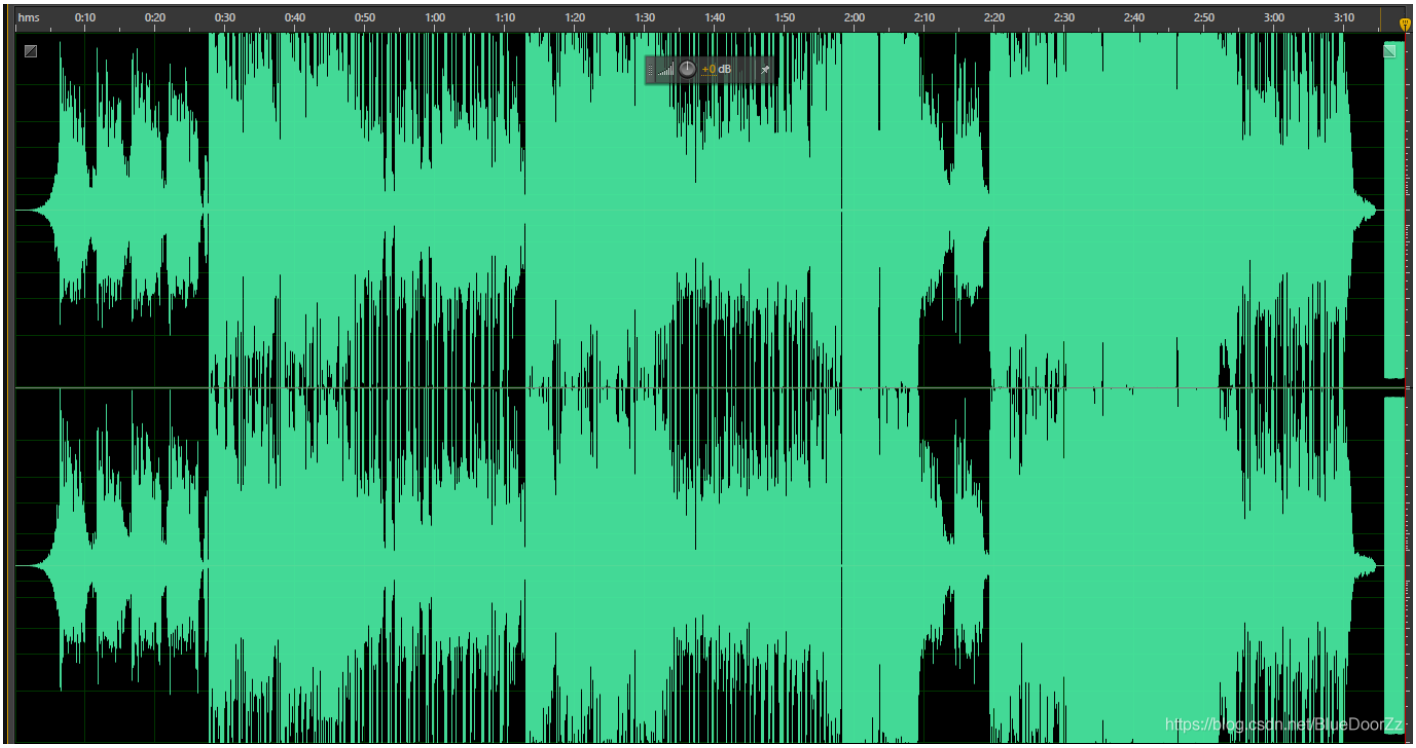
GKCTF2020 部分MISC

原创

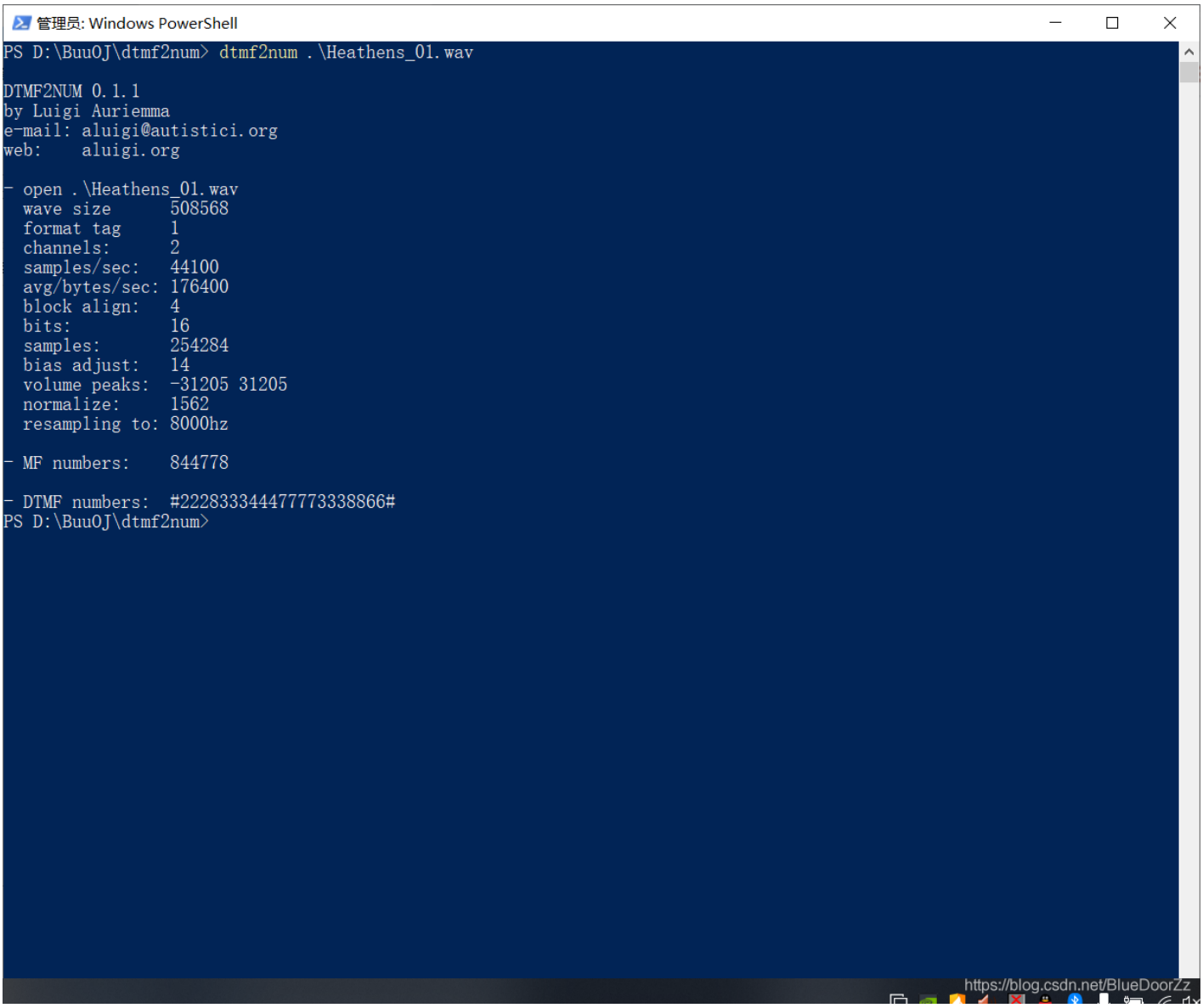
BlueDoorZz 于 2020-05-26 16:00:42 发布 636 收藏

Harley Quinn

下载两个文件，一段音频与一张图片。首先打开Au对音频进行频谱分析：



最后一段与其他明显不同，听一下是一段拨号音，将其截取并另存为.wav文件。使用dtmf2num分析：



一串数字，随便在网上找一张诺基亚的图片，数字对应的是相应的按键，如按三次2就是c，按8是t；由于博主比较懒，就不上图了，最终解密为ctfisfun，第一步至此完成。

然后查看图片，在二进制编辑器中我发现图片后有一串像base64编码的字符串，但是尝试了base58-base100等种种编码以及AES解密后都无效。后官方提示使用free_file_camouflage解密，将图片导入，输入我们前面获得的密文，获得flag。

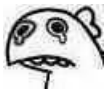
附上dtmf2num的下载地址：https://github.com/aur-archive/dtmf2num。

Sail a boat down the river

这题对星际玩家不太友好。

题目给出两个文件，flag.mp4与vocal.rar。视频文件中有两个关键信息。

我们使用potplayer对flag.mp4逐帧分析，在15秒左右有一张明显的二维码，将其截图扫码，发现是百度网盘的二维码。

网盘需要提取码，题目提示闪烁的光芒，一开始以为是车灯的光，后来官方writeup说是刷卡机的光。 

好吧，一帧一帧的看，短一帧长三帧，拼接起来是摩斯密码，为了保护大家的视力，摩斯密码直接放这了：-.--/.--/---../--.。

解密出yw8g，看来是百度网盘的提取码了。下载文件后是一个数独以及密文，还有密钥的提示，随便玩玩解出

52693795149137，aes解密后得到GG0kc.tf，这就是压缩包密码了。解压出ovex文件，用overture打开，在歌词里看到flag。