



[Adobie] HGAME 2019 week-1 writeup

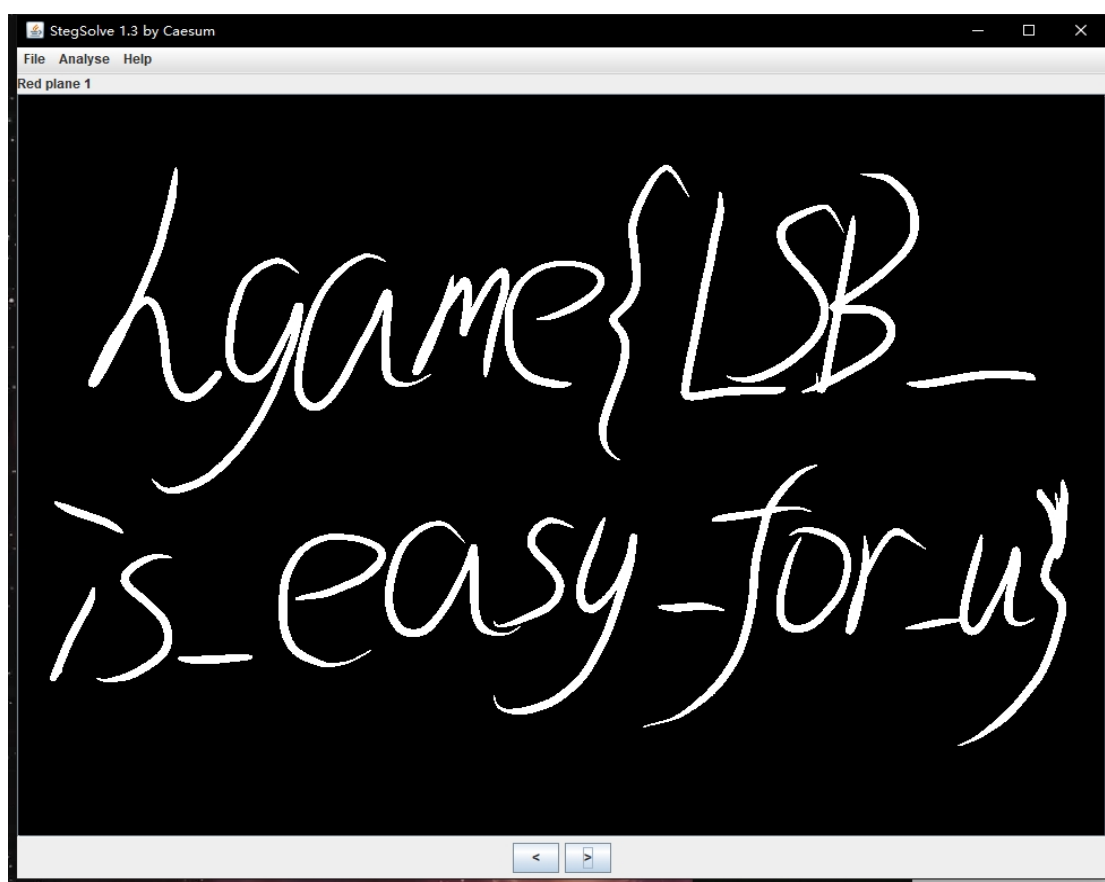
MISC :

1.Hidden Image in LSB

下载得到压缩包，发现两个文件。

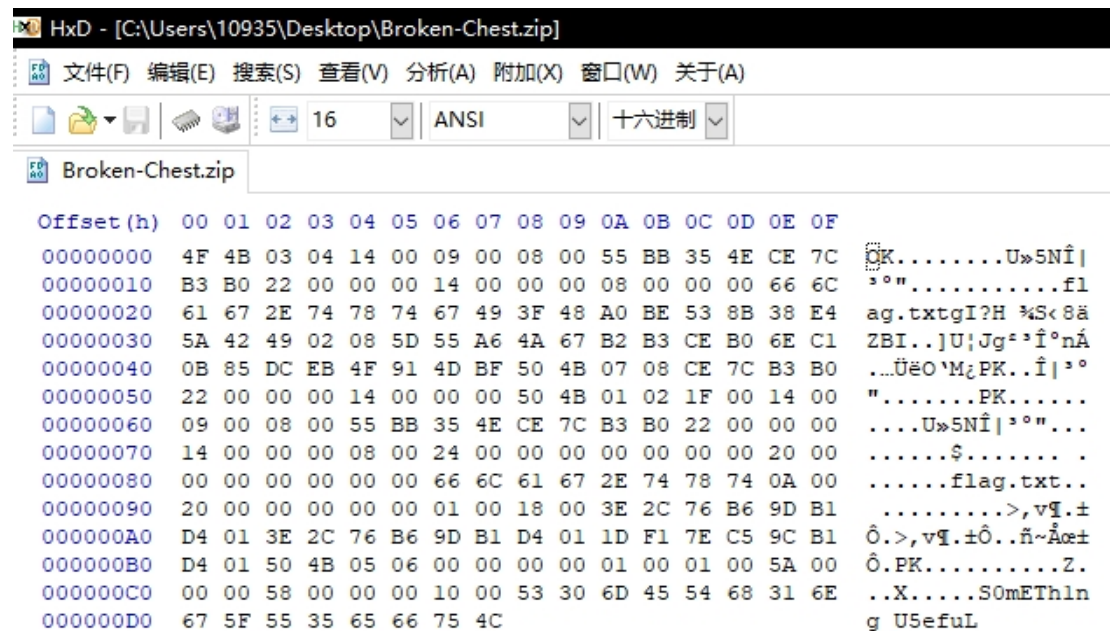
 lsb.py	2,033	871	Python source file	2019/1/24 20...	FAA82994
 power-source....	910,857	910,689	PNG 文件	2019/1/18 16...	79B67118

还不会 py 啊……那先把图片拖出来吧。扔进 stegsolve，查看颜色通道。突然，爆出了 flag。

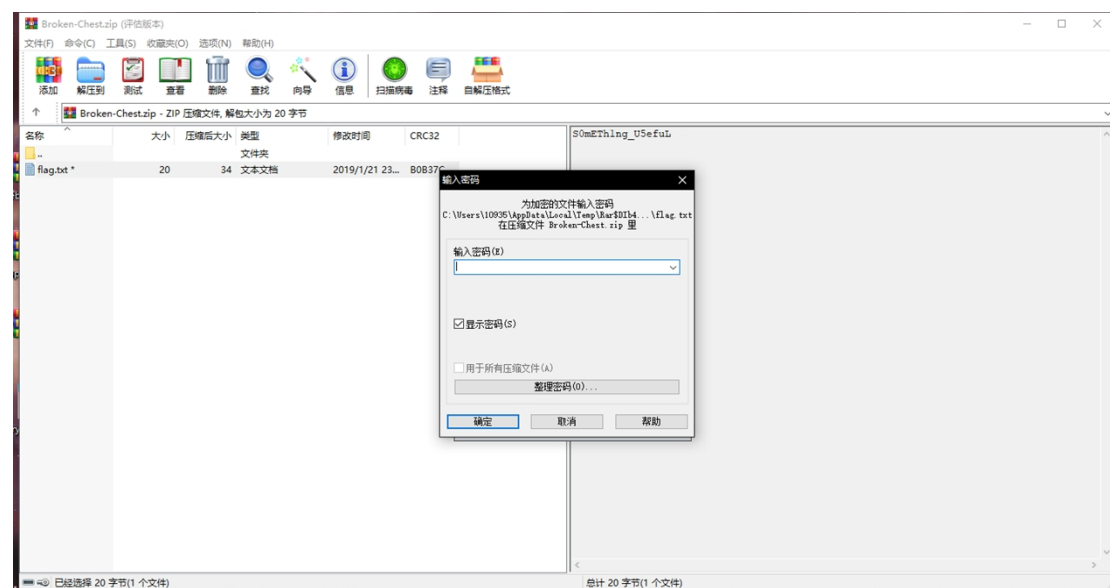


2. Broken Chest

又是一个压缩包。就像题目说的一样，坏掉了。用 HxD 查看 16 进制编码如下：



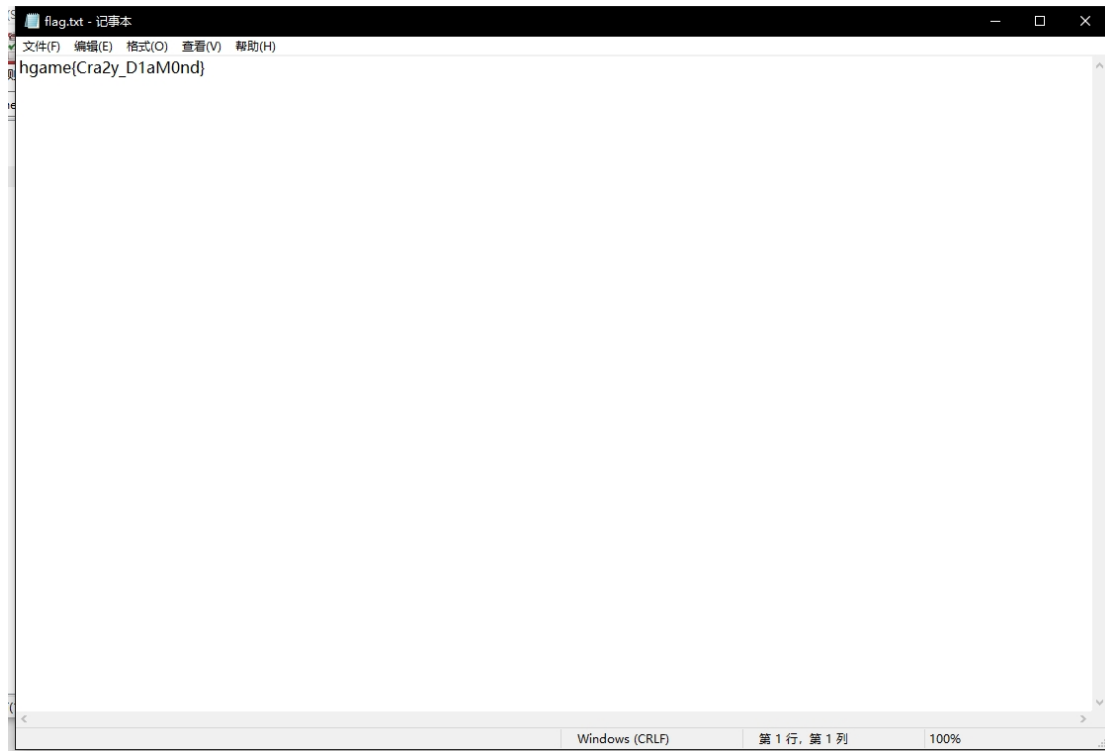
发现头部并不是 zip 文件的 50 4B 03 04，所以手动把 4F 改成 50，保存打开。



呃……需要密码。嗯……右边

S0mETHlng_U5efuL

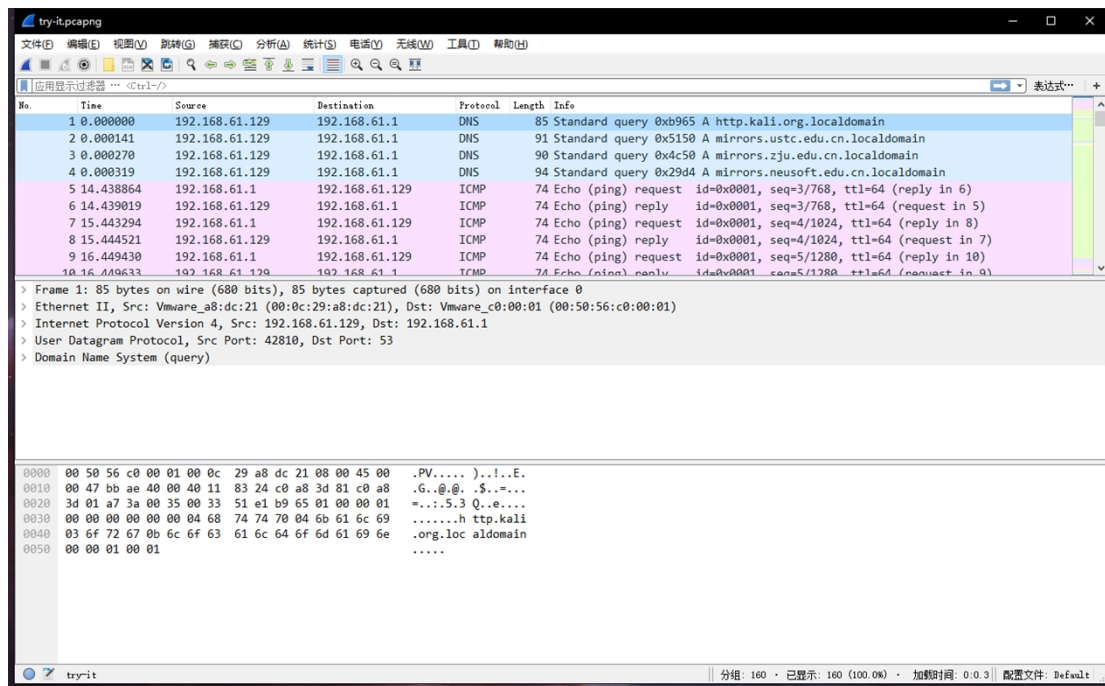
这是啥，试一试先。



意料之中，成功打开。果然是有用的…

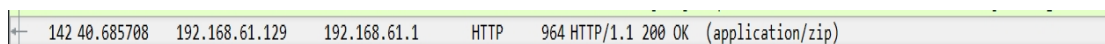
3.无字天书

下载得到一个.pcapng 的文件。由于一开始并不了解这东西，所以直接简单粗暴地改掉后缀为 zip。在此基础上，战斗多日未果。突然想起来，这后缀应该有故事。搜索 pcapng 文件相关的资料，终于明白了正确方向。使用 wireshark 打开下载的 try-it.pcapng。，

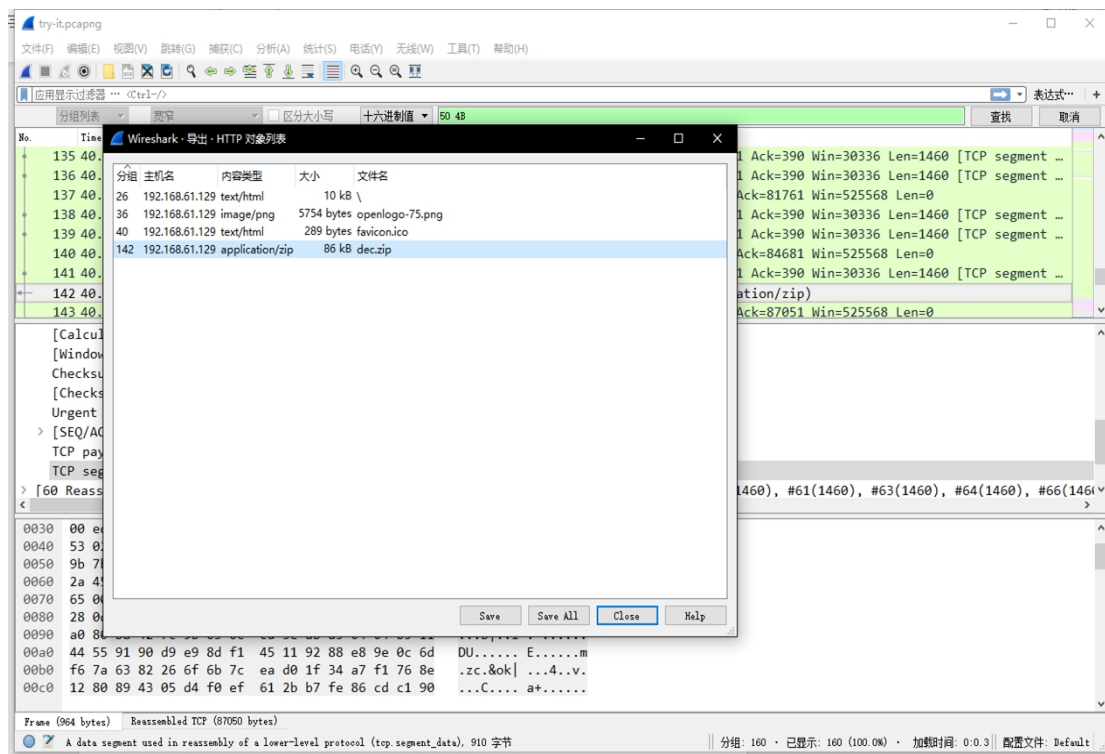


我猜应该会有个压缩包吧。我能想到的最简单的东西就是这个了。

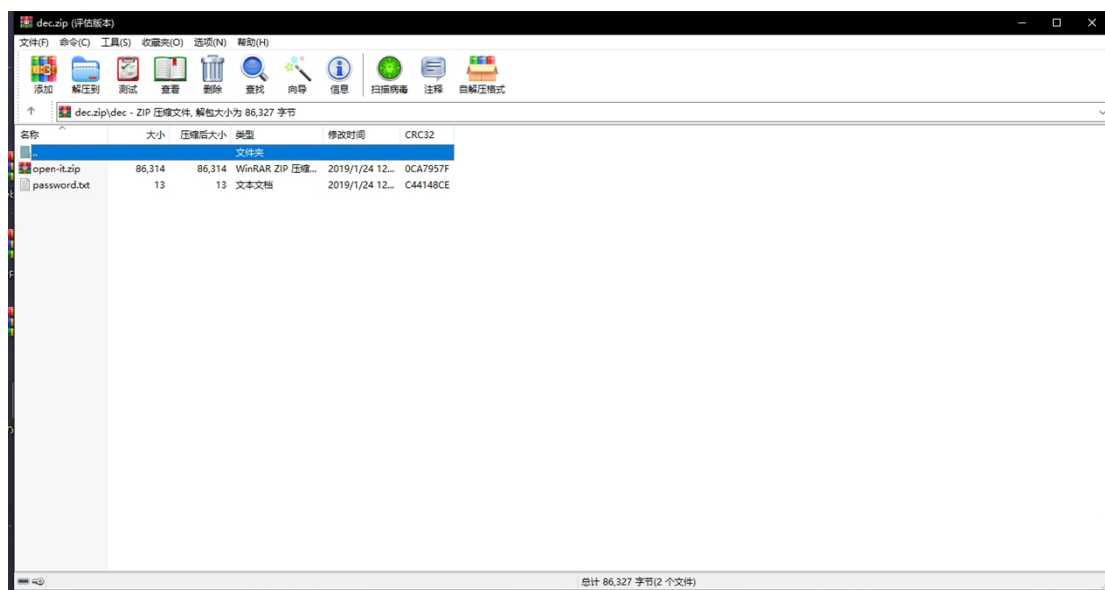
所以搜索 16 进制值 50 4B，真的发现一个压缩包。



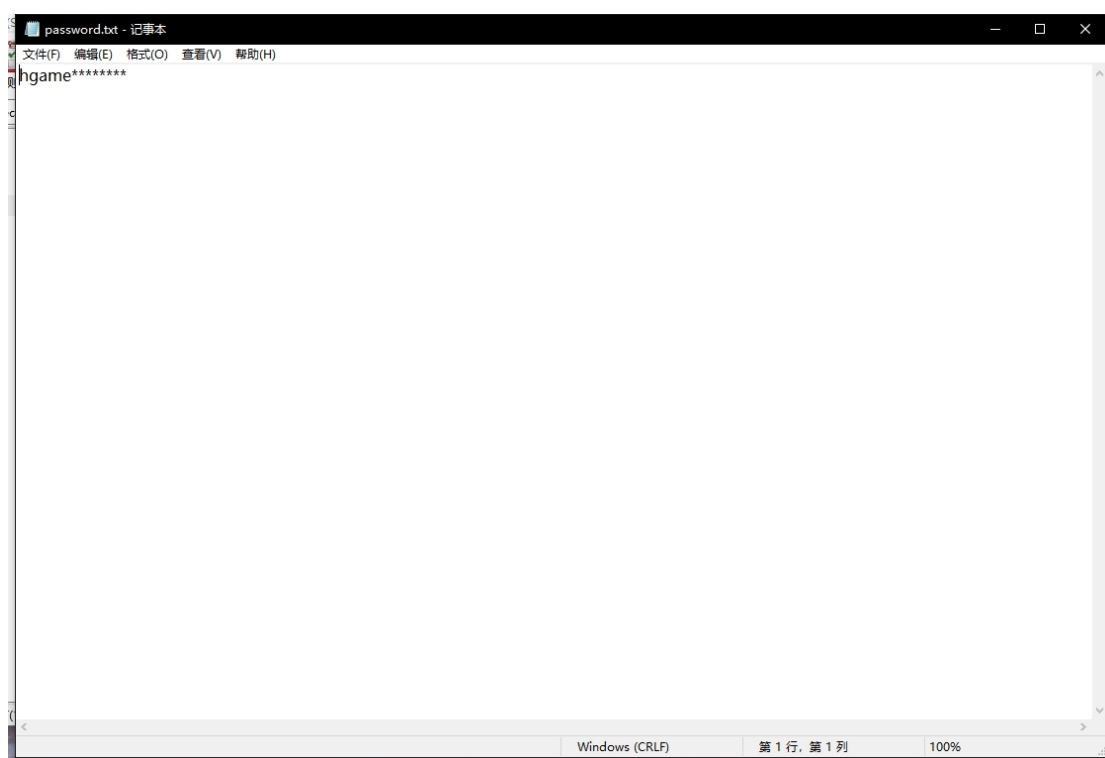
导出对象，



得到一个压缩包，打开发现有东西。



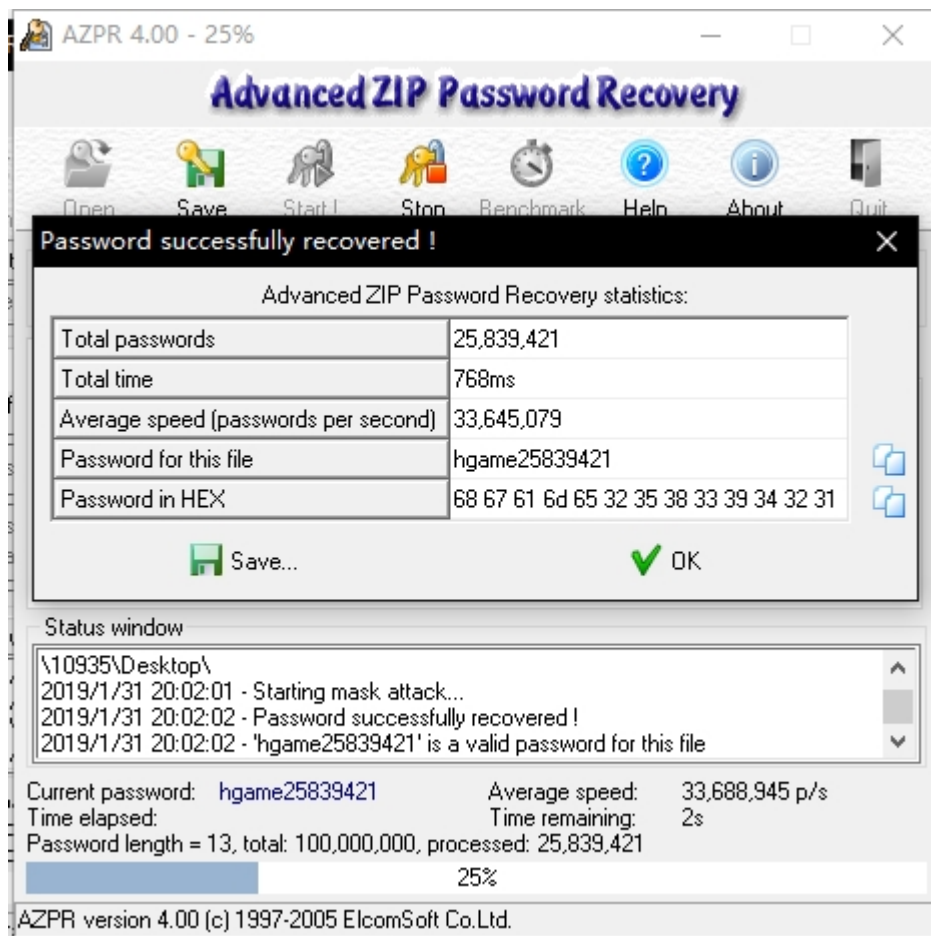
全拖出来，第一个需要密码，而恰好有一个 txt 文件叫 password，



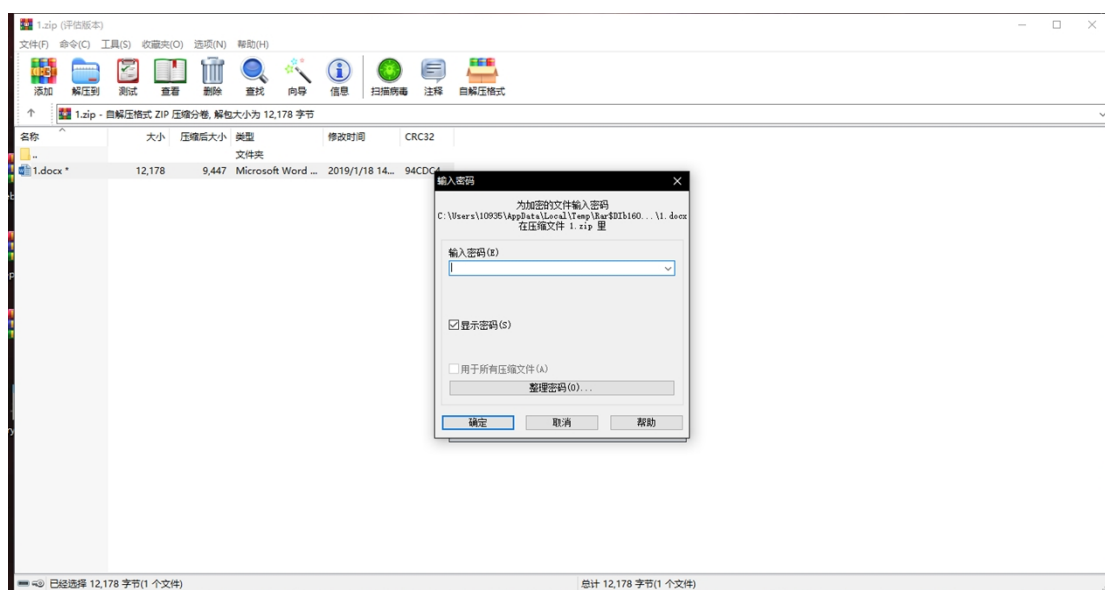
竟然给我看这个，一脸懵逼的我尝试着复制粘贴打开压缩包，当然不行。搜索过 ctf 压缩包解密方式后得知，这是典型的需要掩码攻击破解。于是打开 AZPR,



呃…好像有点久，出题的爷爷不会这么狠吧…那就一种一种来吧，最后在只选择数字时，破解得到了密码。



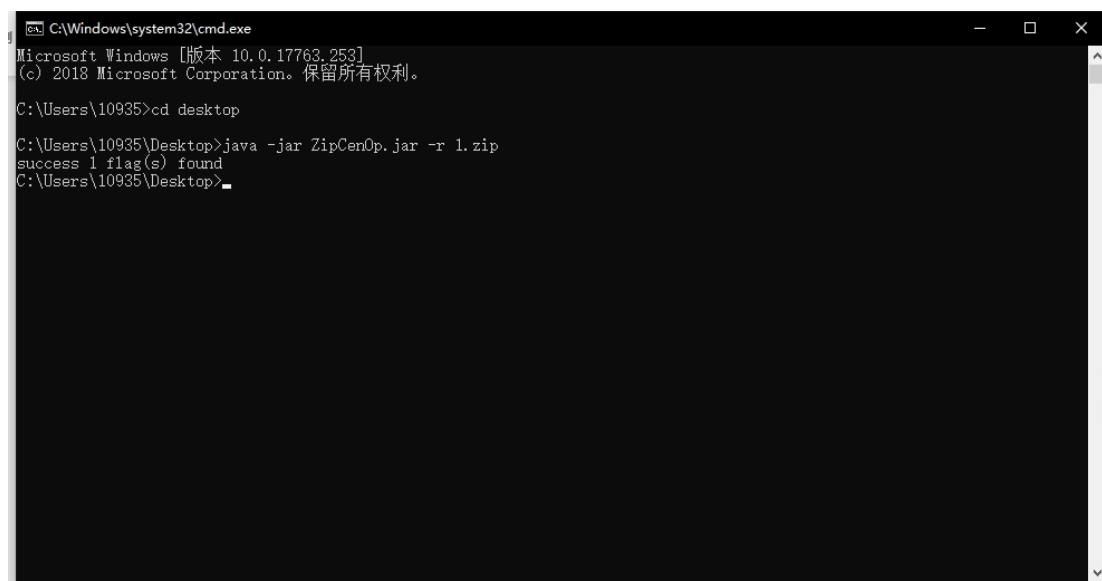
解密后打开压缩包，发现一张图片，小姐姐啊…jpg 文件，丢进 HxD，发现尾部不是 FF D9，所以是有东西的。简单粗暴的，后缀改成 zip，打开了。



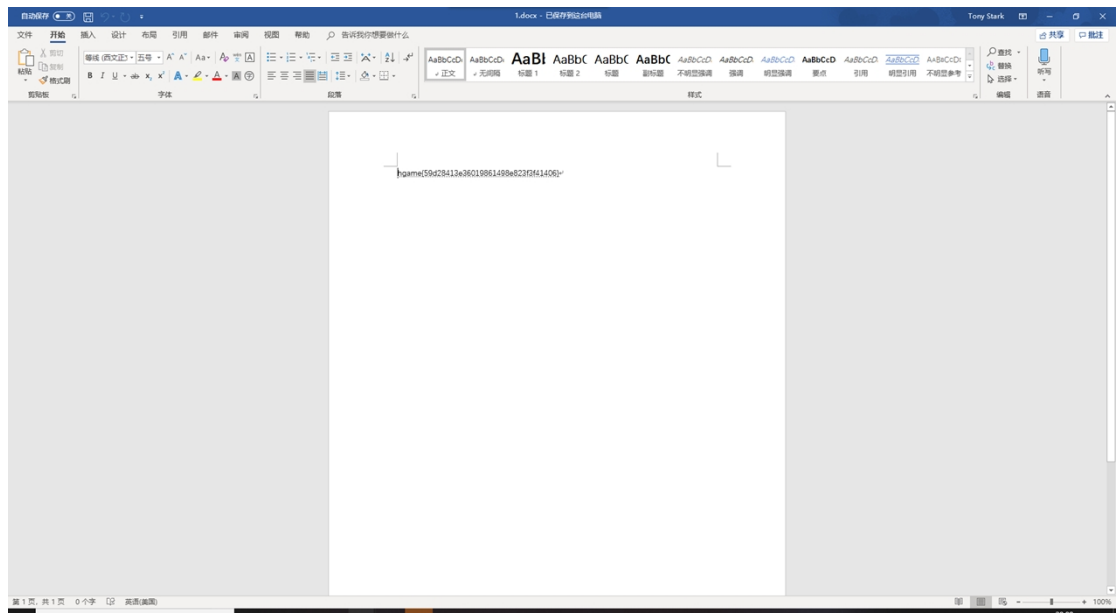
可是需要密码。用 zipperello 尝试破解，却没有发现加密文件，所以这是个伪加密无疑了。



伪加密已经遇到过很多次了，打开 cmd，



直接打开，呃，开不了，修复一下再打开，OK。



……这么长，会不会是什么加密来的，算了先提交试试吧，居然成功了…