**实验4 读取PE文件的输入表和输出表**

1. **实验目的**
   1. 熟悉PE文件的输入表和输出表结构；
2. **实验原理**
   * 1. **输入表**

在 PE文件头的 IMAGE\_OPTIONAL\_HEADER 结构中的 DataDirectory(数据目录表) 的第二个成员就是指向输入表。

每个被链接进来的 DLL文件都分别对应一个 IMAGE\_IMPORT\_DESCRIPTOR (简称IID) 数组结构。输入表的结构如图1所示。

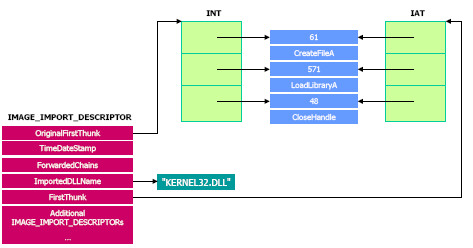


图 1 输入表结构

* + 1. **输出表**

在 PE文件头的 IMAGE\_OPTIONAL\_HEADER 结构中的 DataDirectory(数据目录表) 的第一个成员就是指向输出表。

输出表是用来描述模块中导出函数的数据结构。如果一个模块导出了函数，那么这个函数会被记录在输出表中。输出表的结构如图2所示。

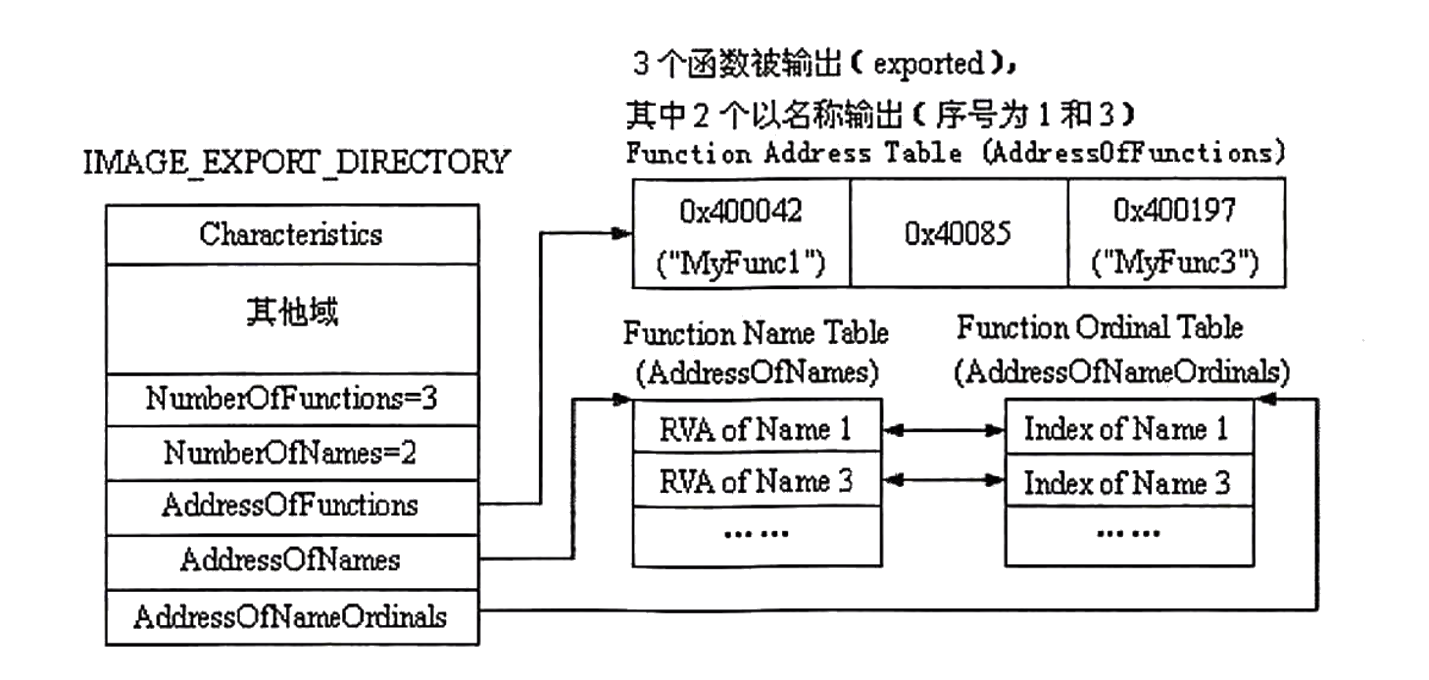
****

图 2 输出表的数据结构

1. **实验环境**

Windows操作系统，MASM32编译环境。

1. **实验内容：**

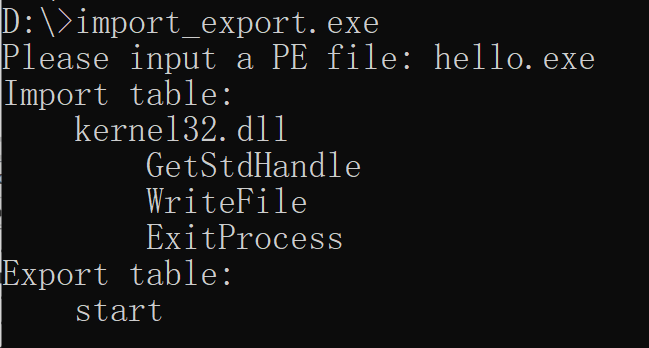


图 3 输入表和输出表实验演示

* + 1. 输入PE文件的文件名，调用Windows API函数，打开指定的PE文件；
    2. 读取PE文件的输入表，显示输入表中引入的DLL文件名和对应的库函数名字；
    3. 读入PE文件的输出表，显示导出函数的函数名；

1. **实验报告**
   * 1. 描述PE文件的**输入表**的作用和数据结构
     2. 描述PE文件的**输出表**的作用和数据结构
     3. 程序的汇编语言源代码和**注释**
     4. 程序测试时，输出结果的截图
     5. 讨论输入表的安全问题