实验三 PE文件结构分析

实验目的：

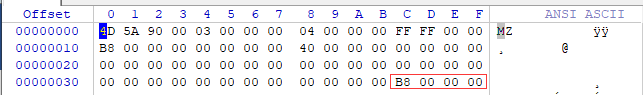
1. 验证局部变量的机制
2. 验证PE文件头结构
3. 验证PE文件目录结构
4. 验证PE文件节表结构

实验内容：

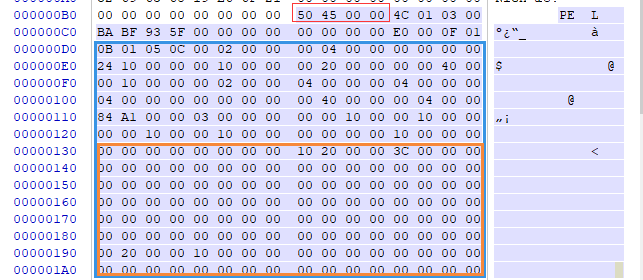
1. 编写程序，要求：1）在数据区定义10个单元的word数组，初始化为确定的数值；2）含1个子程序，在子程序中定义10个单元的word数组，将数据区定义的数组赋给子程序定义的数组；在主程序中调用子程序，记录堆栈变化情况。
2. 在1编写程序的基础上，加入调用MessageBox函数生成exe文件，利用Winhex、OD分析该exe文件的结构；

实例：

1.用Winhex打开文件：



2.找到PE文件头位置（0x000000B8），跳转到这个位置：

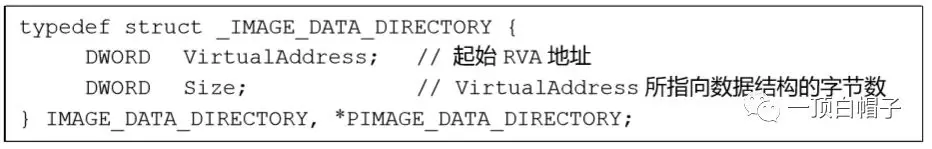


可以看到：

* PE文件标志PE00（4H字节）
* 映像文件头（14H字节）：可以看到4c 01 03 00，其中0x0003表示有3个节（之后手算地址需要用到）
* 可选映像头（0e0H字节），其中包含数据目录表（80H字节）

3. 数据目录表中第二项（导入目录）为：10 20 00 00 3C 00 00 00

根据其结构：

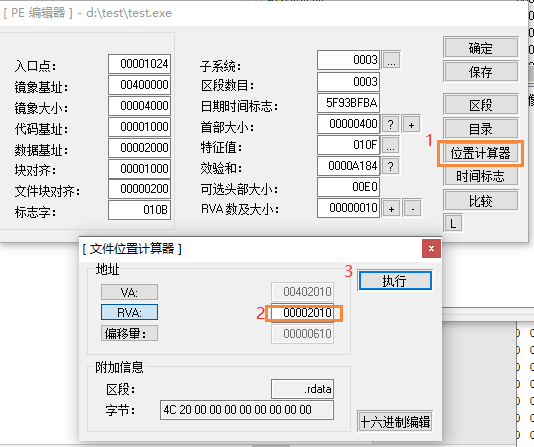


易知：

* 起始RVA地址：0x00002010
* 所指结构的字节数为：0x0000003C

4.由于地址为RVA（相对虚拟地址），因此需要转换：

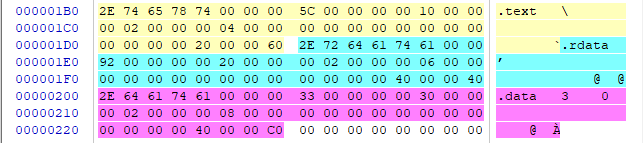
* 方法一：使用工具LordPE



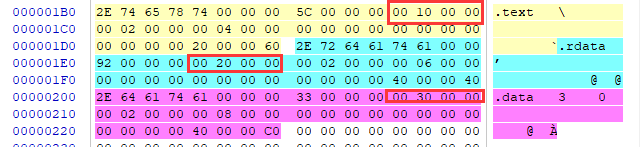
其中偏移量0x00000610即是我们需要的地址。

* 方法二：手动计算

a. 打开节表（紧接PE文件头）

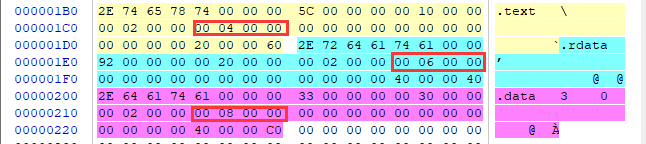


可以看到有三个节。



主意红色标记的三个地址，为该节的RVA地址，可以看出：

0x00002000 < 0x00002010 (导入目录地址) < 0x00003000，因此导入目录在.rdata节中。



这里的三个地址为本节的原始数据在文件中的位置，主要看.rdata的地址为：0x00000600。

综上，可得地址转换公式：

导入表的RVA减去导入表所在的节的RVA再加上引入表所在的节在文件中的位置。

于是可得：

地址 = 0x00002010 – 0x00002000 + 0x00000600

= 0x00000610.（可以看到，和LordPE计算的一样）

跳转到该地址：

