南開大學

汇编逆向课程实验报告

实验一：Hello World！

学　　院 网络空间安全学院
专　　业 信息安全
学　　号 2311819
姓　　名 王雨萌
班　　级 王志周五上午

一、实验目的

a) 熟悉 Win32 汇编 MASM32 的编译环境；

b) 命令行输出 “HelloWorld”

c) 窗口输出 “HelloWorld”

二、实验原理

a) MASM32

MASM32 是国外的 MASM 爱好者自行整理和编写的一个软件包，最高版本为 11.0 版，MASM32 并不是微软官方发布的软件，微软官方发布的软件 MASM 最新版本也只到 6.15 版，微软发布的 MASM 系列版本从 6.11 版才开始支持 windows 编程，6.11 版以前的版本都不支持 windows 编程，只能用来写 DOS 程序。

MASM32 汇编编译器是 MASM6.0 以上版本中的 ml.exe，资源编译器是 Microsoft Visual Studio 中的 rc.exe，32 位链接器是 Microsoft Visual Studio 中的 Link.exe，同时包含有其他的一些如 lib.exe 和 DumpPe.exe 等工具。

MASM 的 windows 编程的教学书籍有《windows 环境下 32 位汇编语言程序设计第二版》。

三、实验过程

Step 01 安装 MASM32 Editor

Step 02 获取并了解 Hello World 程序源代码含义

```
// 文件 1 hello_console.asm
.386  //指定使用 80386 的处理器指令集
.model flat, stdcall //设置 flat 内存模型和函数调用约定（stdcall）
option casemap :none //指定汇编器在处理标识符时不改变大小写
include \masm32\include\windows.inc
 //引入 Windows API
 //这个文件包含了与 Windows 操作系统相关的数据结构、常量和函数的声明，使得后续代码可以使用这些 API

include \masm32\include\kernel32.inc //提供对 Kernel32.dll 中函数的访问，这些函数包括进程管理、内存管理等
include \masm32\include\masm32.inc  //引入 MASM32 的常用宏和函数
includelib \masm32\lib\kernel32.lib //链接 Kernel32.dll 的库文件
includelib \masm32\lib\masm32.lib  //链接 MASM32 库

-------- Main Body Below ---
.data //开始数据的定义
str_hello BYTE "Hello World!", 0  //定义一个以 0 结尾的字符串

.code  //开始代码段的定义
start:  //定义程序开始地点
invoke StdOut, addr str_hello //调用输出函数将字符串打印在控制台上
invoke ExitProcess, 0 //正常结束程序
END start  //指示汇编程序的结束并指定入口点
```

```
// 文件 2 hello_windows.asm
.386 //指定使用 80386 的处理器指令集
.model flat, stdcall //设置 flat 内存模型和函数调用约定（stdcall）
option casemap :none //指定汇编器在处理标识符时不改变大小写
include \masm32\include\windows.inc //引入 Windows API 的基本定义和结构
```

```
include \masm32\include\kernel32.inc     //引入 Kernel32.dll 的头文件

include \masm32\include\user32.inc     //引入 User32.dll 的头文件

includelib \masm32\lib\kernel32.lib     //链接 Kernel32.dll 的库文件

includelib \masm32\lib\user32.lib     // 链接 User32.dll 的库文件，以便调用该库中的用户界面相关函数



.data    /开始数据的定义
        str_hello BYTE "Hello World!", 0 //定义一个以 0 结尾的字符串

.code /开始代码段的定义

start: //定义程序开始地点
        invoke MessageBox, NULL, addr str_hello, addr str_hello, MB_OK
        //创建空窗口，调用输出函数将字符串输出在窗口上
        invoke ExitProcess, 0 //正常结束程序
END start    //指示汇编程序的结束并指定入口点
```

Step 03 运行汇编命令

我们以 `hello_console.asm` 为例：

我们运行`> \masm32\bin\ml /c /Zd /coff hello_console.asm`

其中，`\masm32\bin\ml` 参数是 masm 程序中的子程序 ml，在该程序中，我们调用程序中的 `/c/Zd/coff` 指令，对于**绝对路径**上的 hello_console.asm 进行编译，编译结束后可以得到下图的反馈

```
C:\Users\wangyumeng>\masm32\bin\ml /c /Zd /coff \\Mac\Home\Desktop\Assembly01\hello_console.asm
Microsoft (R) Macro Assembler Version 6.14.8444
Copyright (C) Microsoft Corp 1981-1997.  All rights reserved.

 Assembling: \\Mac\Home\Desktop\Assembly01\hello_console.asm

***********
ASCII build
***********
```

我们运行`>dir`命令，可以得到.obj 文件保存在**当前工作路径**上：

```
C:\Users\wangyumeng>dir
 驱动器 C 中的卷没有标签。
 卷的序列号是 FC72-C628

 C:\Users\wangyumeng 的目录

2024/09/27  14:33    <DIR>          .
2024/02/09  17:19    <DIR>          ..
2024/08/24  08:37    <DIR>          AxGlyph
2024/02/08  23:11    <DIR>          Contacts
2022/05/07  16:00    <DIR>          Desktop
2024/02/08  23:11    <DIR>          Documents
2022/05/07  16:00    <DIR>          Downloads
2024/02/08  23:11    <DIR>          Favorites
2024/09/27  14:36             2,560 hello_console.exe
2024/09/27  15:16             1,548 hello_console.obj
2024/09/27  14:21             2,560 hello_console.obj.exe
2024/09/27  14:28             2,560 hello_windows.exe
2024/09/27  14:28             1,539 hello_windows.obj.obj
2024/02/08  23:11    <DIR>          Links
2022/05/07  16:00    <DIR>          Music
2022/05/07  16:00    <DIR>          Pictures
2024/02/08  23:11    <DIR>          Saved Games
2024/03/24  21:48    <DIR>          Searches
2024/09/27  14:36             1,423 try.obj
2022/05/07  16:00    <DIR>          Videos
```

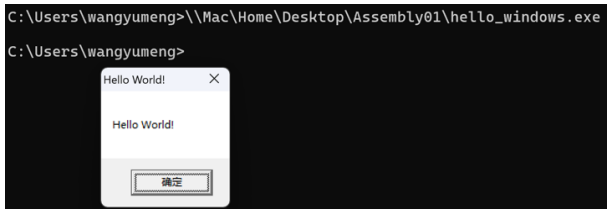
之后我们运行如下链接命令：

我们调用 `\masm32\bin\link` 程序工具，使用程序中的`/SUBSYTEM：CONSOLE` 命令对**绝对路径**上的`.obj 文件`进行链接，生成最后的可执行文件（仍然保存在当前工作路径上）

```
C:\Users\wangyumeng>masm32\bin\link /SUBSYSTEM:CONSOLE hello_console.obj
```

最后的运行结果如下：

```
C:\Users\wangyumeng>hello_console.exe
Hello World!
```



四、实验结论及心得体会

汇编语言博大精深，相对于我们熟知的高级语言，十分难懂，但是兼容性很强。目前比较迷茫如何学好汇编语言。