实验二 PE文件结构分析

# 实验目的

1．了解PE文件的输入表结构；

2．手工解析PE文件的输入表；

3．编程实现PE文件输入表的解析。

# 实验内容

1. **第一步：手动解析输入表结构**
2. 使用工具箱中的工具everything,寻找当前系统中任意一个exe文件，文件名称是：
3. 使用LordPE“PE编辑器”打开exe文件，确定可选头部大小是：00E0（00F0则是64位文件，请返回第一步重新选择exe文件），点击“目录”，确定输入表的RVA，截图如下（图1）：
4. 点击PE编辑器右侧的“位置计算器”，得到文件偏移值，截图如下（图2）：
5. 使用16进制编辑工具，跳转到相应的输入文件偏移地址，输入表是每个IID对应一个DLL，根据IID大小，这里取20字节的数据进行分析，将输入表第一个IID结构的数据与IID结构体的成员一一对应，具体如下所示：

IMAGE\_IMPORT\_DESCRIPTOR {

OriginalFirstThunk =

TimeDateStamp =

ForwarderChain =

Name =

FirstThunk =

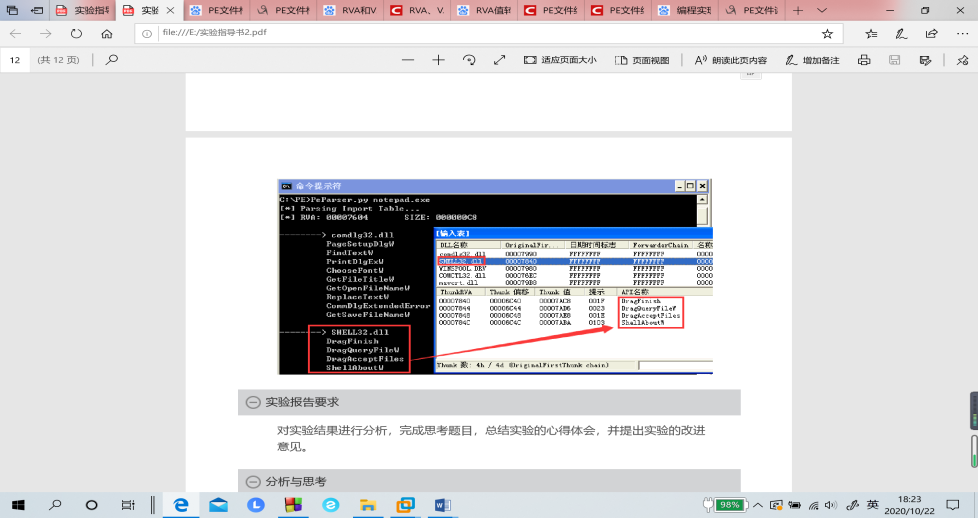
}

1. 关注OriginalFirstThunk和Name两个成员，其中Name是一个RVA，用步骤**(3)**的方法得到其文件偏移值为 ，在16进制编辑工具转到这个偏移地址，可见输入表的第一个DLL名为 ，截图如下（图3）：
2. 分析一下OriginalFirstThunk，它指向一个类型为IMAGE\_THUNK\_DATA的数组，上面已经分析出了它的值为 ，这是一个RVA，用步骤**(3)**的方法得到文件偏移地址 。在16进制编辑工具转到这个偏移地址，其中前面4个字节的数据为 ，截图如下（图4）：
3. 可以看出，这是 （填“以名字”或“以序号”）的方式输入函数；
4. 以名字的方式则用与步骤**(3)**相同的方式在16进制编辑工具中对应IMAGE\_IMPORT\_BY\_NAME结构的数据，可以看到函数的输入序号为 ，函数名为 ，截图如下（图5）：
5. 以序号的方式则可知道其调用的是系统内 号函数（转十进制）
6. 验证：使用LordPE单击“目录表”界面中输入表右侧的“…按钮”，打开输入表对话框，可以验证获取的DLL名和函数名/序号值是否正确。截图如下（图6）：
7. **第二步：编程实现输入表的解析**

程序要求：

调用程序解析PE文件输入表，输出**输入表大小，RVA，以及调用的每个dll的名称和相应的调用的函数名称**。

1. 从数据目录表的第二项读取输入表的RVA以及大小，找到第一个IID的文件偏移位置，获取IID的数据，获取IID中Name成员的RVA值和OriginalFirstThunk的RVA值，循环直到得到一个空的IID，表明这是最后一个IID，结束解析循环；
2. 将步骤(1)中获得的Name的RVA转换为文件偏移值，并读取DLL的名字
3. 解析IID对应的INT数组。将步骤(1)中OriginalFirstThunk的RVA值转为文件偏移值，指向一个类型为IMAGE\_THUNK\_DATA的数组，判断输入函数方式。循环获取IID对应的IMAGE\_THUNK\_DATA结构，等于0,表示是最后一个IMAGE\_THUNK\_DATA，结束循环。
4. 运行程序即可看到输入表的解析结果，与LordPE的解析结果是否一致，输出参考与验证截图示例如下：



完成以下函数使程序运行成功，并给出结果截图

Is\_valid\_pe:检查文件合法性并读取数据，主要检查MZ标志和PE标志来校验合法性，随后读取数据目录表到self.data\_dirs，读取节表头到self.sec\_hdrs

parse\_import\_table：输入表结构解析。

rva\_to\_offset：RVA转偏移地址

parse\_iid\_int：解析每个IID对应的IMAGE\_THUNK\_DATA类型的INT数组

参考代码：

# -\*-coding:utf-8-\*-

import sys

import struct

class PeParser:

def \_\_init\_\_(self,file\_path):

self.MZSIG = b'MZ'

self.PESIG = b'PE\0\0'

self.path = file\_path

#将十六进制数据转换为小端格式的数值

def get\_dword(self, data):

return struct.unpack('<L', data)[0]

#提取ASCII字符串

def get\_string(self, ptr):

beg = ptr

while ptr < len(self.data) and self.data[ptr] != 0:

ptr += 1

return self.data[beg:ptr]

def parse(self):

self.read\_data()

if not self.is\_valid\_pe():

print("[Error] Invalid PE file")

self.parse\_import\_table()

#读取文件数据

def read\_data(self):

fd = open(self.path, "rb")

self.data = fd.read()

fd.close()

#检查文件合法性并读取数据

def is\_valid\_pe(self)：

#RVA转偏移地址

def rva\_to\_offset(self,rva):

#输入表结构解析

def parse\_import\_table(self):

# 解析每个IID对应的IMAGE\_THUNK\_DATA类型的INT数组

def parse\_iid\_int(self,ptr):

if \_\_name\_\_ == "\_\_main\_\_":

if len(sys.argv) == 2:

p = PeParser(sys.argv[1])

p.parse()

实验代码：

结果截图：