wav文件隐写：Deepsound+TIFF图片PS处理（ AntCTF x D^3CTF 2022 misc BadW3ter）

原创

Hardworking666 于 2022-03-08 22:12:21 发布 354 收藏 1

分类专栏： CTF 文章标签： wav deepsound tiff D3CTF AntCTF

本文链接：https://blog.csdn.net/Hardworking666/article/details/123363550

解题步骤

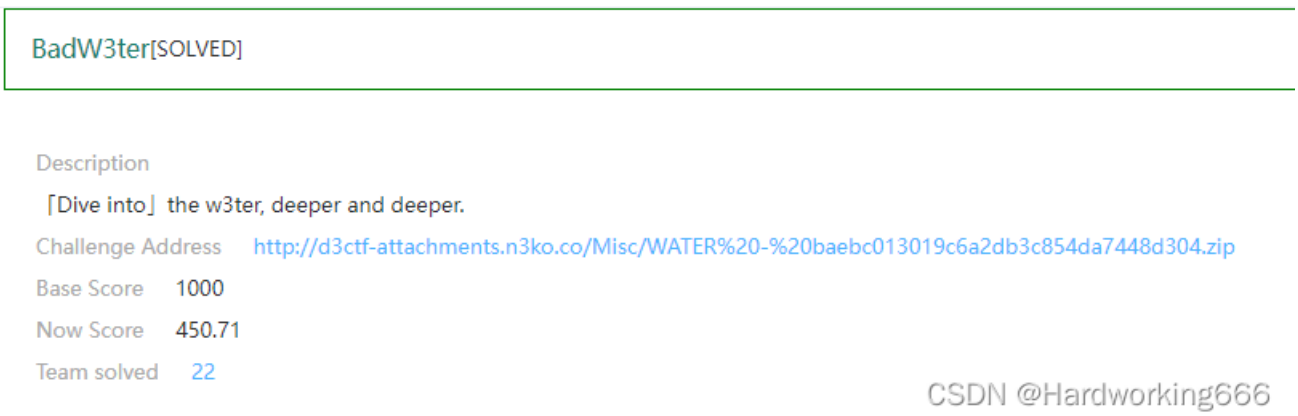
- wav文件头实例分析
- 修改wav头
- DeepSound隐写
- file识别文件+PS处理

AntCTF x D^3CTF背景：

三支“电子科大”队伍：杭电 Vidar-Team、西电 L-Team 及成电 CNSS 共同举办，蚂蚁金服安全应急响应中心赞助。

官网：https://d3ctf.io/#/

题目：BadW3ter



wav文件头实例分析

```
[ 地址 ]  [                文件内容                ][   ASCII    ]
00000000h: 52 49 46 46 22 60 28 00 57 41 56 45 66 6D 74 20 ; RIFF"`(.WAVEfmt
00000010h: 12 00 00 00 01 00 01 00 22 56 00 00 44 AC 00 00 ; ........"V..D? .
00000020h: 02 00 10 00 00 00 66 61 63 74 04 00 00 00 F8 2F ; ......fact....?
00000030h: 14 00 64 61 74 61 F0 5F 28 00 00 00 00 00 00 00 ; ..data餘(.......
00000040h: 00 00 FF FF 00 00 FF FF 01 00 FE FF 02 00 FD FF ; ..  ..  ..? ..?
00000050h: 03 00 FB FF 05 00 F8 FF 08 00 F6 FF 0A 00 F5 FF ; ..? ..? ..? ..?
00000060h: 09 00 F8 FF 04 00 00 00 F7 FF 14 00 DA FF 40 00 ; ..? ....? ..? @.
00000070h: 93 FF BF 00 6C FE D3 06 50 00 38 FC BB 00 55 FF ; ? ? l  .P.8  .U
00000080h: 59 00 8A FF 38 00 AA FF 16 00 BD FF 06 00 CB FF ; Y.? 8.? ..? ..?
00000090h: F7 FF DC FF EE FF DE FF ED FF E9 FF EF FF EE FF ; ? ? ? ? ? ? ? ?
000000a0h: E9 FF EA FF E8 FF E9 FF F2 FF E9 FF EC FF E4 FF ; ? ? ? ? ? ? ? ?
000000b0h: E7 FF E2 FF E6 FF E4 FF E8 FF F4 FF F1 FF E9 FF ; ? ? ? ? ? ? ? ?
000000c0h: E3 FF E4 FF E4 FF E5 FF E3 FF E6 FF E0 FF E1 FF ; ? ? ? ? ? ? ? ?
```


（1）**52 49 46 46**，这个是Ascii字符“RIFF”，这部分是**固定格式**，表明这是一个WAVE文件头。

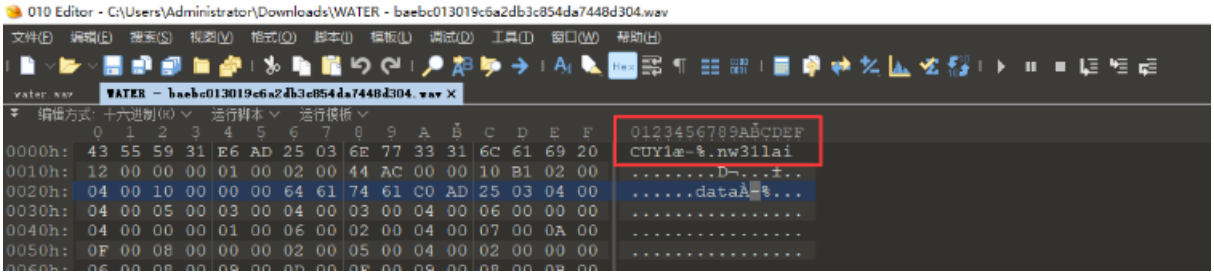
（2）22 60 28 00，这个是我这个WAV文件的**数据大小**，这个大小包括除了前面4个字节的所有字节，也就等于文件总字节数减去8。16进制的“22 60 28 00”对应是十进制的“2646050”。

（3）**57 41 56 45 66 6D 74 20**，也是Ascii字符“WAVEfmt”，这部分是**固定格式**。

wav文件格式分析与详解

修改wav头

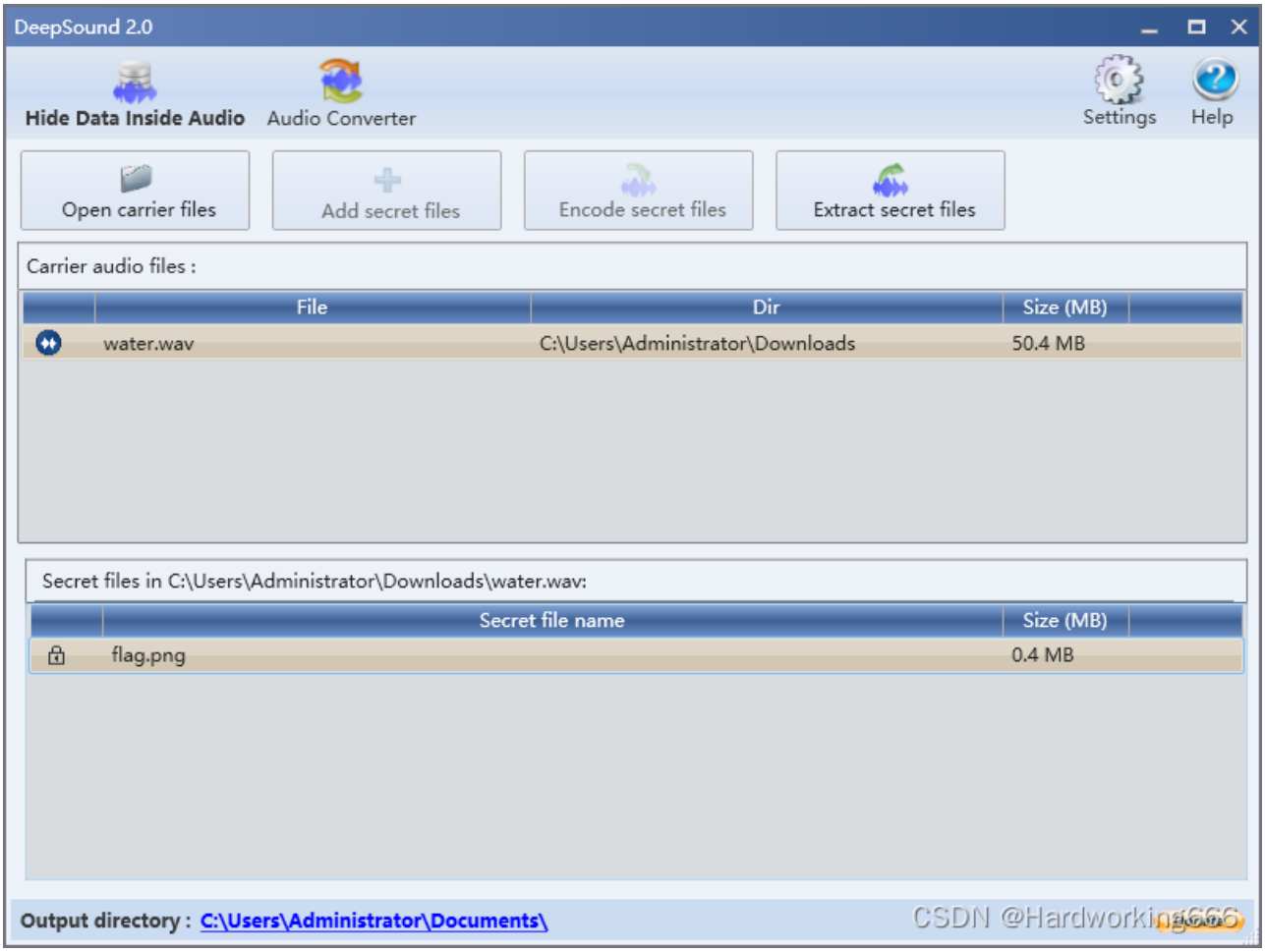
附件是wav，对比正常的wav发现前十六个字节被修改，第一行的内容猜测是密码： CUY1nw31lai
改回来：



DeepSound隐写

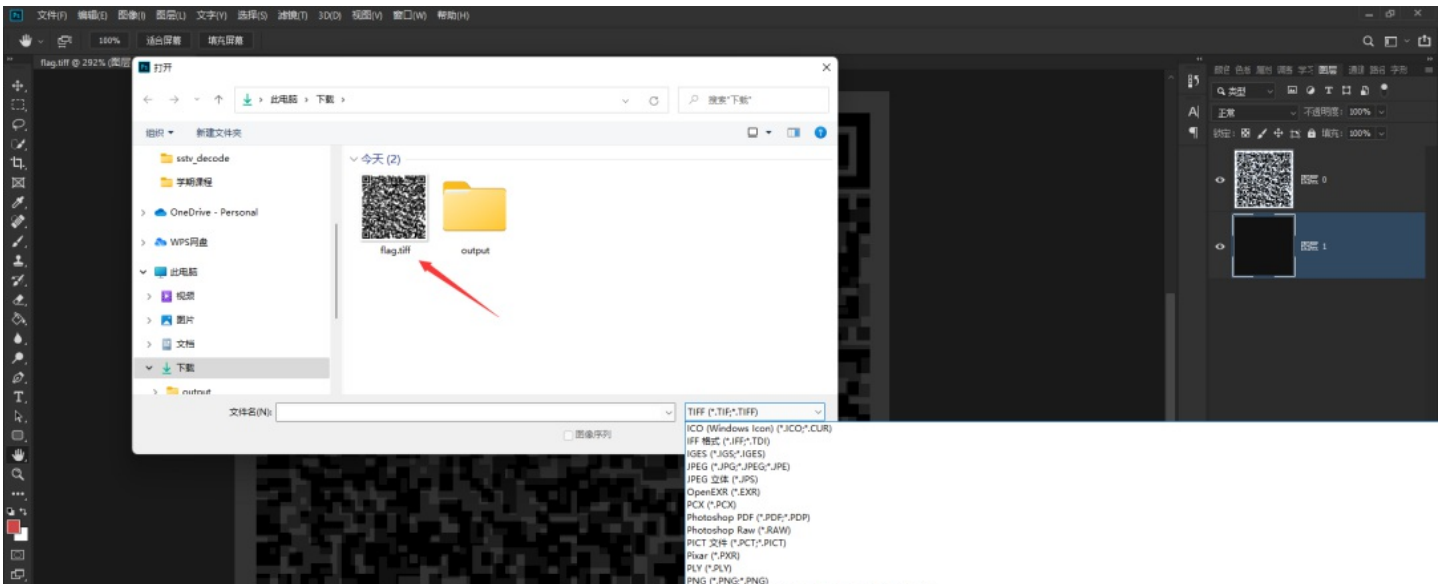
DeepSound是一款可以**将文件添加到歌曲中的软件，可把非常私密的文件隐藏在歌曲里**。

输入前面的密码。得到flag.png



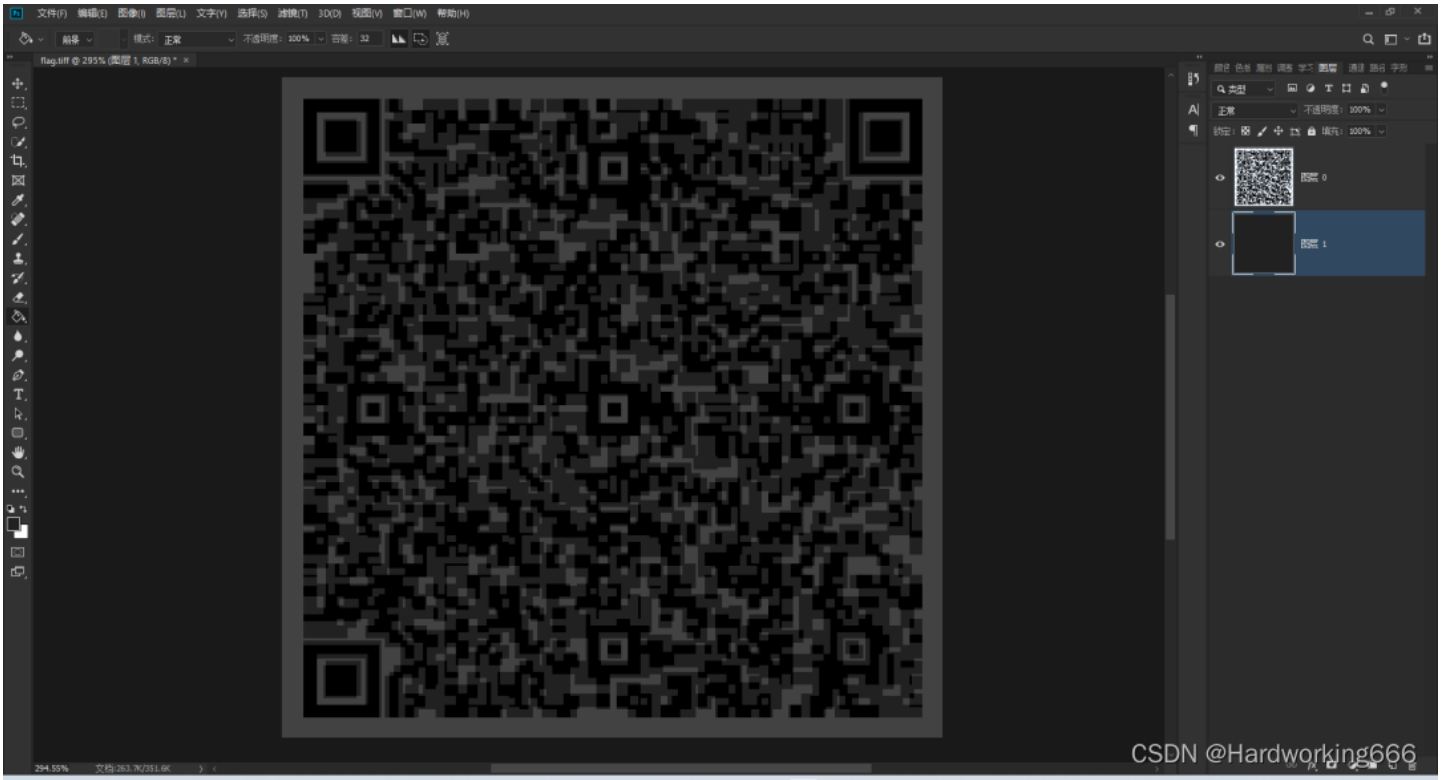
file识别文件+PS处理

file识别文件发现flag.png是TIFF文件，PS打开TIFF文件

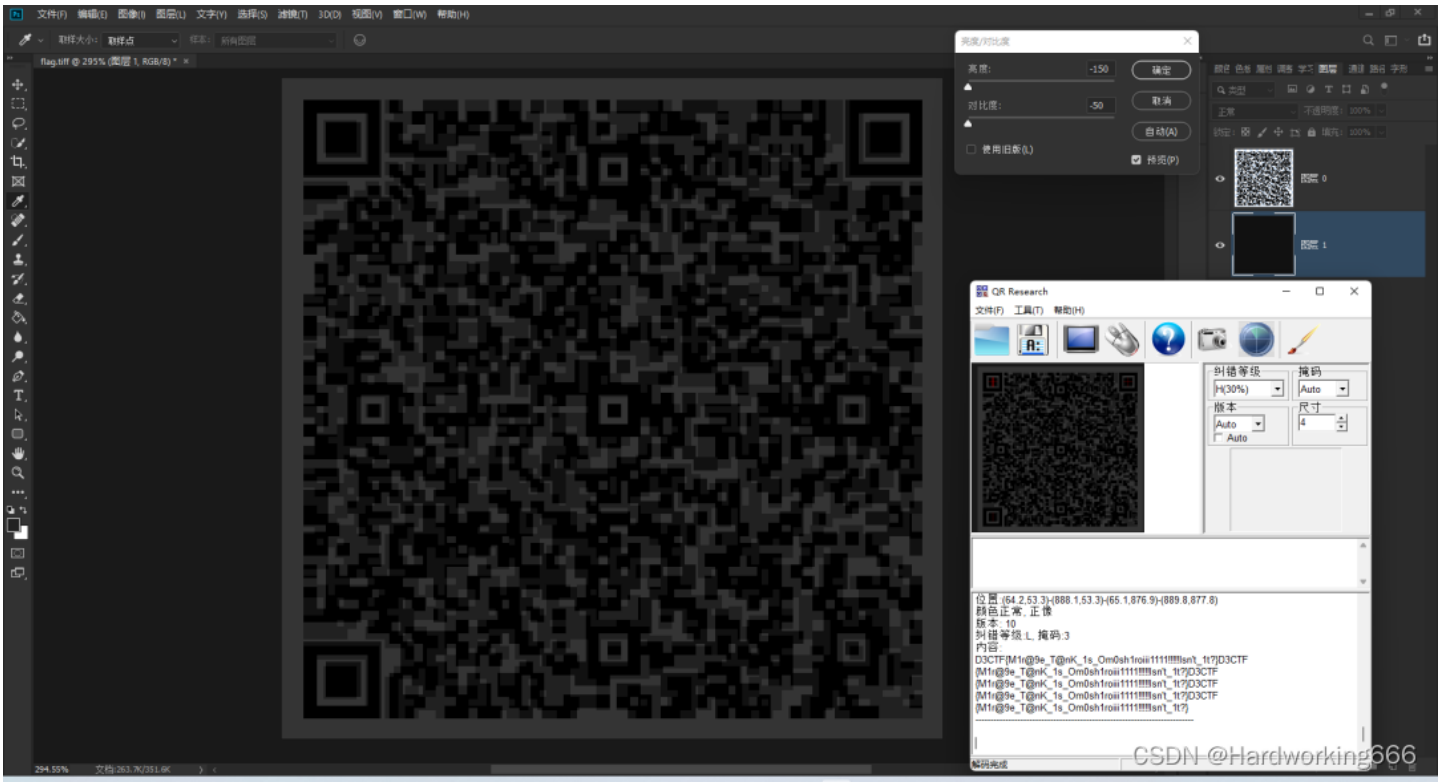


有两个图层，有一个白底图层，这个二维码是三部分颜色组成：黑、白、灰

把白底图层涂成灰色(和二维码图层中的灰色一样的：[33,33,33])，用油桶或者填充都可以



然后 图像->调整->亮度/对比度 直接将亮度，对比度拉到最低，扫描二维码即可得到flag：
D3CTF{M1r@9e_T@nK_1s_Om0sh1roiii1111!!!lsn't_1t?}



此题参考链接，作者：末初