汇编语言与逆向技术实验报告

Lab1 - HelloWorld

学号：1911590 **姓名：**周安琪 **专业：**计算机科学与技术

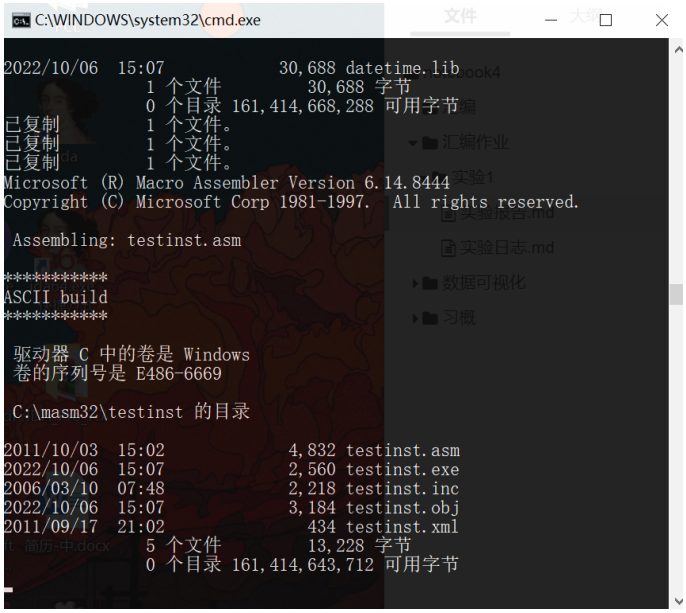
1 实验内容

- 熟悉Win32汇编MASM32的编译环境
- 命令行输出"HelloWorld"
- 窗口输出"HelloWorld"

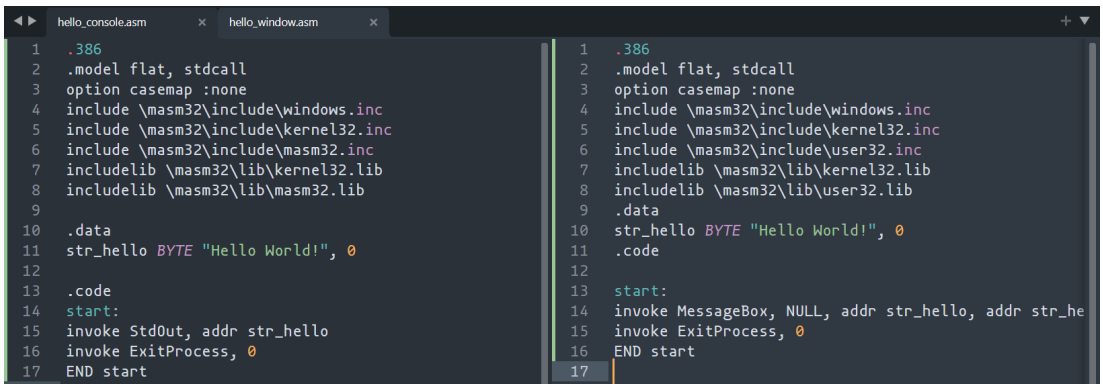
2 实验步骤

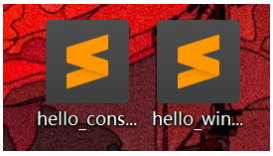
2.1 下载和安装

从MASM32官网下载zip安装包，随后按照指引一步步安装。



2.2 生成.asm源程序





对源程序的解析如下：

2.2.1 hello_console.asm

```
1 .386
```

表示使用的指令集是386的。

```
1 .model flat, stdcall
```

表示程序的内存模式是flat。

stdcall说明了参数的传递约定，包括参数传递时压栈的顺序和由谁恢复栈指针。

```
1 option casemap :none
```

指定标签为大小写敏感

```
1 include \masm32\include\windows.inc
2 include \masm32\include\kernel32.inc
3 include \masm32\include\masm32.inc
4 includelib \masm32\lib\kernel32.lib
5 includelib \masm32\lib\masm32.lib
```

引用一些库函数。

```
1 .data
```

表示数据段（并非真正表意），程序中需要使用的数据保存在这里，该段为可读的。

```
1 str_hello BYTE "Hello World!", 0
```

指定 `str_hello` 的内容是 `"Hello World!"`，0代表字符串的末尾。

```
1 .code
```

表示代码段。

```
1 start:
```

表示代码的开始。

```
invoke StdOut, addr str_hello
```

invoke关键字表示这个函数是从其它库中导入的。它调用输出函数stdOut，传入的参数是str_hello的地址。

```
invoke ExitProcess, 0
```

调用退出程序的函数ExitProcess。

```
END start
```

2.2.2 hello_window.asm

其他都和 `hello_console.asm` 一致。

```
invoke MessageBox, NULL, addr str_hello, addr str_hello, MB_OK
```

调用函数MessageBox，第一个str_hello是作为对话框的标题，第二个str_hello是作为对话框的内容。

2.3 对源程序进行汇编生成.obj文件

```
C:\Users\16834\Desktop>\masm32\bin\ml /c /Zd /coff hello_console.asm
Microsoft (R) Macro Assembler Version 6.14.8444
Copyright (C) Microsoft Corp 1981-1997.  All rights reserved.

 Assembling: hello_console.asm

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


C:\Users\16834\Desktop>\masm32\bin\ml /c /Zd /coff hello_window.asm
Microsoft (R) Macro Assembler Version 6.14.8444
Copyright (C) Microsoft Corp 1981-1997.  All rights reserved.

 Assembling: hello_window.asm

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

下面是对该汇编指令的解析：

```
\masm32\bin\ml /c /Zd /coff hello_console.asm
```

`\masm32\bin\ml` 是汇编器可执行程序的路径地址。

`/c` 指定这一步操作只编译不链接。

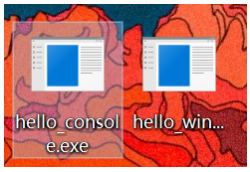
`/coff` 是指定产生的目标文件的格式是coff。

`/Zd` 是给目标文件加上调试信息。

2.4 对目标程序进行链接生成.exe文件

```
C:\Users\16834\Desktop>\masm32\bin\link /SUBSYSTEM:CONSOLE hello_console.obj
Microsoft (R) Incremental Linker Version 5.12.8078
Copyright (C) Microsoft Corp 1992-1998. All rights reserved.


C:\Users\16834\Desktop>\masm32\bin\link /SUBSYSTEM:WINDOWS hello_window.obj
Microsoft (R) Incremental Linker Version 5.12.8078
Copyright (C) Microsoft Corp 1992-1998. All rights reserved.
```




```
1 \masm32\bin\link /SUBSYSTEM:CONSOLE hello_console.obj
```

`/SUBSYSTEM` 是告诉链接器可执行文件的运行平台是，在这两个case中分别是CONSOLE和WINDOWS。

2.5 执行可执行文件

Console Hello World：

```
C:\Users\16834\Desktop>hello_console.exe
Hello World!
C:\Users\16834\Desktop>
```

MessageBox Hello World：

3 实验截图

详情见上文。

4 实验心得

在这次实验中了解了更多汇编语言的细节，也增加了实践经验。