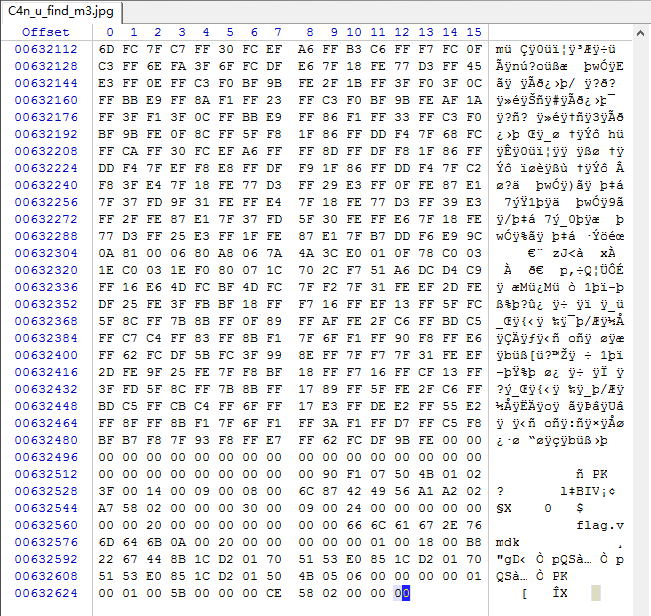
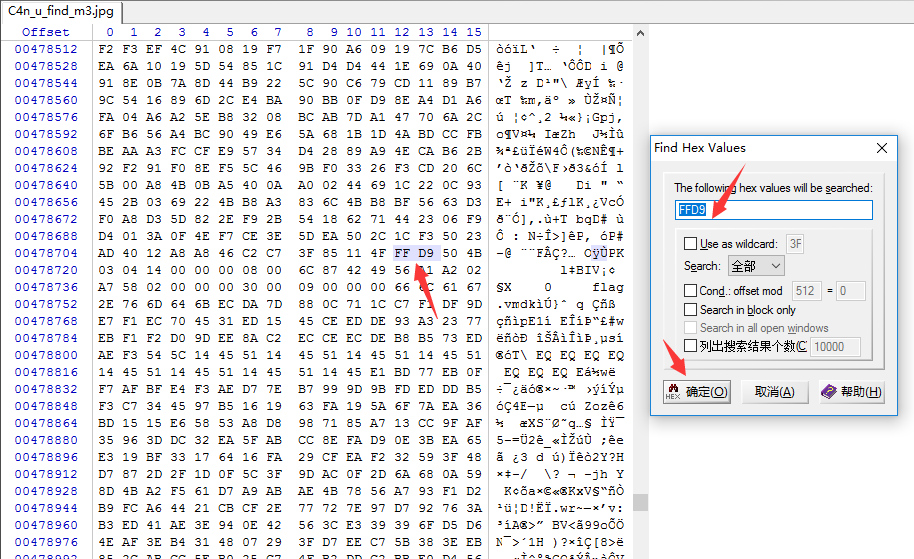
1、使用WinHex打开题图分析

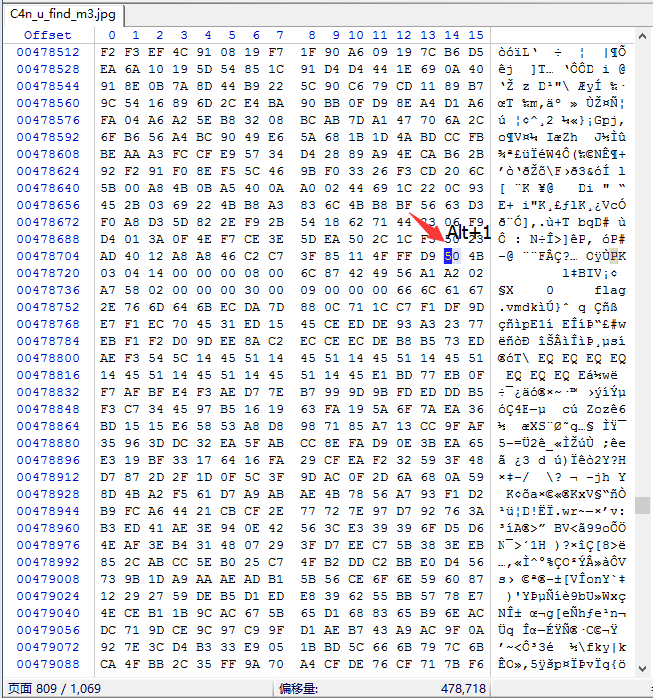


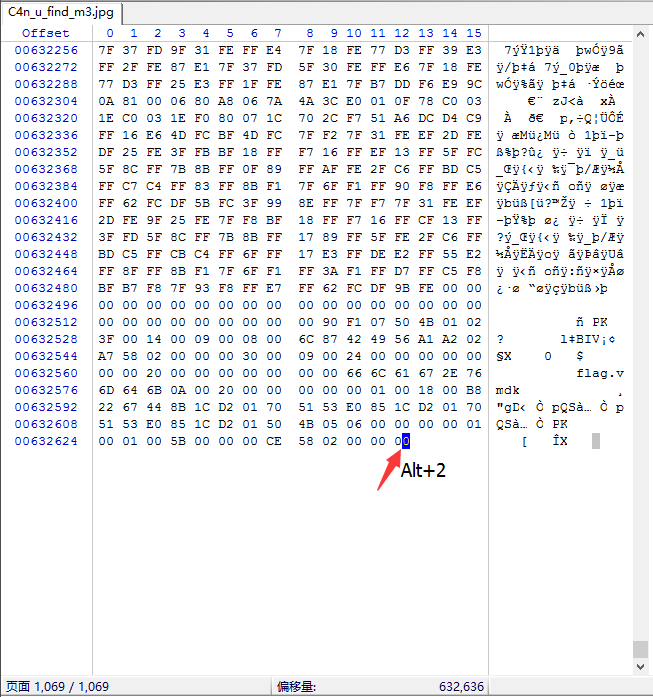
根据[JPG文件结构分析](http://blog.csdn.net/hnllei/article/details/6972858JPG文件结构分析)一文我们知道正常的jpg文件结尾应该是FF D9，但是文件最后却不一致，说明此文件结尾不在最后，而是在中间的某个部分，而之后数据应该是附加上的，因为图片查看器会忽视jpg结束标志符FF D9之后的内容，所以附加数据不会影响到图像的正常显示。

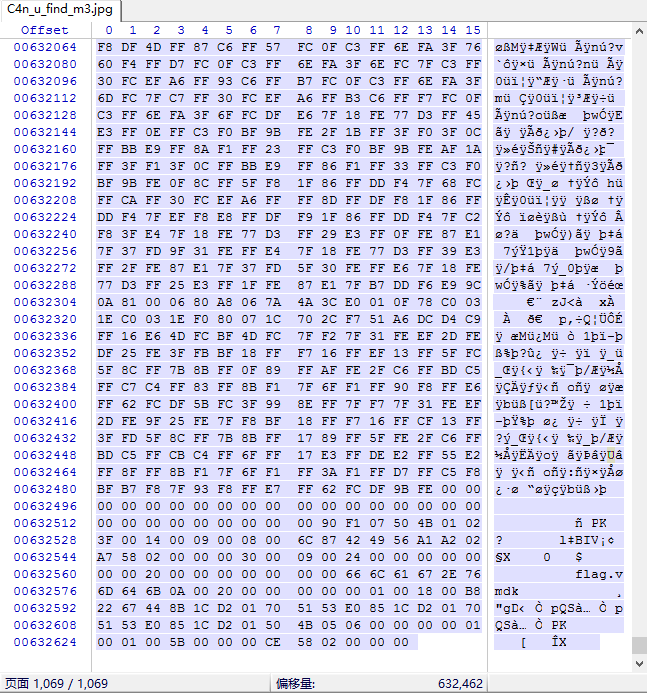
通过Ctrl+Alt+X快捷键查找jpg文件结束标志。



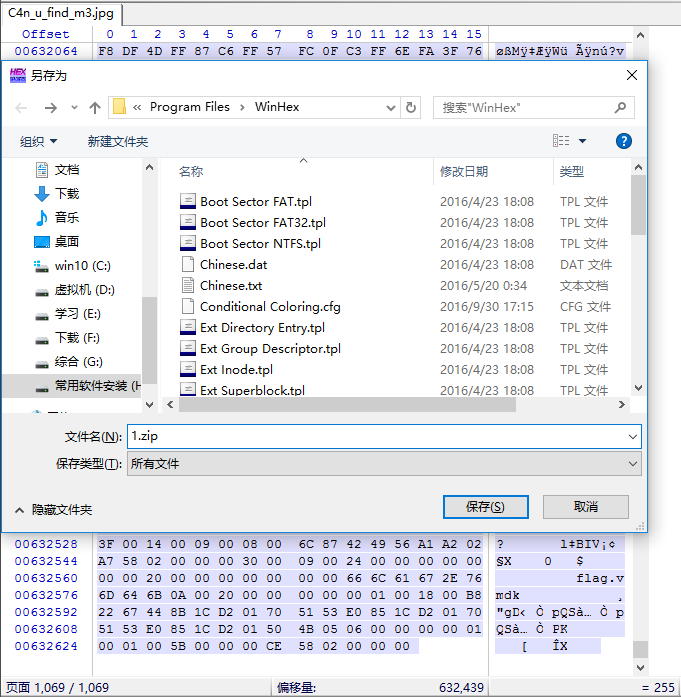
通过搜索引擎搜索，根据[zip文件格式说明](http://blog.sina.com.cn/s/blog_4c3591bd0100zzm6.html)一文知道0x04034b50（小端存储方式）是zip的文件头标识，于是将zip分离出来。



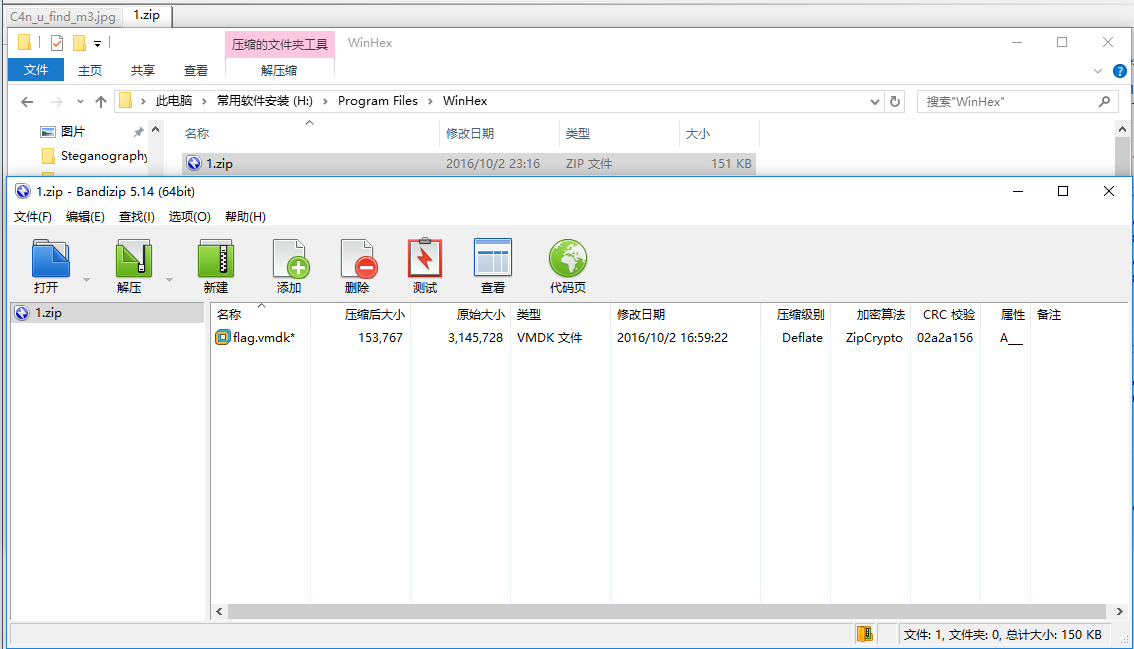




选中数据块之后Ctrl+Shift+N复制到新文件并命名为1.zip，保存。



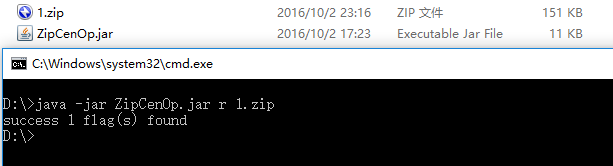
2、对zip文件去除伪加密



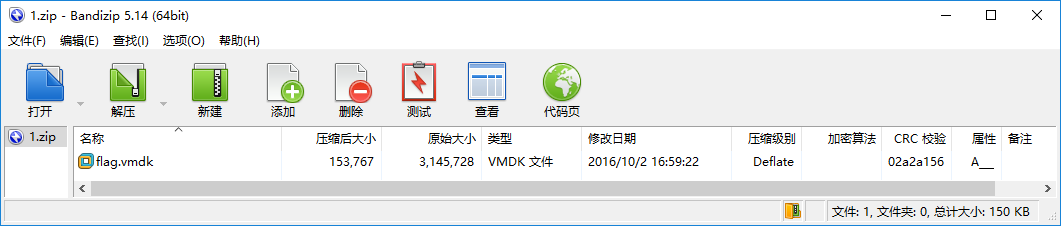
找到zip文件打开发现zip是加密的，但是当使用zip密码穷举工具如Ziperello尝试爆破密码时却提示zip没有加密，这说明zip是伪加密的。



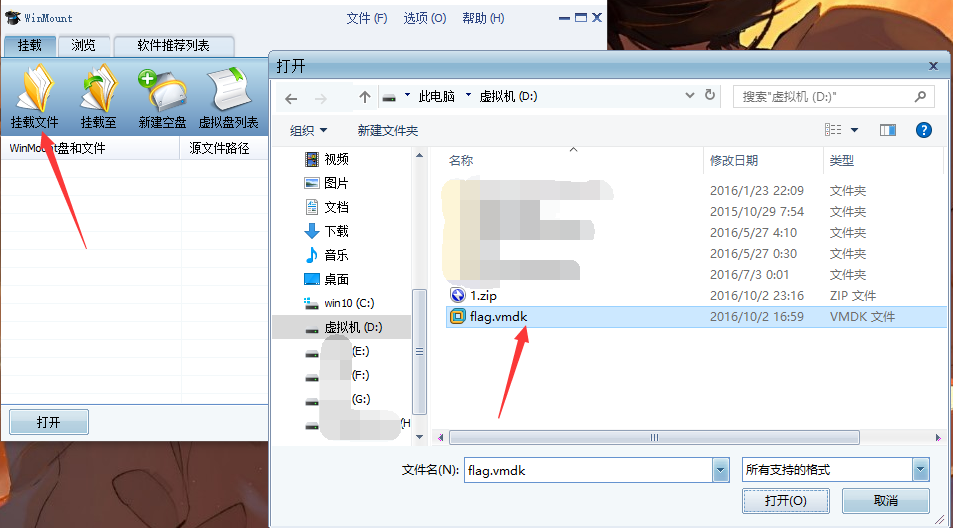
于是使用ZipCenOp工具尝试对zip文件去除伪加密处理。

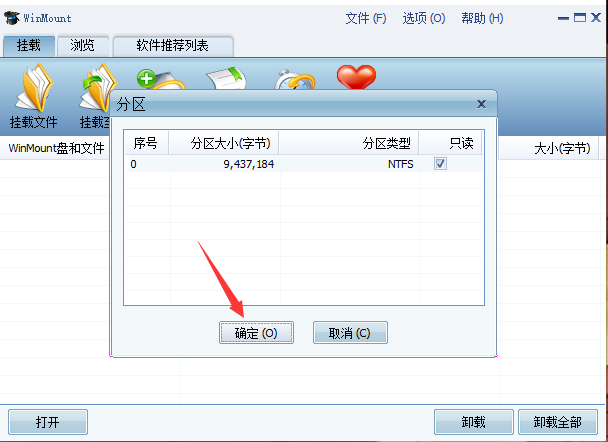


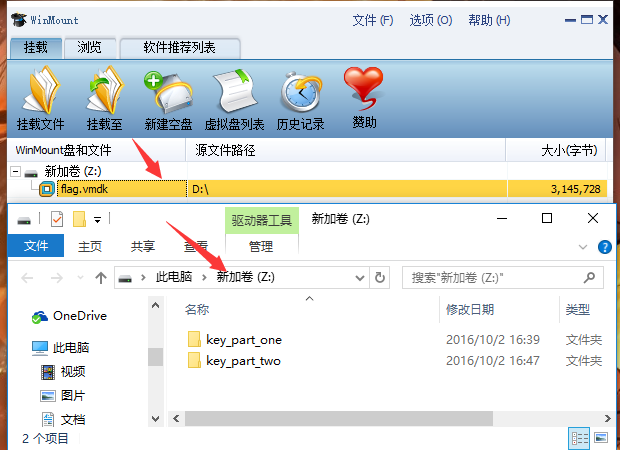
再次打开1.zip文件发现不在提示有加密。



解压并使用WinMount挂载flag.vmdk文件。



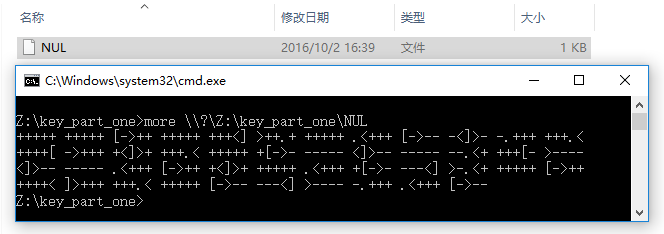




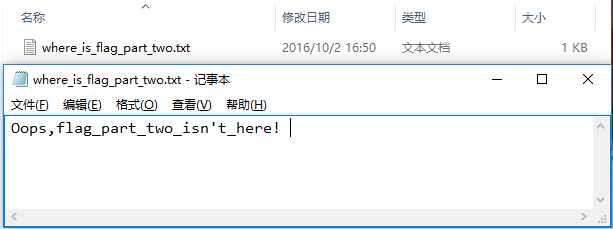
4、使用相应DOS命令查看隐蔽交换数据流和交换数据流

浏览发现两个目录key\_part\_one和key\_part\_two，打开key\_part\_one发现一个名为NUL文件，然而却不能通过正常的方式查看里面的内容。

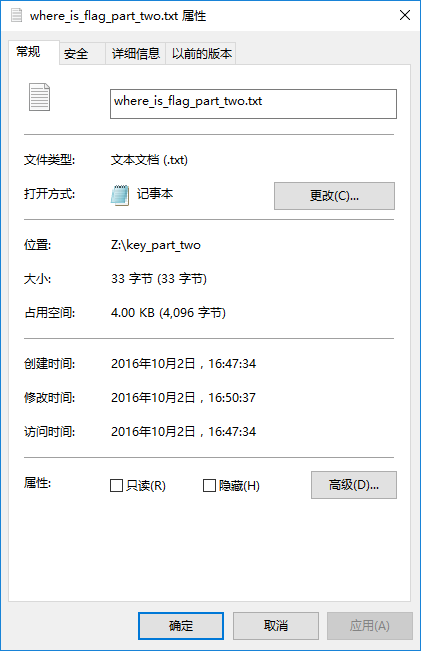
通过大量的搜索可以知道这是一种Windows下隐蔽交换数据流实现的数据隐藏，如果出于恶意目的可以使用这种方式将恶意软件、病毒、木马隐藏到正常的文件来逃过安全软件的检测并执行。虽然通过一般的方式不能正常访问，但是可以通过类似more \\?\Z:\key\_part\_one\NUL命令访问。（NUL是MSDN列出的保留设备名之一，保留设备名是用来将输出数据发送到周边硬件设备，命令中的“\\?\”表示取消字符串解析，并将文件直接发送到文件系统，通过融合保留设备名和“\\?\”前缀可以绕过标准的文件解析，直接创建一个以保留设备名命名的文件）



打开key\_part\_two目录，打开where\_is\_flag\_part\_two.txt文件却提示flag不在里面。

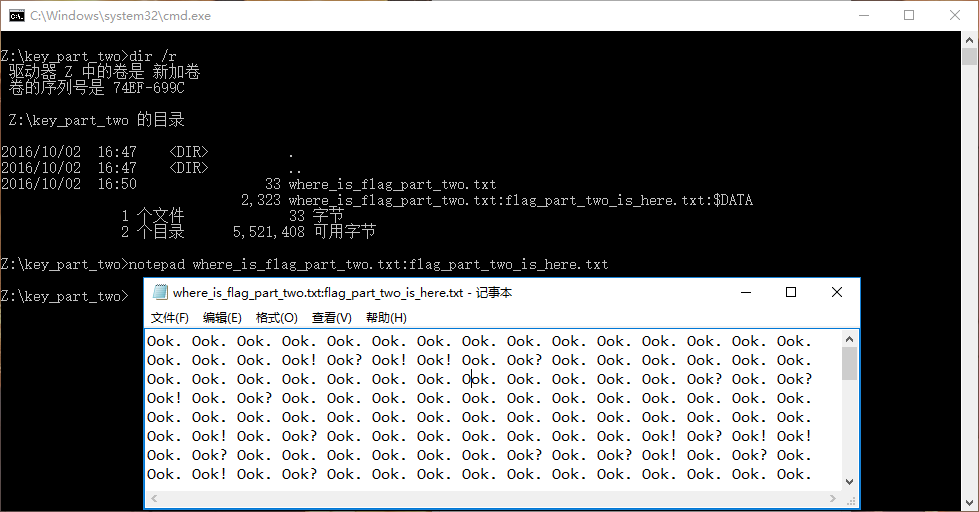


当查看where\_is\_flag\_part\_two.txt的属性时发现文件大小和占用空间相差很大。



通过大量的搜索可以知道这是通过Windows NTFS文件系统的交换数据流方式实现的数据隐藏，利用这种方式可以做许多恶意攻击，详细利用方式可以参考[一个用ADS（供选数据流）隐藏Windows后门的方法](http://www.freebuf.com/articles/73270.html) 和[NTFS ADS（NTFS数据交换流） 带来的WEB安全问题](http://www.xcl0ud.net/?p=9) 等文章。

可以通过以下命令访问交换数据流：



5、解码隐藏的数据

通过搜索可以知道两部分文本内容分别是brainfuck和Ook编程语言编码的结果，通过[在线解码](https://www.splitbrain.org/_static/ook/) 分别得到flag两部分，组合得到完整的flag。

