实验吧/隐写术/小苹果

原创

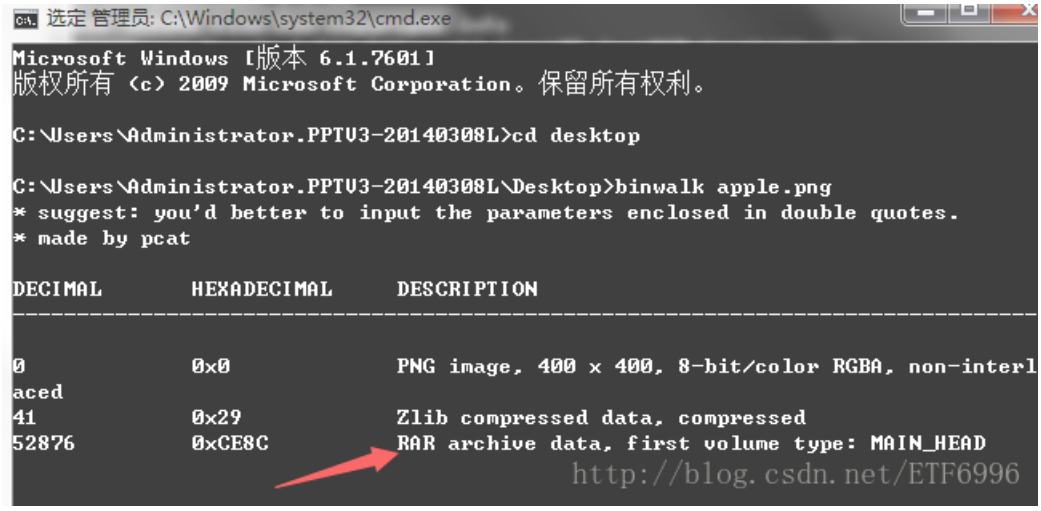
SIAT_啊哦 于 2017-04-12 20:17:47 发布 3405 收藏

分类专栏： CTF 文章标签： unicode 当铺密码 mp3stego

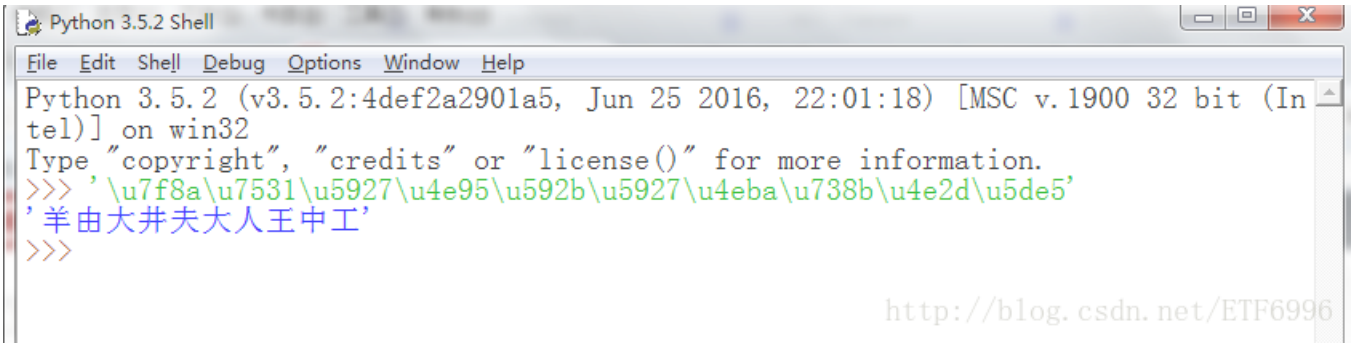
本文链接：https://blog.csdn.net/ETF6996/article/details/70146940

题目链接

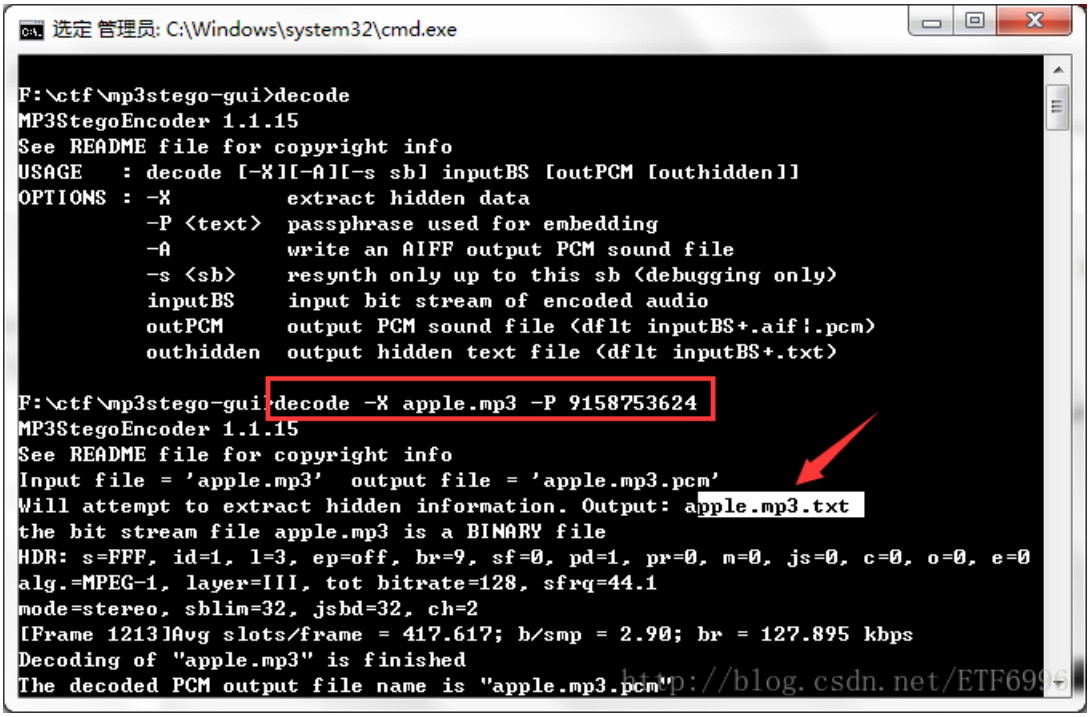
1. 首先binwalk，发现有个RAR



2.解压RAR，得到apple.mp3,自然联想到mp3stego，然后decode，但是需要输入decode密码，再回头看看图片，发现是一个二维码，扫描后得到\u7f8a\u7531\u5927\u4e95\u592b\u5927\u4eba\u738b\u4e2d\u5de5，很明显是Unicode加密，直接在python3.5里面进行Unicode解码后得到：



3.得到：羊由大井。。。，一看是当铺密码，再进行解密得：9158753624，即mp3stego的decode密码如下：



4.在生成的apple.mp3.txt中看到一串base64，解密即得flag