Writeup of BlueDon CTF's MISC-1:杂项全家桶

原创

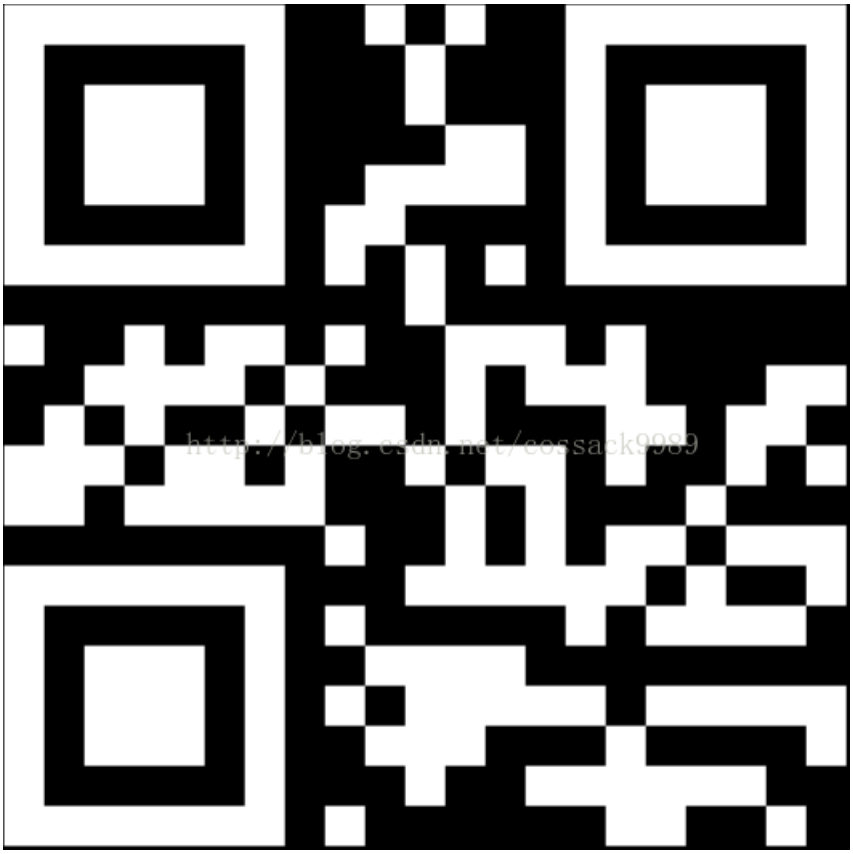
C0ss4ck 于 2017-10-30 21:23:50 发布 2024 收藏 1
分类专栏： MISC_of_CTF 文章标签： MISC CTF BlueDon
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/cossack9989/article/details/78397527
版权


MISC_of_CTF 专栏收录该内容
3 篇文章 0 订阅
订阅专栏

突然发现bdctf的初赛竟然还有一轮，拿起电脑顺手干了一题~。

Step1：

下载附件后解压得一个打不开的png文件，发现文件头被损坏，修正后打开得下图

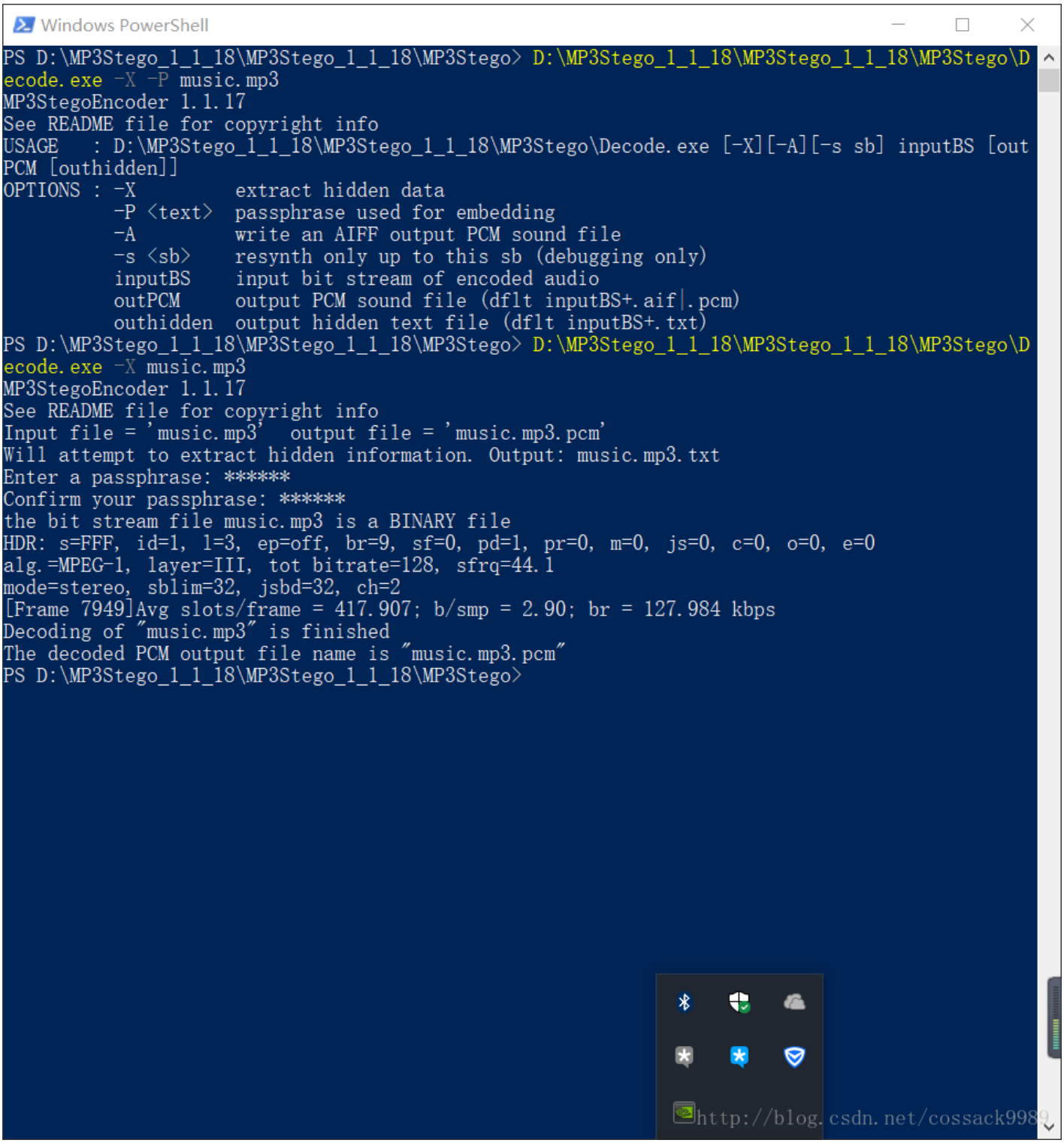


Step2：

很明显需要反色一下，用stegosolve的colour inversion（Xor）进行反色，扫码得到一串当铺密码“工井大人夫王”译得485376。这个时候本来以为是在png里面藏了个加密压缩包什么的，一番搜索之后并没有发现啥……陷入沉思。

Step3：

再打开010editor，发现png文件后面跟着一个rar，解压得一个mp3文件，用audacity一番操作之后并没有发现什么有价值的信息，于是用命令行操作MP3stego，



得到music.mp3.txt（decode文本），获得字符串fx4qx0hj_4_cg{Wvf}，显然是凯撒密码，列出所有位移结果后得到flag，即bdctf{4_Sm4rt_b0y}