**汇编语言与逆向技术实验报告**

**Lab1-HelloWorld**

**学号：2113662 姓名：张丛 专业：信息安全**

1. **实验内容**
   1. 熟悉Win32汇编MASM32的编译环境；
   2. 命令行输出“HelloWorld”
   3. 窗口输出“HelloWorld”
2. **实验步骤**

1、编辑：用编辑软件（Notepad）形成源程序（改后缀为.asm）,如：hello\_console.asm和hello\_window.asm. （关键代码见下文程序解析）

2、编译：用汇编程序（\masm32\bin\ml.exe）对源程序进行汇编，形成目标文件（.obj），格式如下：

“\masm32\bin\ml /c /Zd /coff hello\_console.asm”

“\masm32\bin\ml /c /Zd /coff hello\_window.asm”

3、连接：用连接程序（\masm32\bin\link.exe）对目标程序进行连接，形成可执行文件（.exe），格式如下：

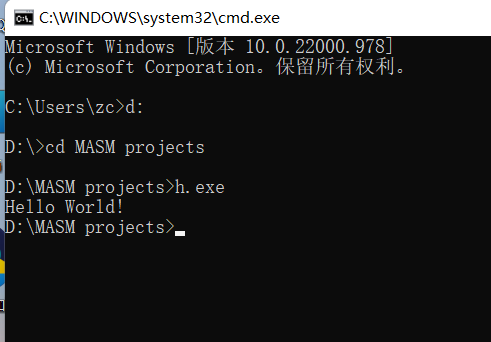
“\masm32\bin\Link /SUBSYSTEM:CONSOLE hello\_console.obj”

“\masm32\bin\Link /SUBSYSTEM:WINDOWS hello\_window.obj”

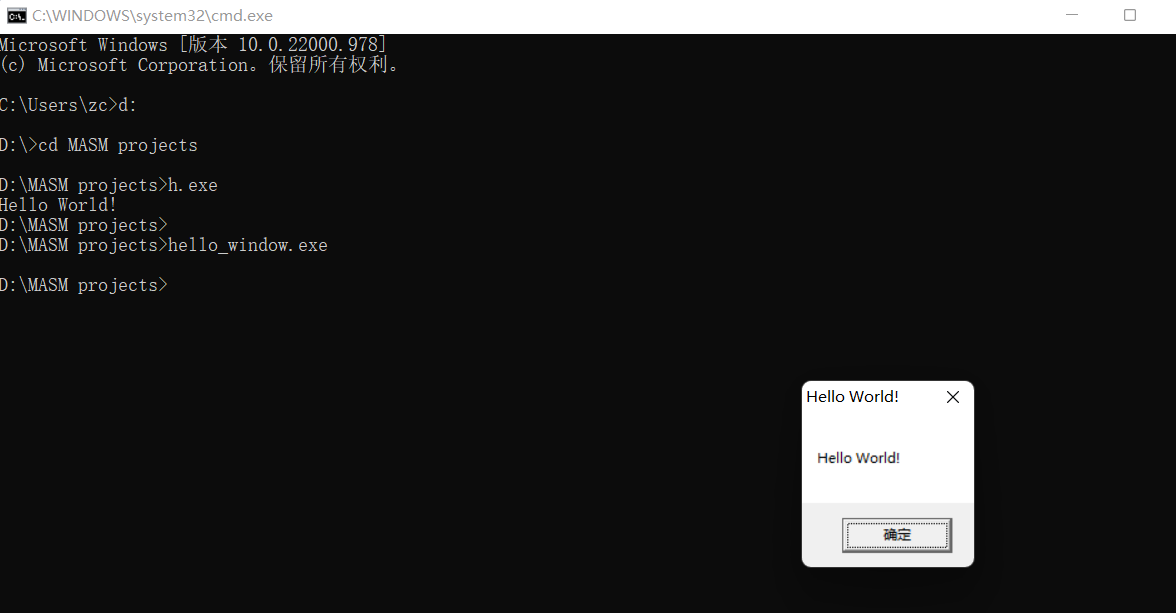
4、执行：如果结果在屏幕在显示，则直接执行可执行文件。

1. **实验截图**

命令行输出：



窗口输出：



1. **汇编命令和参数解析**

“\masm32\bin\ml /c /Zd /coff hello\_console.asm”

Ml程序可以汇编并链接一个或者多个汇编语言源文件

/c 只编译、不链接

/Zd 在目标文件中生成行号信息

/coff 生成Microsoft公共目标文件格式

“\masm32\bin\link /SUBSYSTEM:CONSOLE hello\_console.obj”

lnk.exe链接器，将obj文件合并，生成可执行文件

/SUBSYSTEM,生成命令行程序

1. **汇编程序解析**

汇编程序1: hello\_console.asm

.386

//允许汇编80386处理器的非特权指令，禁用其后处理器引入的汇编指令

.model flat, stdcall

//初始化程序的内存模式：平坦模式、调用约定

option casemap :none

//大小写敏感

include \masm32\include\windows.inc

include \masm32\include\kernel32.inc

include \masm32\include\masm32.inc

//函数的常量和声明

includelib \masm32\lib\kernel32.lib

includelib \masm32\lib\masm32.lib

//链接库

.data

str\_hello BYTE "Hello World!", 0

//定义已初始化数据段的开始

.code

//定义代码段的开始

start:

invoke StdOut, addr str\_hello

//将内存数据输出到命令行窗口

invoke ExitProcess, 0

//退出程序执行

END start

//标记模块的结束，指定程序的入口点

汇编程序2: hello\_window.asm（部分同上）

.386  
.model flat, stdcall

option casemap :none

include \masm32\include\windows.inc

include \masm32\include\kernel32.inc

include \masm32\include\user32.inc

includelib \masm32\lib\kernel32.lib

includelib \masm32\lib\user32.lib

.data  
str\_hello BYTE "Hello World!", 0

.code

start:

invoke MessageBox, NULL, addr str\_hello, addr str\_hello, MB\_OK

//invoke Mess MessgeBox 调用函数名

// NULL 父窗口句柄

// MB\_OK 按钮类型

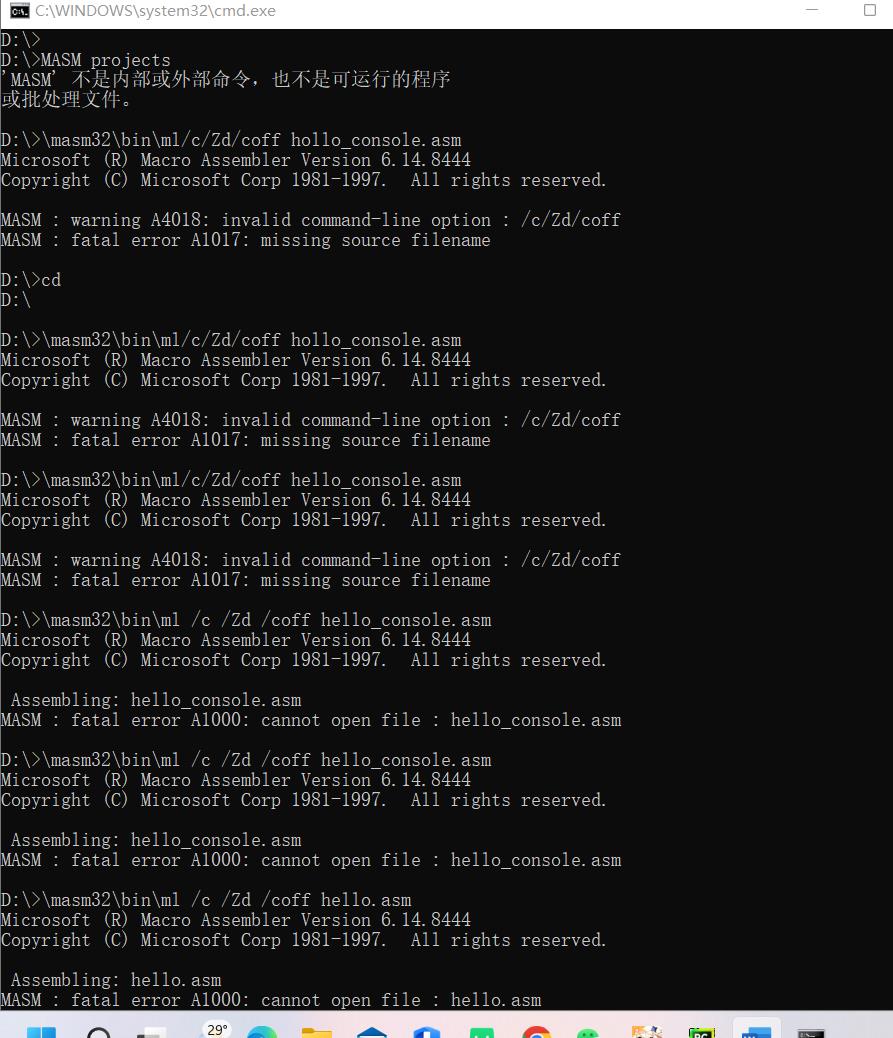
invoke ExitProcess, 0

//退出程序执行

END start

1. **实验心得**

首先，本次实验经历了大量试错，甚至两节实验课错着错着就结束了，在课后也用了许多时间。下图为部分试错截图。

****

总结为以下几点：

* + 1. 没接触过命令行，对很多基本操作不了解，需要去网上学习，并多次实际操作。例如，从C盘根目录转到D盘根目录，以及进一步进入D盘文件等等。
    2. 用记事本形成源文件时出现问题。改文件后缀时，文件扩展名显示不全，即“hello\_window.asm”实际为“hello\_window.asm.txt”。此时仍然需要去网上学习如何更改文件扩展名。
    3. 汇编命令代码之间有空格，如果不是直接复制而是手打的话，需要注意。
    4. 使用命令行编译和连接时，命令行需要从D盘进入到源程序所在文件。即“D:\>\masm32\bin\ml /c /Zd /coff hello\_window.asm”失败，“D:\MASM projects>\masm32\bin\ml /c /Zd /coff hello\_window.asm”成功。
    5. Masm32安装不完全。
    6. 运行“hello\_window.exe”文件时用命令行。
    7. 总之还需多加学习