

CTFmisc常见音频隐写总结

原创

man103 已于 2022-03-30 20:27:54 修改 198 收藏 3

文章标签: [音频](#)

于 2022-03-15 18:50:55 首次发布

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/qq_51652400/article/details/123504708

版权

文章目录

[写在前面](#)

[常见工具](#)

[解题思路](#)

[文件头](#)

[波形图](#)

[频谱图](#)

[有key的隐写](#)

[拨号隐写](#)

[SSTV](#)

[DIFF](#)

[MP3隐写](#)

[总结](#)

写在前面

音频隐写题型比较少, 目前见到的大部分用工具就可以直接解出来, 难度不大, 这里做一个比较简单的总结。示例的题目比较随缘(有些例题不一定找得到了), 重点是解题思路。

常见工具

Audacity, Adobe Audition(简称au), SilentEye, DeepSound, MMSSTV, e2eSoft, mp3stego。

解题思路

第一步当然是先听一下有没有什么关键的信息, 比如摩斯电码(有间隔的长短电波), SSTV(连续刺耳的电波), 拨号隐写之类的。如果不知道是什么声音先自行百度, 听过就不会忘。然后打开以上工具看一看是否存在什么隐写, 如果都没有办法的话可以欣赏一下音乐就下号了。

文件头

wav文件头: `52494646E6AD250357415645666D7420`

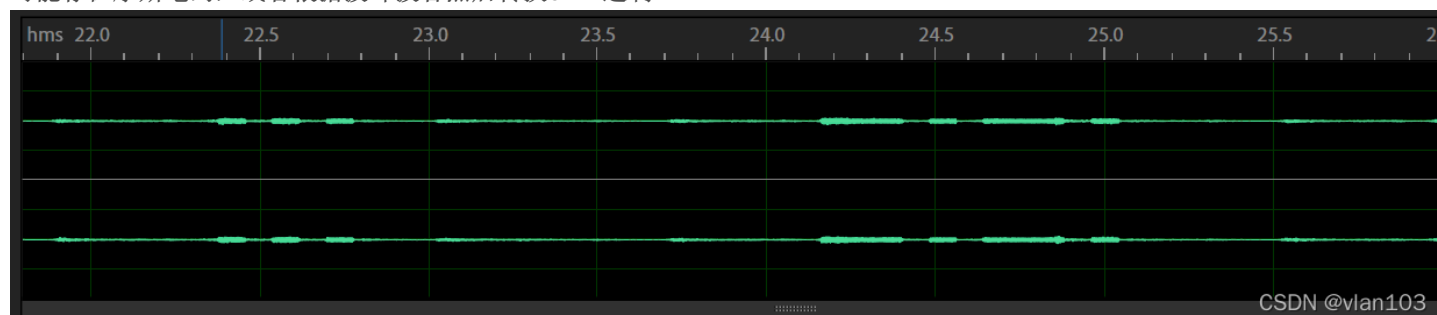
波形图

使用工具：**Audacity/Adobe Audition**

文件类型：**wav**

直接放大即可观察波形图即可。

可能存在摩斯电码，或者根据波峰波谷然后转换01二进制



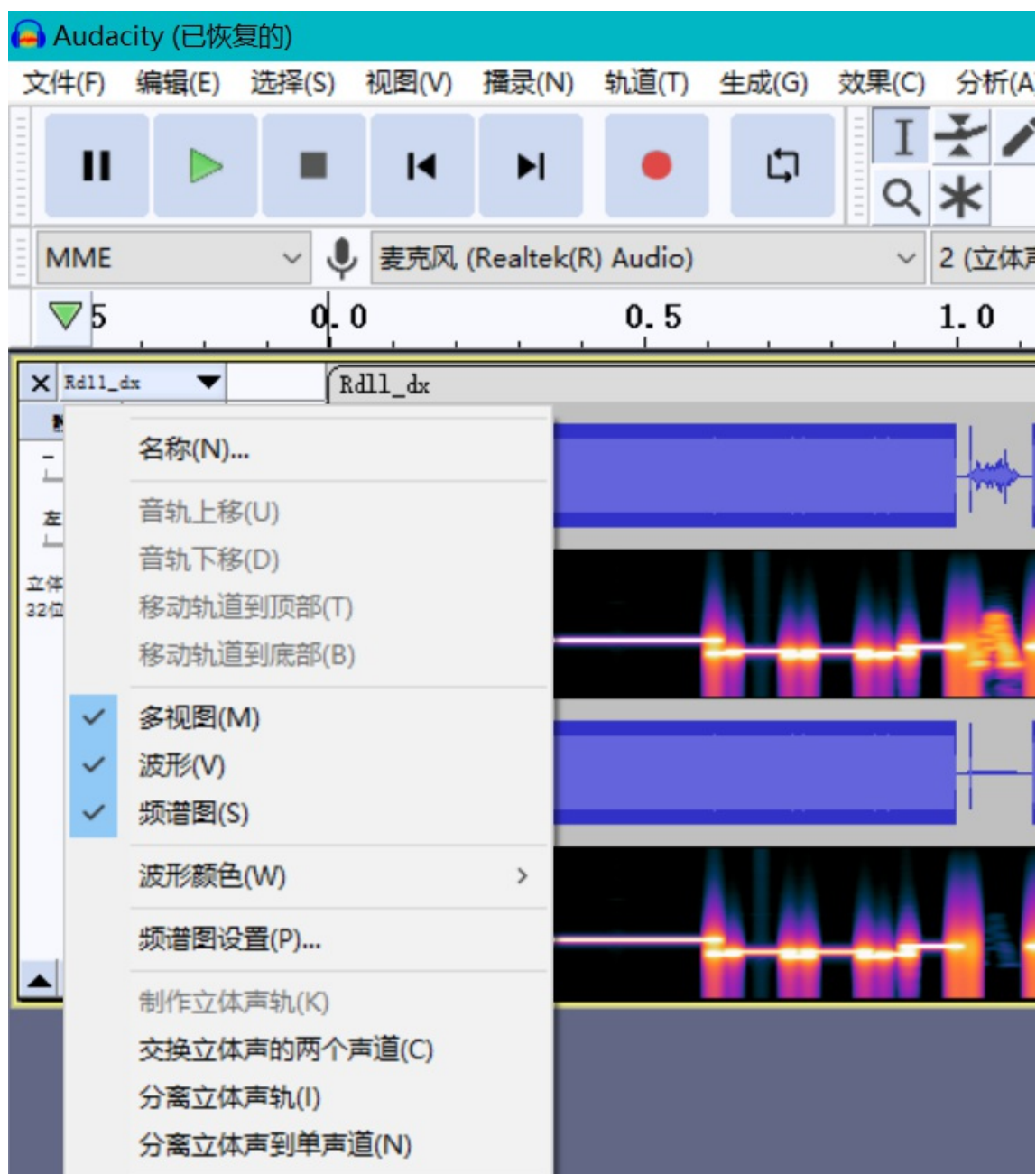
因为做题太少波峰波谷的说实话没遇见过，很多师傅都写了也就带一下

频谱图

使用工具：**Audacity**

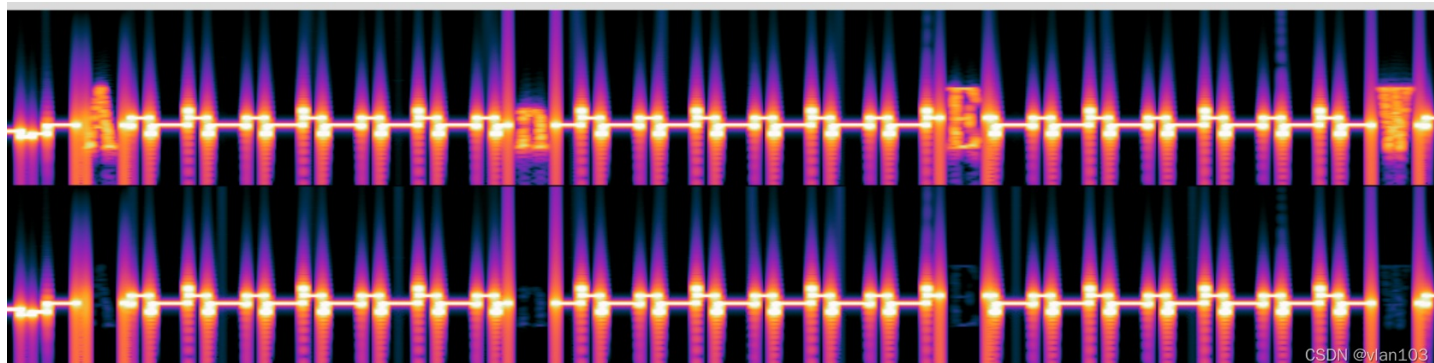
文件类型：**wav**

查看多视图





即可获取隐藏信息，如果简单的话就可能直接get flag了

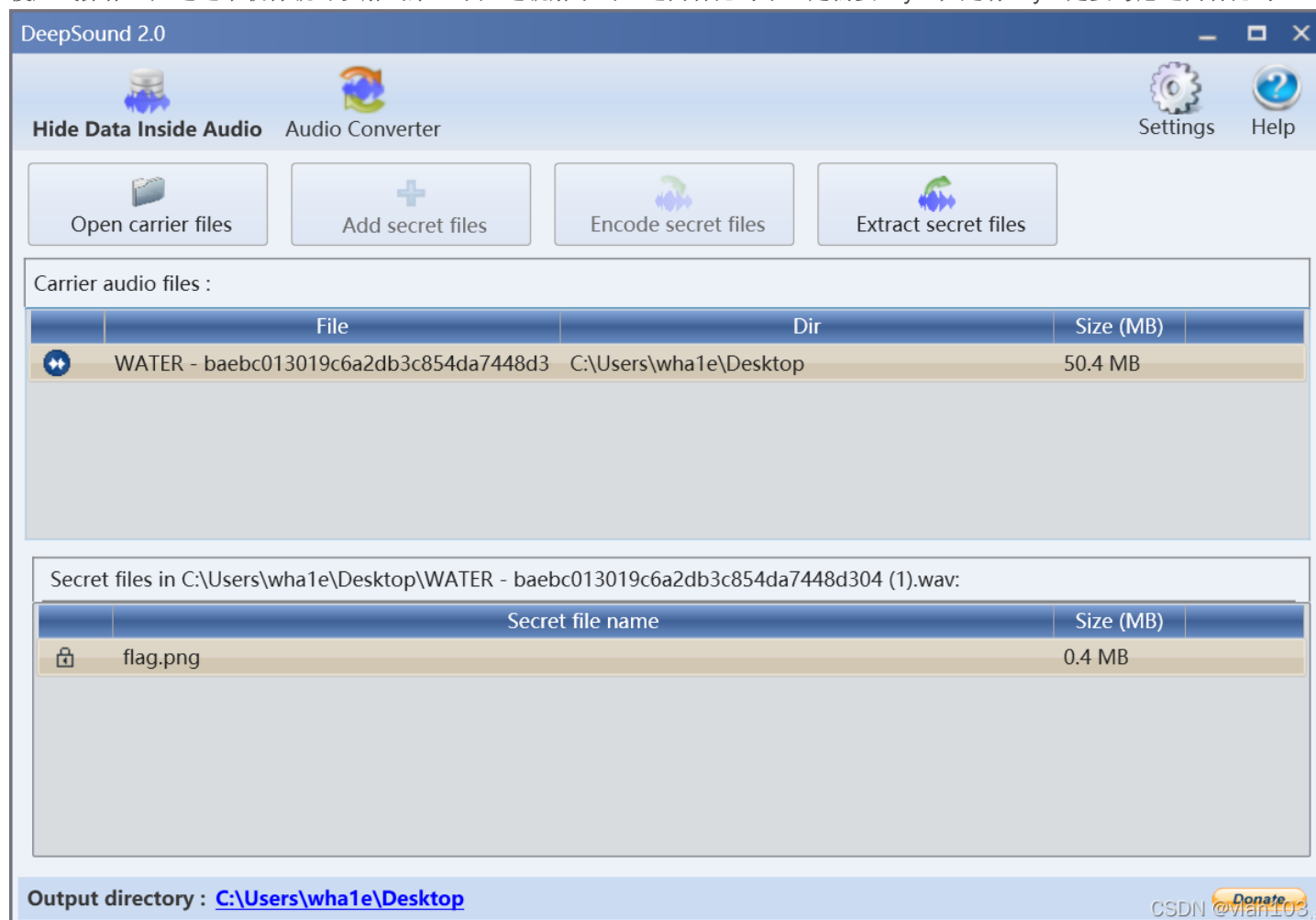


有key的隐写

使用工具：**silenteye**、**deepsound**

文件类型：**wav**

傻瓜式操作，知道这个软件就可以解出来，不知道就解不出。这两种隐写不一定需要key，但是有key一定要考虑这两种隐写。



拨号隐写

经常打10086的时候对方可能说需要XX服务请按1，需要XX服务请按2，对于不同的数字有不同的声音，就可以隐写一些数据。可以通过DTMF提取出来。

DTMF脚本地址：<https://github.com/ribt/dtmf-decoder>

SSTV

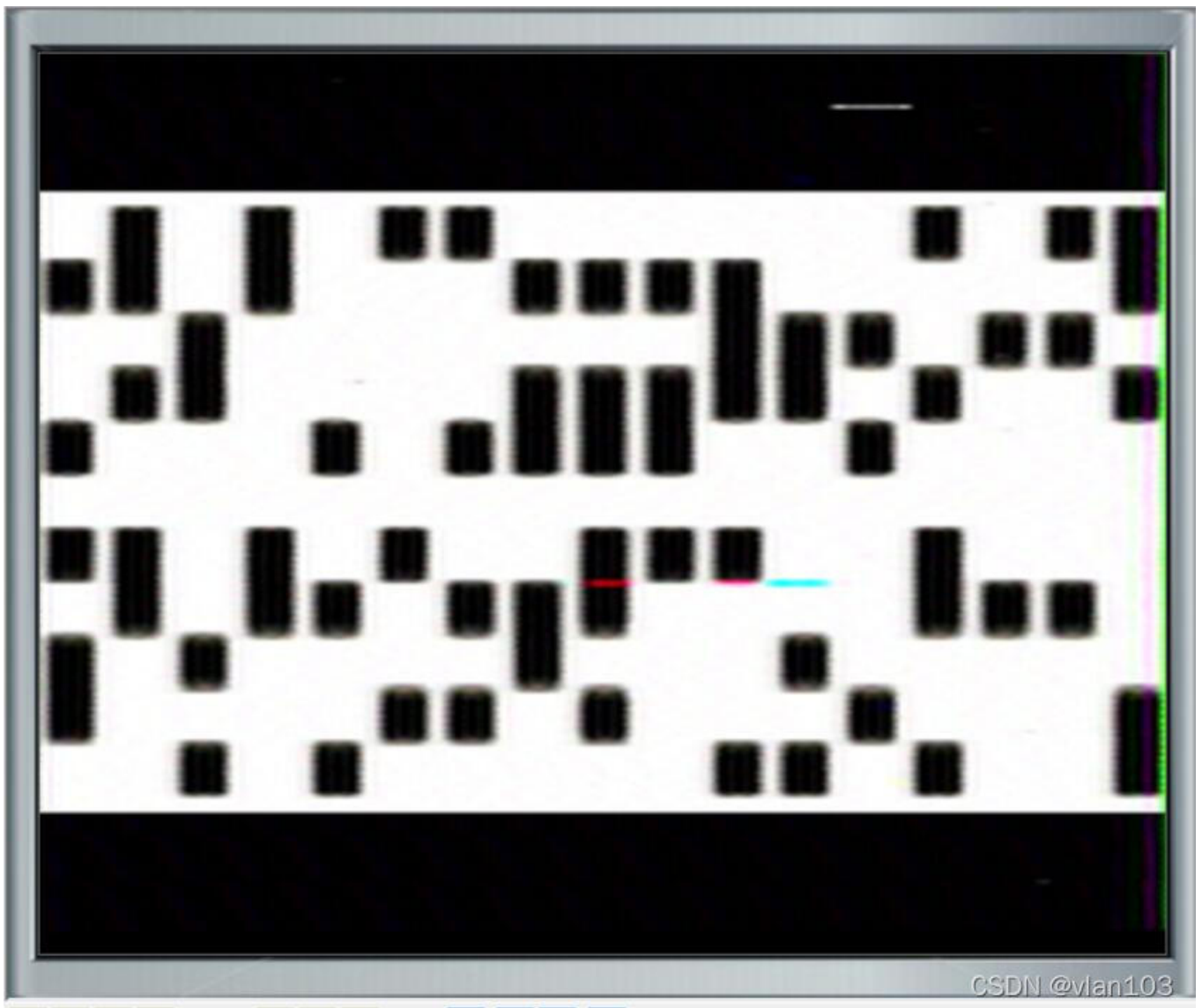
慢扫描电视（Slow-scan television 简称SSTV）是业余无线电爱好者的一种主要图片传输方法，慢扫描电视通过无线电传输和接收单色或彩色静态图片。

表示这玩意真的出烂了，傻瓜式操作

使用工具：**MMSSTV**，**e2eSoft**

文件类型：**wav**

这里强推虚拟声卡e2eSoft这个工具。SSTV正常解法需要一台设备播放一台设备收音，还容易收到杂音的干扰，虚拟声卡就可以很好的避免这个问题。而且，播放SSTV给人一种美国间谍在秘密通信的感觉。

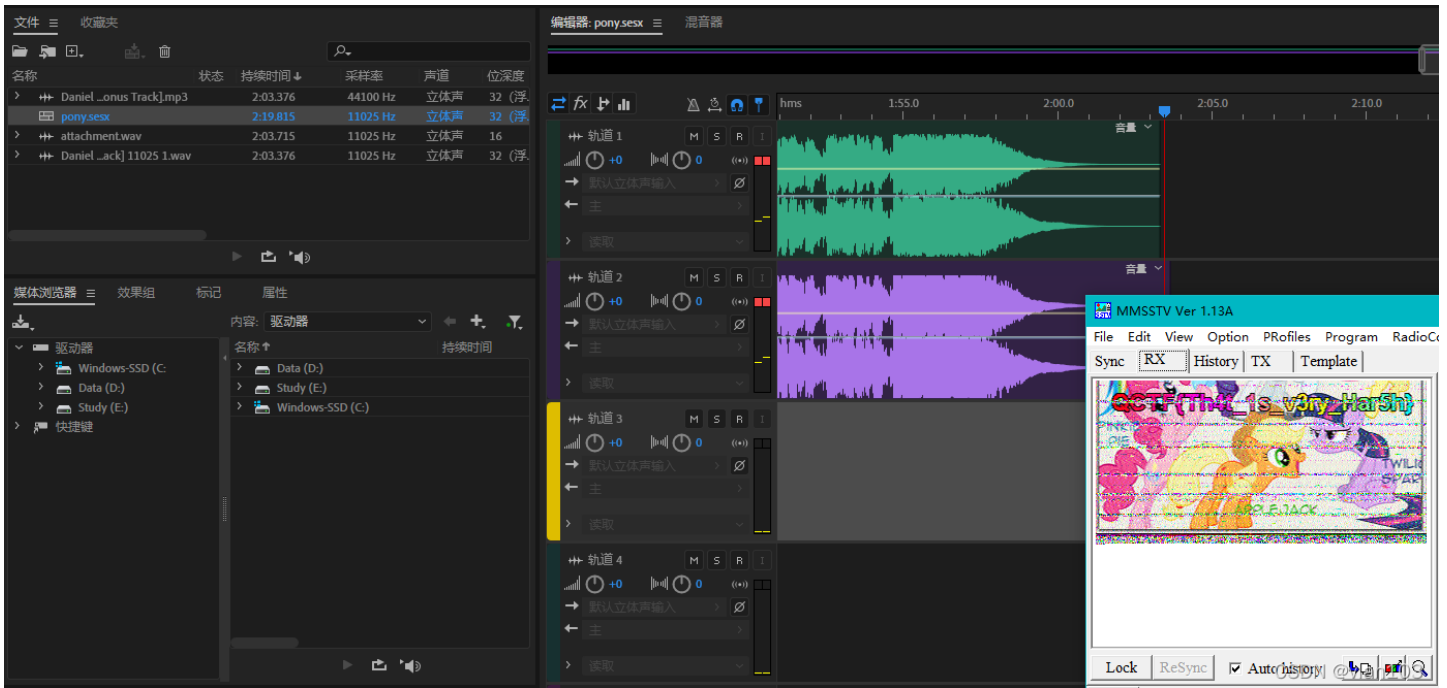
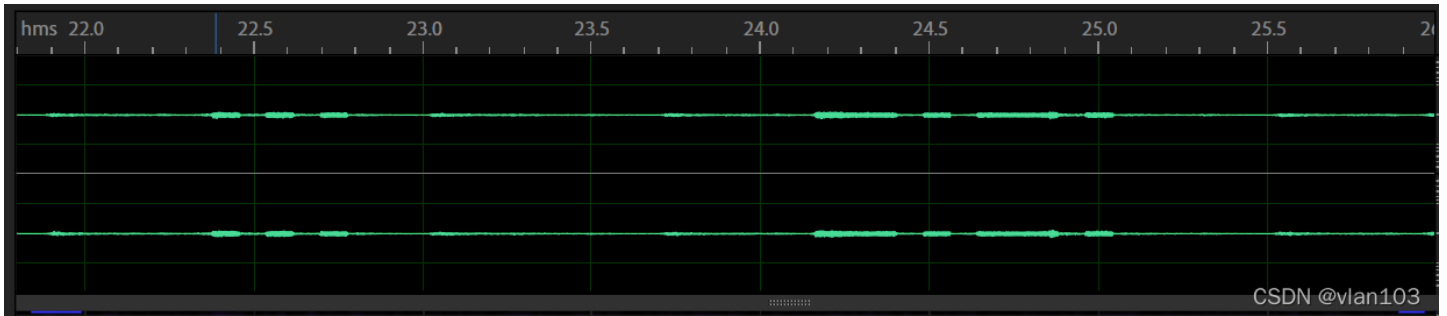
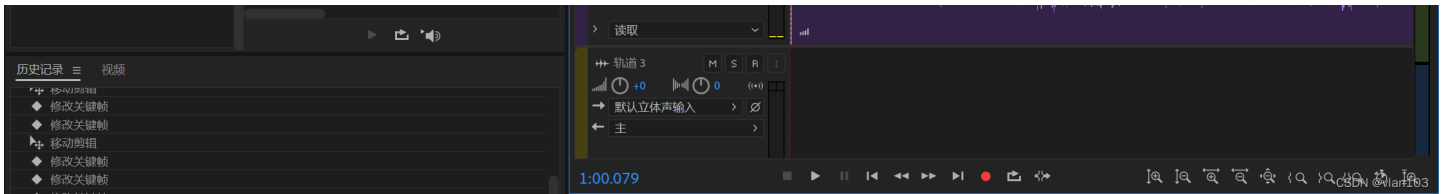


DIFF

使用工具：**Adobe Audition**

文件类型：**wav**

diff比起前面直接使用工具会有一点点麻烦，所以往后排了一点。我这里用的是Au的反相。将得到的音频文件与原曲Diff，或许就可以发现隐藏在其下面的隐藏音频，如摩斯电码，SSTV



MP3隐写

使用工具：mp3stego

文件类型：mp3

隐藏信息

-E 读取隐藏信息文件的内容, -P 设置密码

encode.exe -E hidden_text.txt -P pass svega.wav svega_stego.mp3

解密信息

decode.exe -X svega_stego.mp3 -P pass

这里举一个去年出的题目的例子

```
E:\mp3stego\MP3Stego>Decode.exe -P s3cret -X E:\mp3stego\MP3Stego\不能说的秘密.mp3
MP3StegoEncoder 1.1.19
See README file for copyright info
Input file = 'E:\mp3stego\MP3Stego\不能说的秘密.mp3' output file = 'E:\mp3stego\MP3Stego\不能说的秘密.mp3.pcm'
Will attempt to extract hidden information. Output: E:\mp3stego\MP3Stego\不能说的秘密.mp3.txt
the bit stream file E:\mp3stego\MP3Stego\不能说的秘密.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=1, pd=0, pr=0, m=0, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=48.0
mode=stereo, sblim=32, jsbd=32, ch=2
[Frame 3447]Frame cannot be located
Input stream may be empty
Avg slots/frame = 384.005; b/smp = 2.67; br = 128.002 kbps
Decoding of "E:\mp3stego\MP3Stego\不能说的秘密.mp3" is finished
The decoded PCM output file name is "E:\mp3stego\MP3Stego\不能说的秘密.mp3.pcm"

E:\mp3stego\MP3Stego>
```

svega.wav	2018/11/6 23:00	WAV 文件	1,781 KB
不能说的秘密.mp3	2021/9/24 17:08	MP3 文件	1,294 KB
不能说的秘密.mp3.pcm	2022/3/15 17:16	PCM 文件	15,516 KB
不能说的秘密.mp3.txt	2022/3/15 17:16	文本文档	1 KB

```
C:) 不能说的秘密.mp3.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
flag{wha1e_W4nt_@_gir1Fri3Nd}
```

CSDN @vian103

总结

音频文件隐写暂时就总结这么多，比较简单，属于知道就能做，后续如果有新题型我将持续更新。