Misc

2.至少像那雪一样

用 binwalk 扫描图片，发现文件是合成的，进行分离操作，（binwalk 分离文件错误，后改用 foremost），得到.jpg 和.zip 文件，压缩包里有加密的图片和 flag.txt。

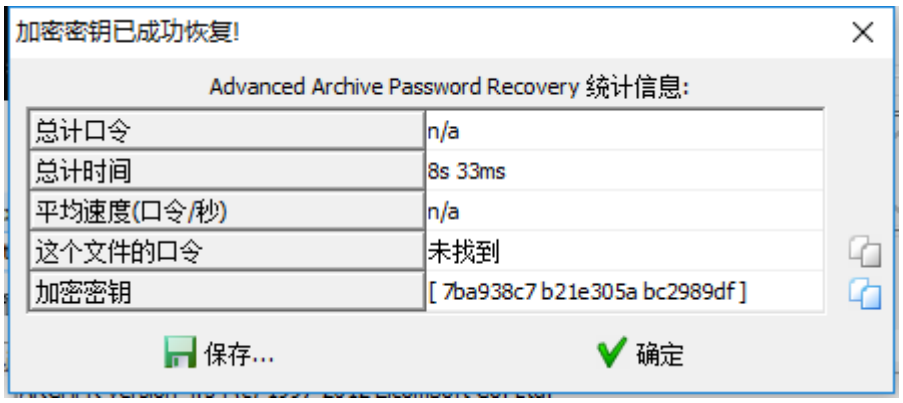
```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
30            0x1E            TIFF image data, big-endian, offset of first image directory: 8
885851        0xD845B         Zip archive data, encrypted at least v2.0 to extract, compressed size: 75, uncompressed si
ze: 240, name: flag.txt
886204        0xD85BC         End of Zip archive, footer length: 22
```

jpg	2019/2/11 23:49	文件夹	
zip	2019/2/11 17:25	文件夹	
audit.txt	2019/2/11 17:23	文本文档	1 KB
flag.txt	2019/2/7 13:19	文本文档	1 KB

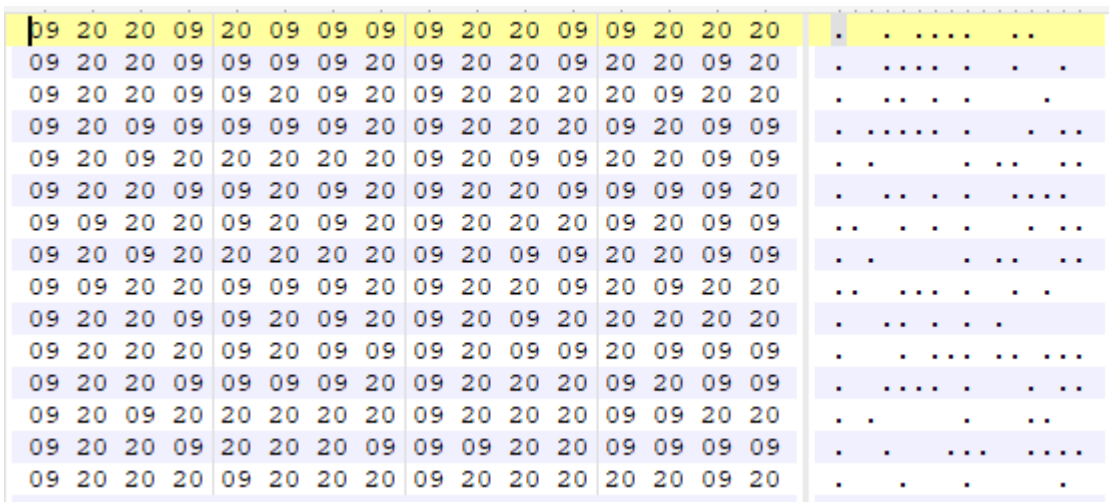
将图片压缩，发现其 crc32 与加密图片一致，可用明文攻击。

00000000.jpg	443,170	442,571	JPG 文件	2019/2/11 17:23	93C74849
至少像那雪一样.jpg	443,170	442,571	JPG 文件	2019/2/7 13:04	93C74849
flag.txt	240	63	文本文档	2019/2/7 13:19	82D89E74

尝试后，得到密钥，



导出解密后的文件，打开 txt，发现空白，但文件有一定大小，用 010editor 打开，表示为 16 进制，发现一堆 09 与 20，怀疑是 09 表示 0，20 表示 1，尝试后，将二进制转为字符，得到 flag。



```
01101000011001110110000101101101011001010111101101000001011101000101111101001100011001010110
6867616d657b41745f4c656135745f4c316b655f744861745f736e30777d
hgame{At_Lea5t_L1ke_tHat_sn0w}
```

3.旧时记忆

没什么好说的，搜索存储器，在其发展历史中发现图片应该是打孔卡，对照打孔规则得到字符，加上 hgame{}提交。

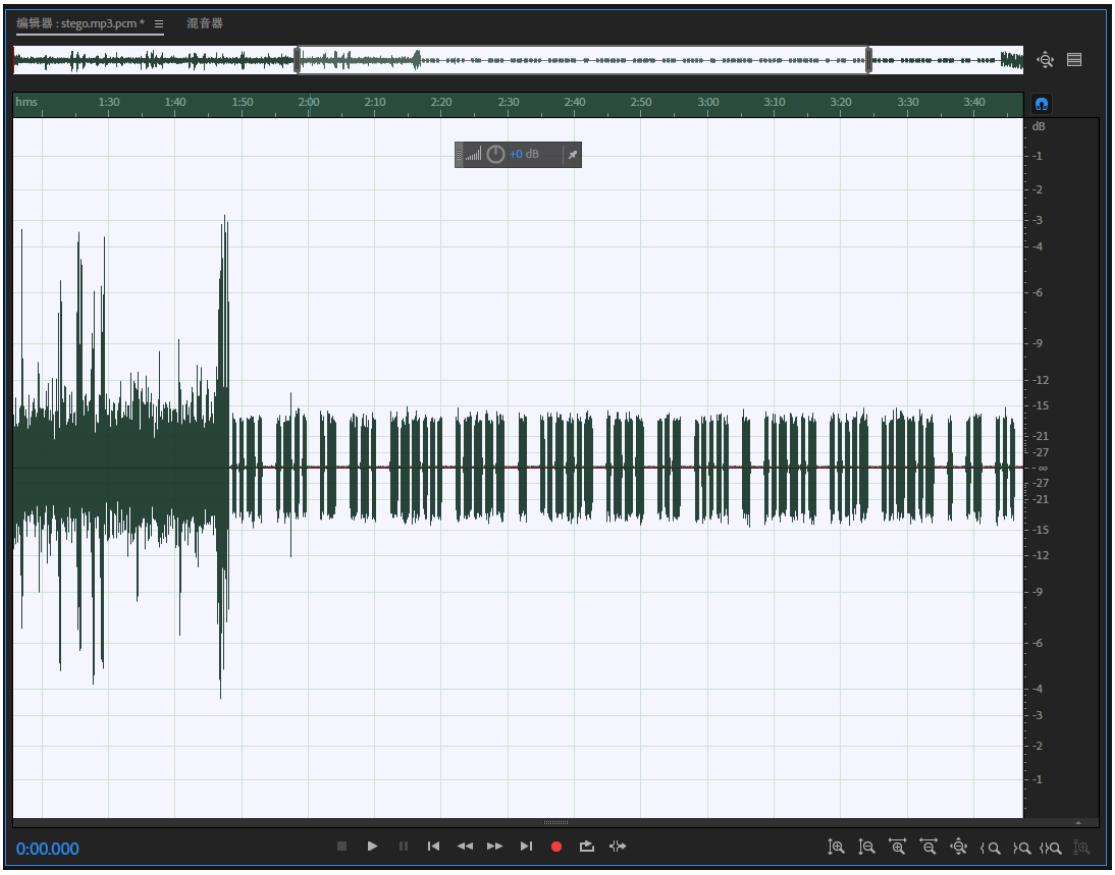
0LD_DAY5%M3MORY

4.听听音乐?

音频隐写，用 MP3Stego 得到.txt 和.pcm 文件，打开文档，发现被忽悠了，

Maybe you think you are right, but in fact, it's wrong.

Flag 应该在音频文件里，用 au 打开，波形有一定规律，但很难看出是什么，应该被改过，尝试进行滤波，得到明显的摩斯密码，



转换后得到 flag。