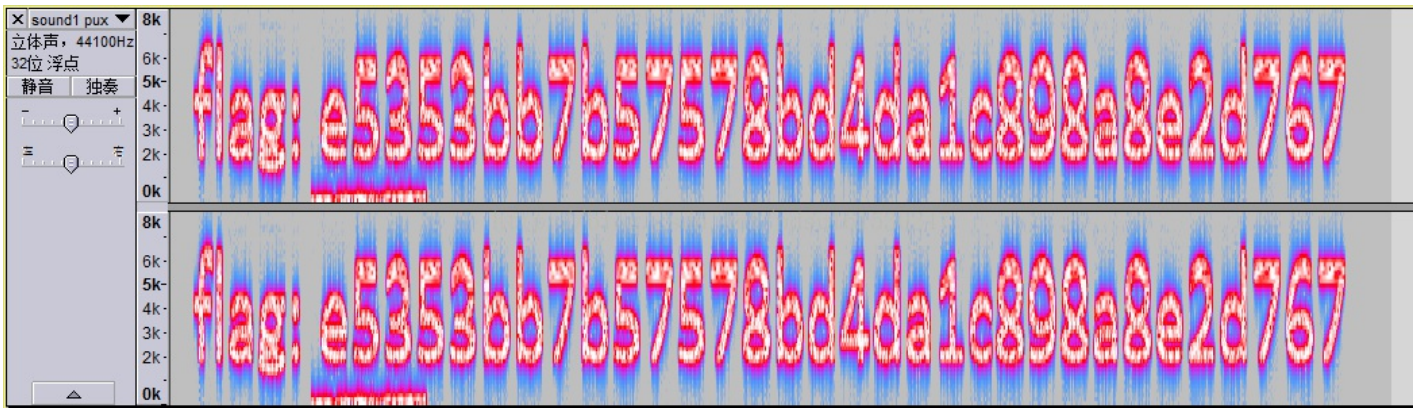


0x01音频转换隐写

例题：链接

使用Audacity打开.wav文件，将波形图转换为频谱图



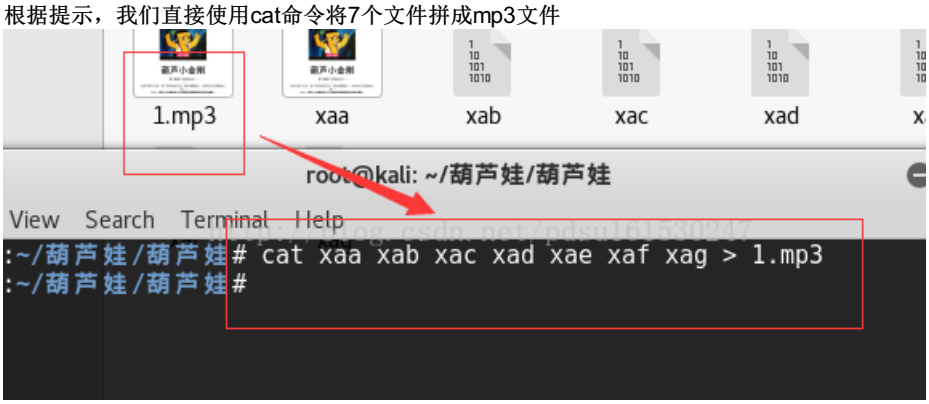


0x02MP3Stego隐写

此隐写的介绍和工具下载链接
例题：i春秋第四期社区赛题第三题（葫芦娃.zip）链接
在kali下解压压缩包

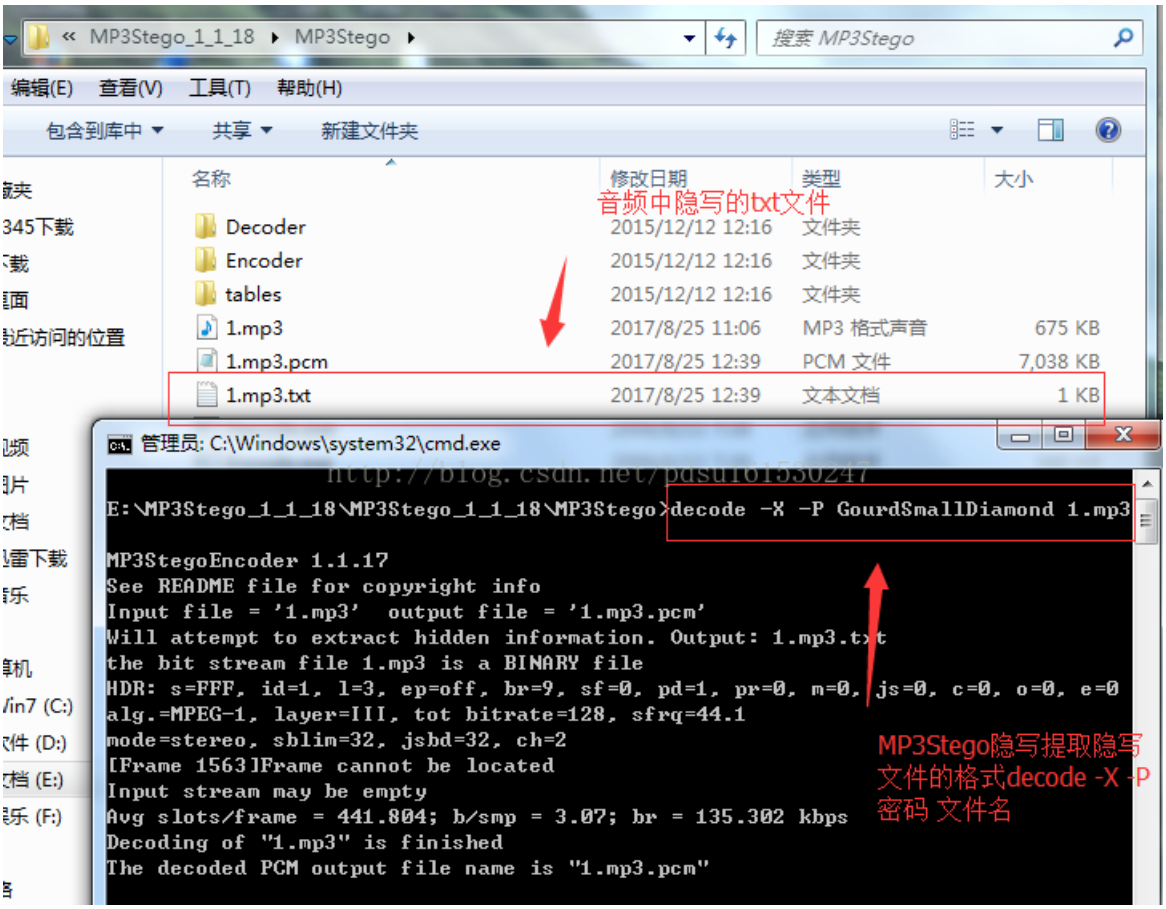
打开第一张图片

根据提示，我们直接使用cat命令将7个文件拼成mp3文件

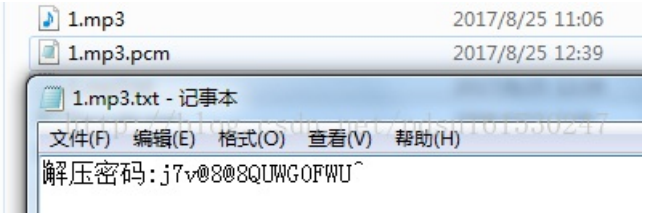


并且提示中还说葫芦小金刚英文名称就是歌曲的密码，跟音频有关还涉及音频密码，最有可能的就是mp3stego隐写

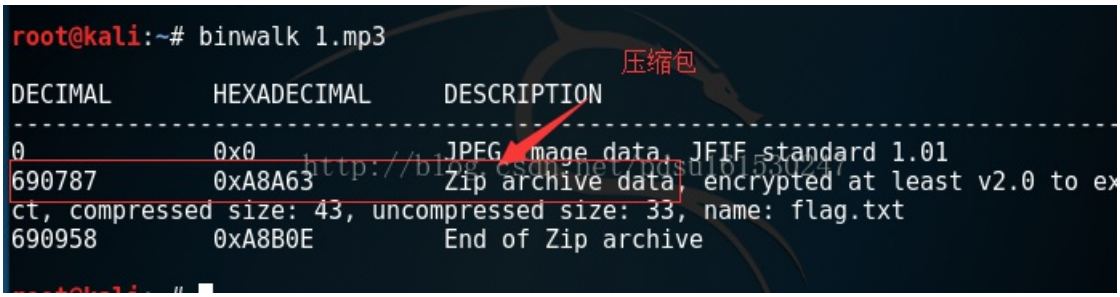
葫芦小金刚的英文名Gourd Small Diamond，去空格GourdSmallDiamond



打开txt文件



回到原来的音频文件1.mp3中，使用binwalk分析文件



里面有个压缩包，在根据上面的1.txt中的解压密码，就对上了！
分离压缩包，使用1.txt中的解压密码

拿到flag。

0x03待更新

碰到新的音频隐写会继续更新！