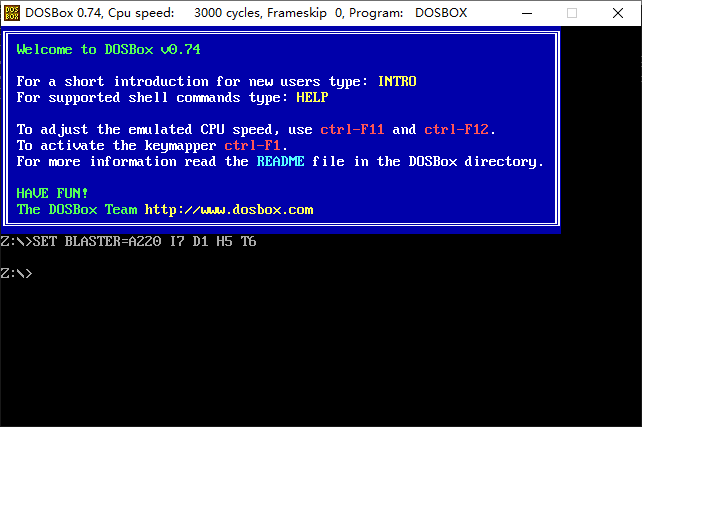
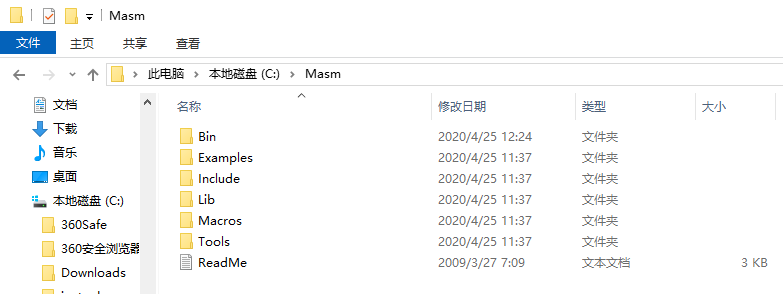
Windows 10下的MASM环境

# 下载并解压“DOSBox 0.74 for Win32”,在Windows桌面生成一个DOSBox快捷方式，也可以将快捷方式加到工具栏上，方便快速启动。



# 下载并解压“MASMForDOSBox202，文件在MASM目录下，将此MASM目录拷贝到C盘根目录下，可能需要Windows管理员权限。,在Windows桌面生成一个DOSBox快捷方式，也可以将快捷方式加到工具栏上，方便快速启动。检查一下C:\MASM\BIN目录下的文件。这是我们将要用到的工作目录，看看里面的应用程序是否齐全。



C:\MASM\BIN目录下的文件：

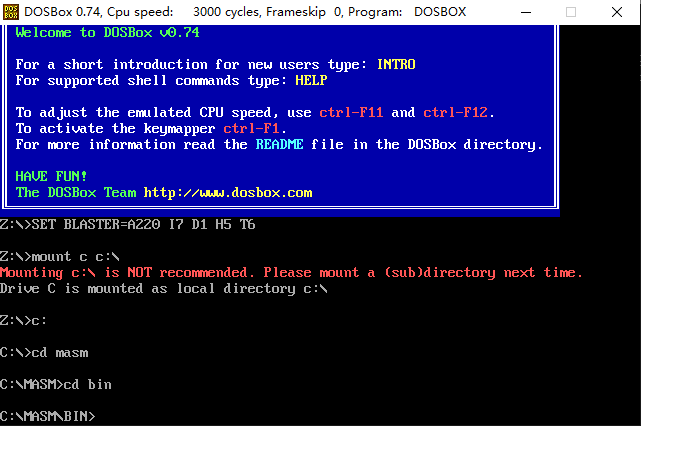


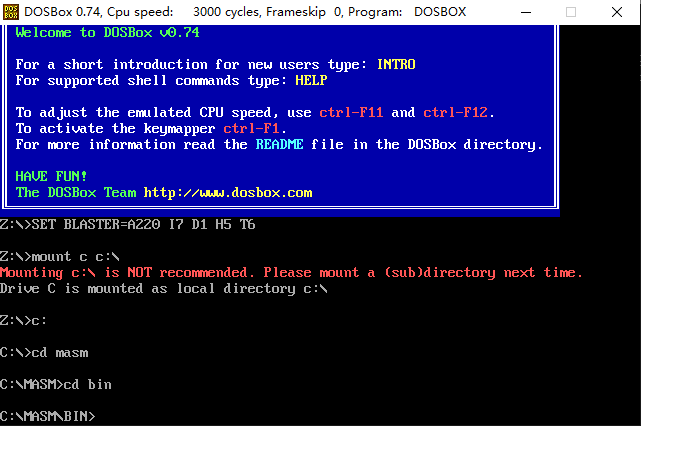
# 运行DOSBox。

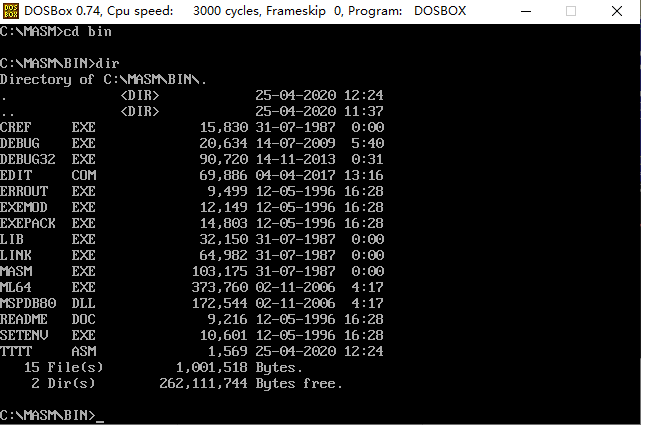
# 在DOSBox窗口里运行： mount c c:\

CD c:\

CD masm

CD BIN



会看到以下内容：

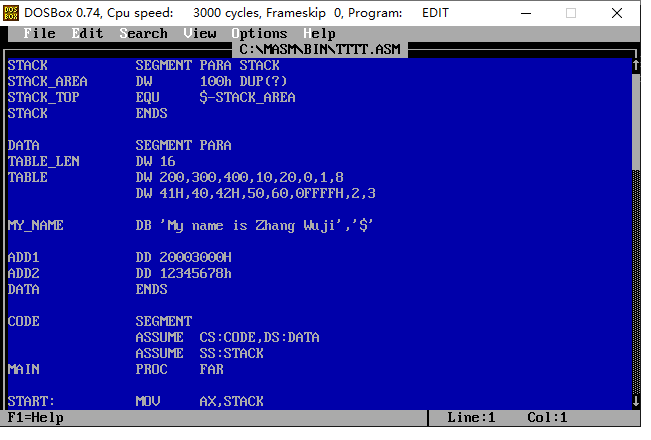
至此，你的MASM实验环境已经建立好。

执行exit，回车。将退出DOSBox，返回Windows桌面。

# 接下来做一个测试，验证该环境能不能工作。 将准备好的例题TTTT.asm，拷贝到C:\MASM\BIN下。

重新执行DOSBox, 并在DOS下执行上述第4步的命令。

然后执行EDIT tttt.asm。将其中的”Zhang Wuji”，改成你的大名。



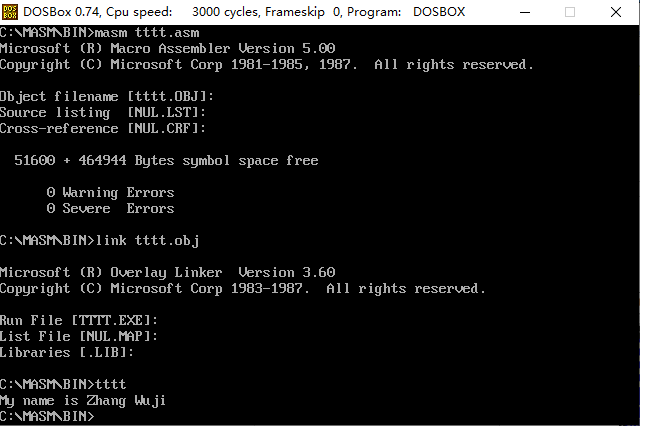
然后执行命令序列：

masm tttt.asm

link tttt.obj

ttttt

看看是否显示你的名字（Hello Word成功）。

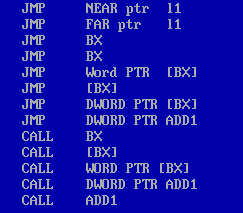


# 以上是预习的基本要求。

# 以下第6,7步是选做的预习题。试一试，费劲或不明白没关系，实验课上会讲解！

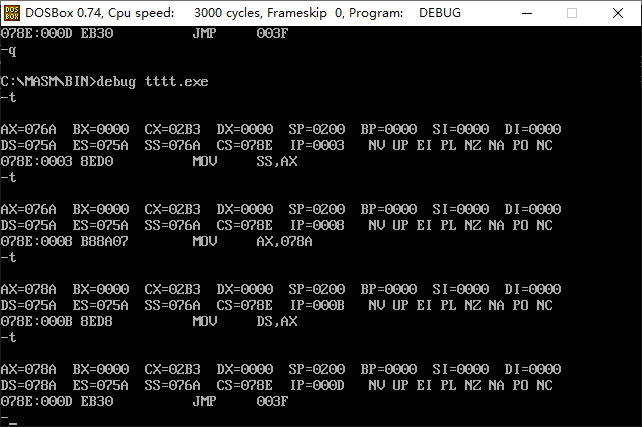
# 接下来，读懂TTTT.asm程序，预习并练习DEBUG 的操作、命令，然后完成以下练习：

# 在DEBUG下，修改IP值，想办法执行这几条指令：

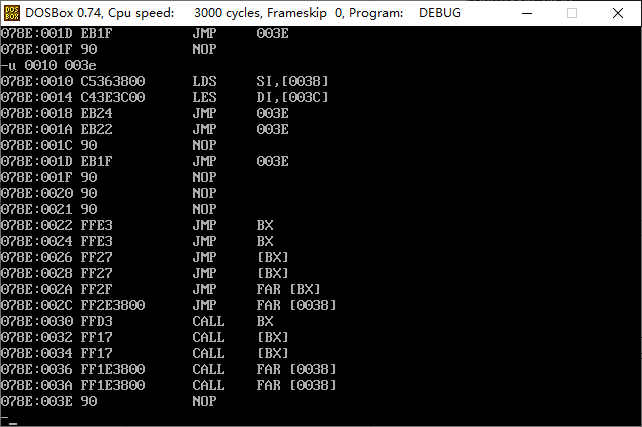


每次都可以修改IP。

每次都修改IP，单步执行一条命令。修改IP，单步执行CALL DWORD PTR ADD1后，内存数据段、堆栈段的内存图。

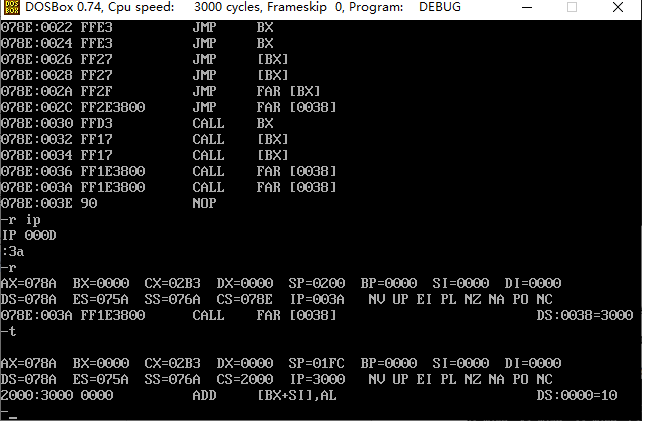


找到那几条转移指令，看看变成什么样了。从078E：000D开始，被填了不少NOP。注意：CALL DWORD PTR ADD1被编译成了(078e:003A那一行)CALL FAR [0038]。



通过R IP  
003A

来执行。



注意执行CALL DWORD PTR ADD1后的寄存器（8个通用寄存器、4个段寄存器）的值。

CS:IP,SP都有变化。此时DS：0，SS：[SP]处的内存，就是我们要的内存图，是什么意思，能说明白吗？数据段里，我们的ADD1,ADD2在哪（DS：0038处）？堆栈段栈顶在哪，里面有什么（SS:01FC处）？

