《防病毒技术》

实验报告

姓名： 包xx

学院： 计算机学院

班级： 信安14-xx班

学号： 0814xx

指导老师： 朱xx

实验一 PE结构分析

一、实验目的

1. 掌握PE分析工具的使用方法；

2. 练习Win32汇编编程；

二、实验要求

1. 结合上课内容，独立完成编码、调试，要给出测试数据和实验结果。

2. 整理上机步骤，总结经验和体会。

3. 完成实验报告，提交程序源码。

4. 写出PE分析工具的使用过程，实例分析。

5. 完成实验思考题。

三、实验内容

1、手工或编程从user32.dll中获得MessageBoxA的函数地址；

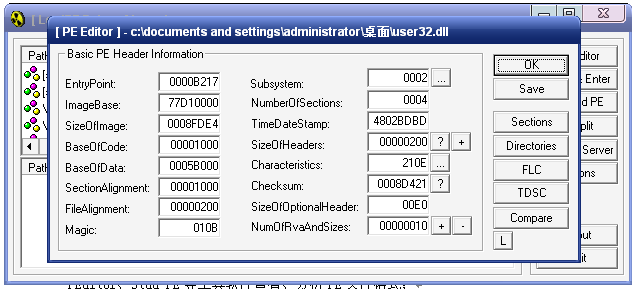
2、查阅资料，结合第2章内容，根据PE结构编写一个小的工具软件，或者用PE Explorer、PEditor、Stud\_PE等工具软件查看、分析PE文件格式；

3、针对PE文件格式，请思考：Win32病毒感染PE文件，须对该文件作哪些修改？

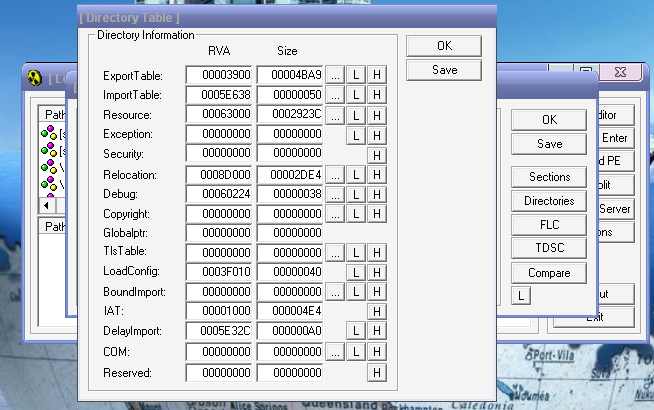
四：实验过程：

1、手工或编程从user32.dll中获得MessageBoxA的函数地址；

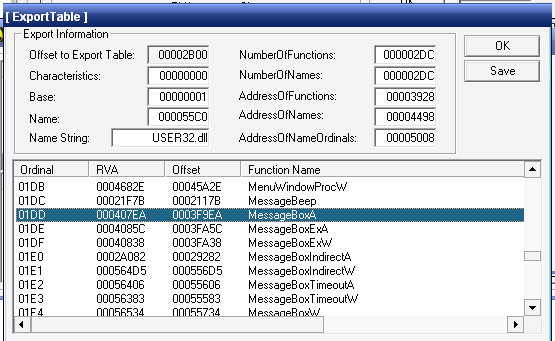
下载LOADPE，打开user32.dll。



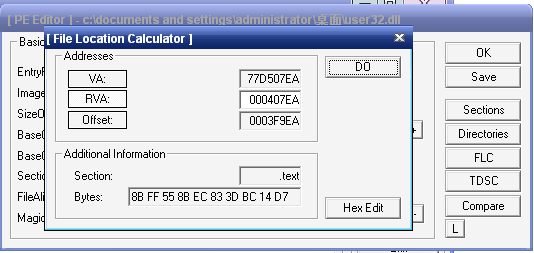
打开目录表



进入输出表，在输出表中即可找到MessageBoxA的信息，Ordinal为01DD，RVA为000407EA，Offset为0003F9EA。



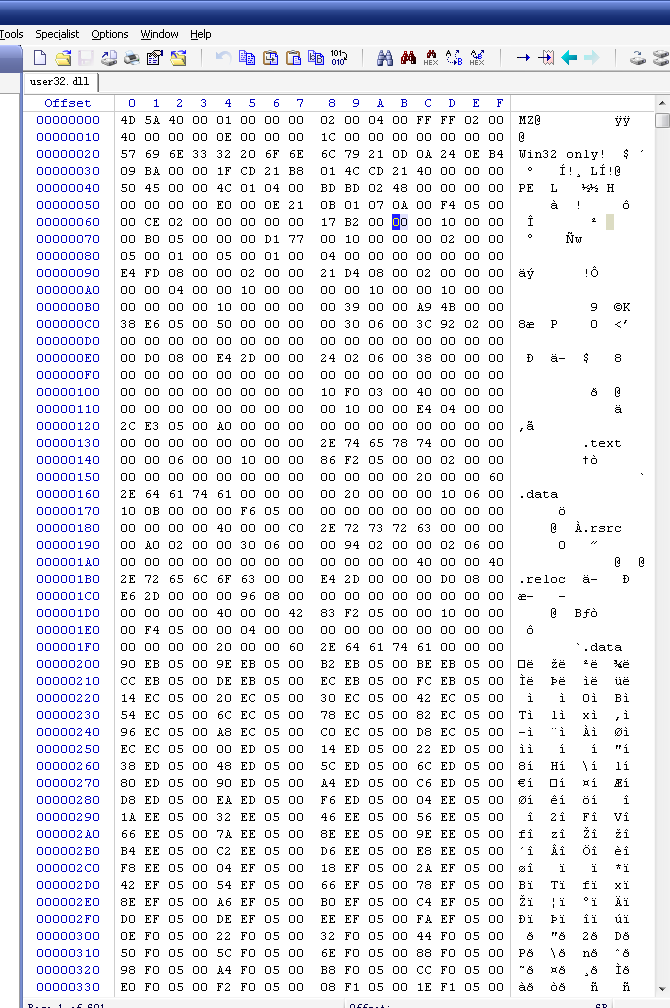
利用LoadPE自带的位置计算器就可以计算出MessageBoxA的函数地址，为77D507EA。



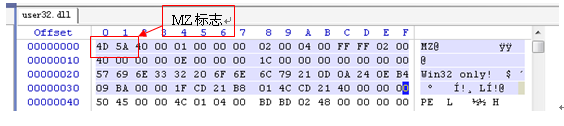
2、查阅资料，结合第2章内容，根据PE结构编写一个小的工具软件，或者用PE Explorer、PEditor、Stud\_PE等工具软件查看、分析PE文件格式；

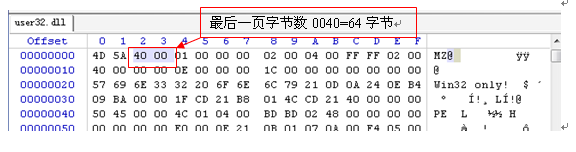
使用winhex打开user32.dll文件。、

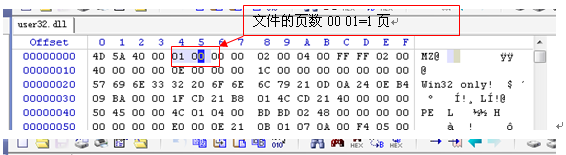
可以看到PE文件首部包括DOS头（MZ文件头），PE文件头，可选映像头，数据目录表等

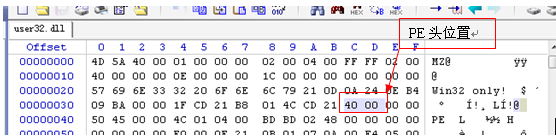


其中，MZ文件头占64个字节，最开始时是MZ标志，然后是最后一页的字节数，文件的页数，重定位地址（PE头开始）等。

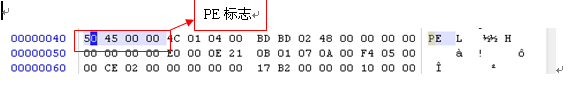


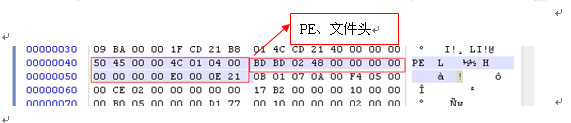




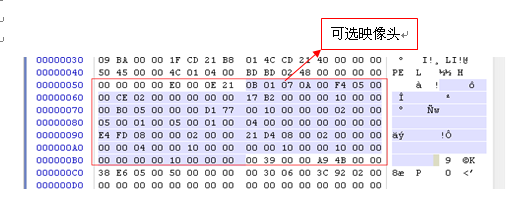


接下来是PE文件头，

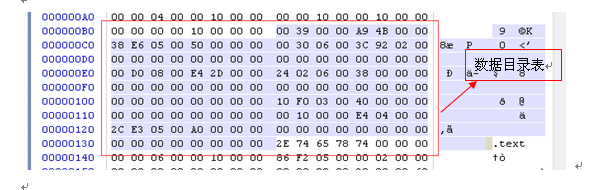




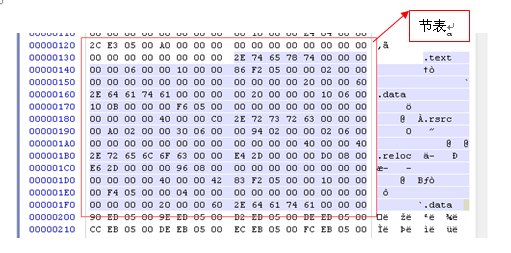
PE文件头之后就是可选映像头，包含了PE文件的逻辑分布信息。



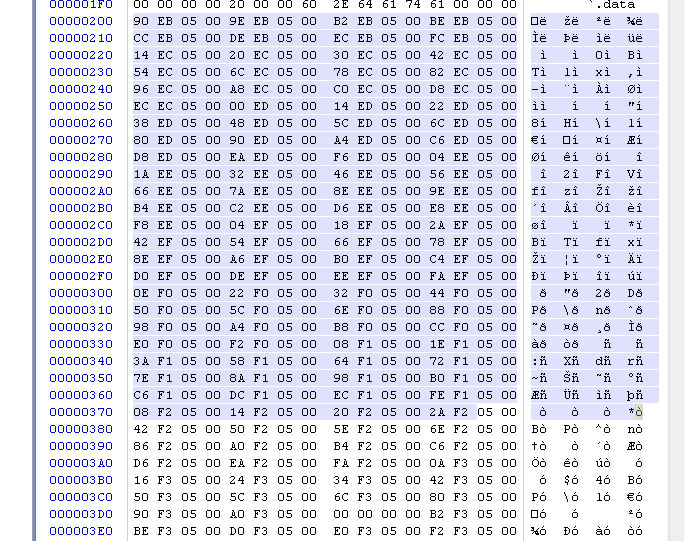
接下来是数据目录表：



160个字节的节表，有代码节.text，数据节.data，资源节.rsrc，重定位节.reloc，



余下的为节和调试信息。



3、针对PE文件格式，请思考：Win32病毒感染PE文件，须对该文件作哪些修改？

1.节表，病毒将自身写入节表，就需要写入节名，节的实际字节数，偏移地址，对齐后的大小以及本节开始的位置，则节表中会发生改变。

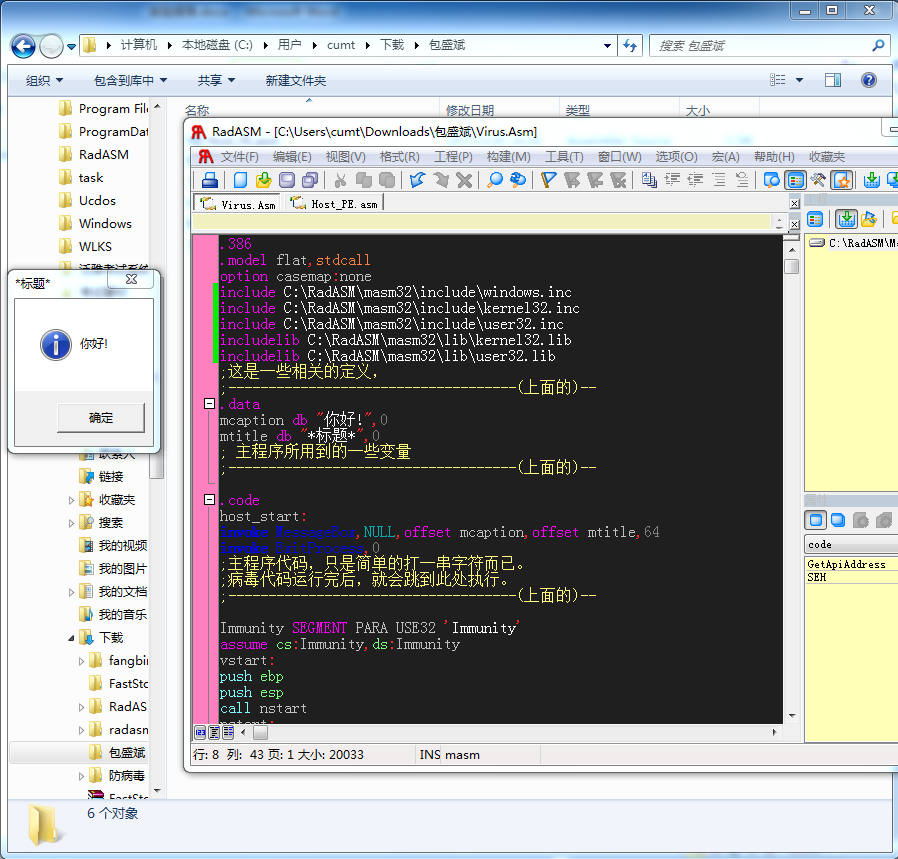
2.映像文件头的节表数目：因为节表发生的改变，所以，印象文件头中的节表也需要进行更改。

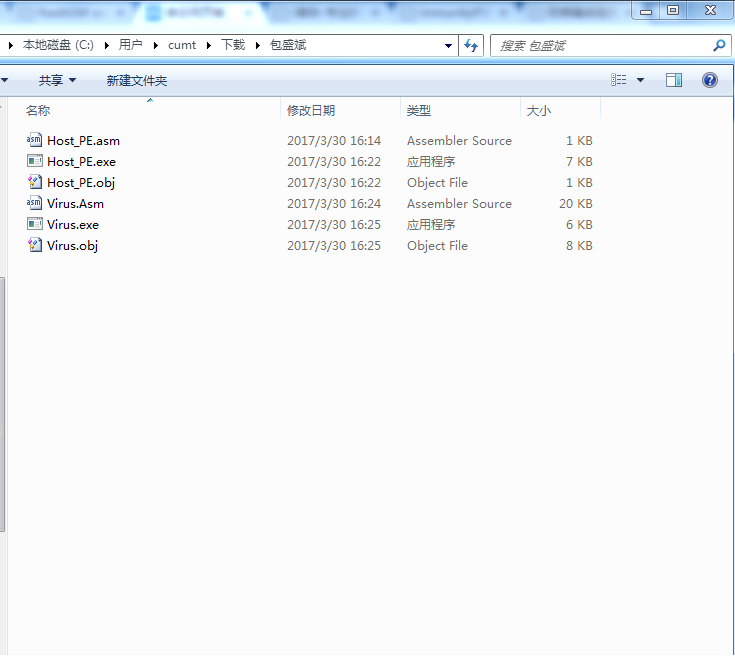
3.更新SizeOfImage（内存中整个PE映像尺寸=原SizeOfImage+病毒节经过内存节对齐后的大小）

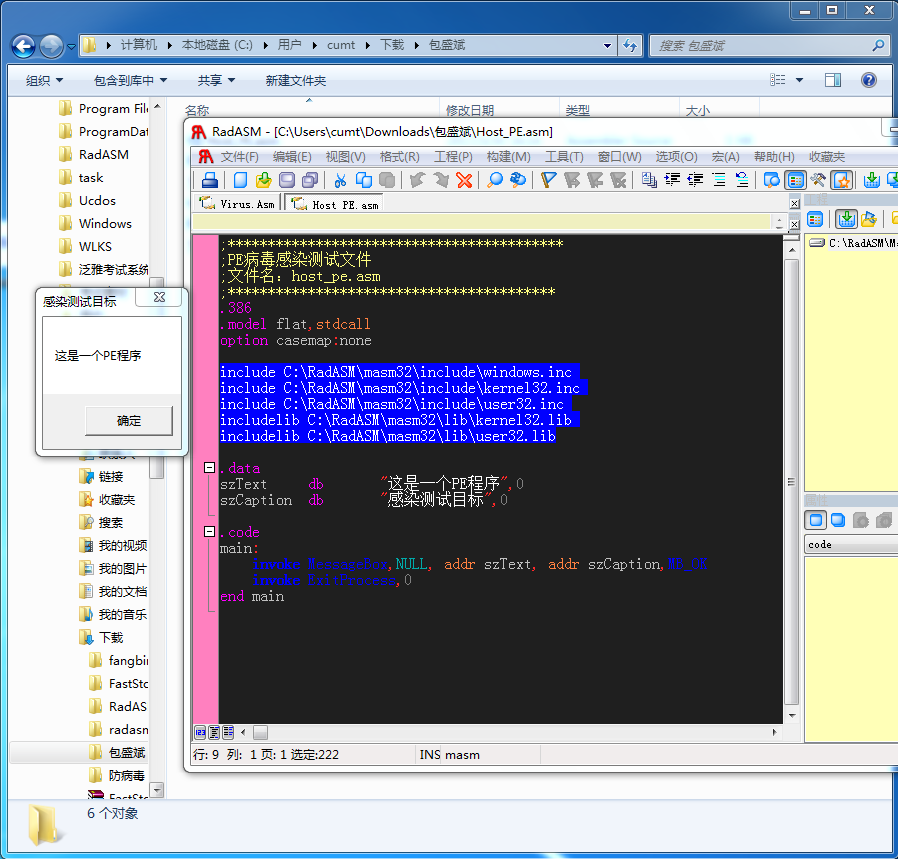
4.PE文件头：被写入了感染标记，病毒代码被加入到了新节中，并将当前位置设置为了文件末尾

实验二

1、更改include路径

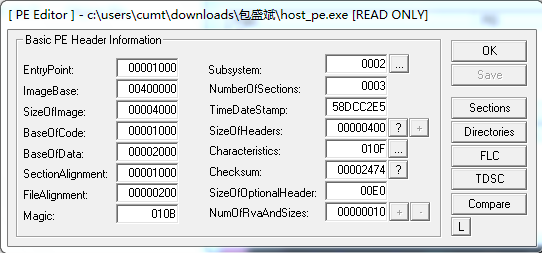


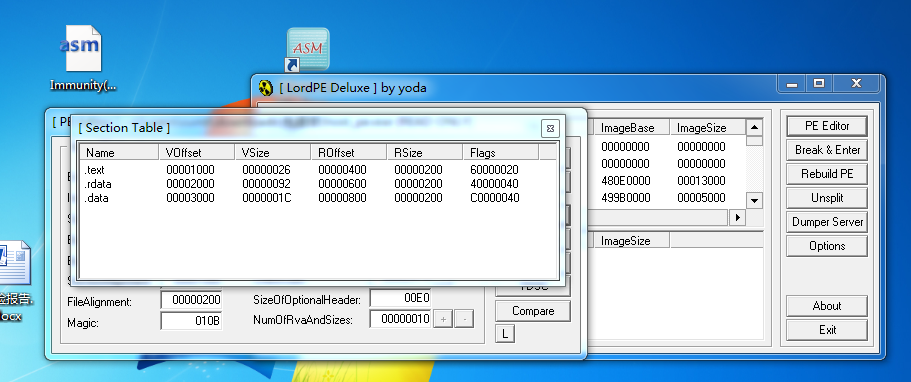




2、用LoadPE打开未感染的host\_pe.exe，入口地址为00001000，

其节表只有三个





3、用LoadPE打开感染的host\_pe.exe，入口地址为00004000，

其节表变为四个

