

汇编快速入门(3)

By: 凌晨五点

第三节：windows下汇编工具— debug.exe的使用

知识点

- ▣ 软件安装配置
- ▣ 使用debug查看CPU、内存

准备

- ▣ 1. DOSBox环境模拟器与debug.exe
- ▣ 2.课程资源
 - 链接: <http://pan.baidu.com/s/1i5NtshR>
密码: slnp

将网盘中的工具目录下载



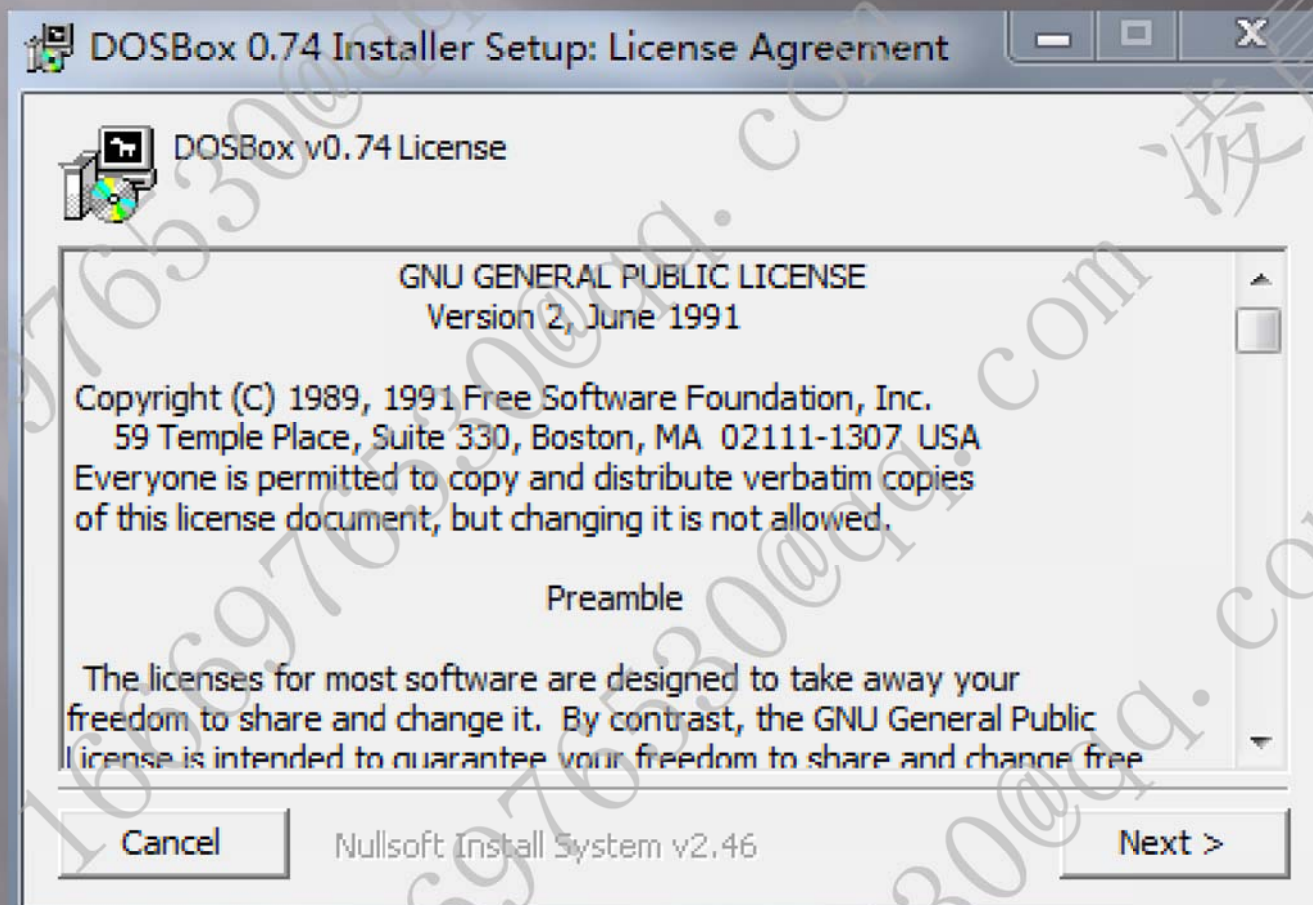
Windows7下使用汇编

- ▣ 安装DOSBox0.74-win32-installer.exe
- ▣ 配置DOSBox操作目录

安装DOSBox0.74-win32- installer.exe

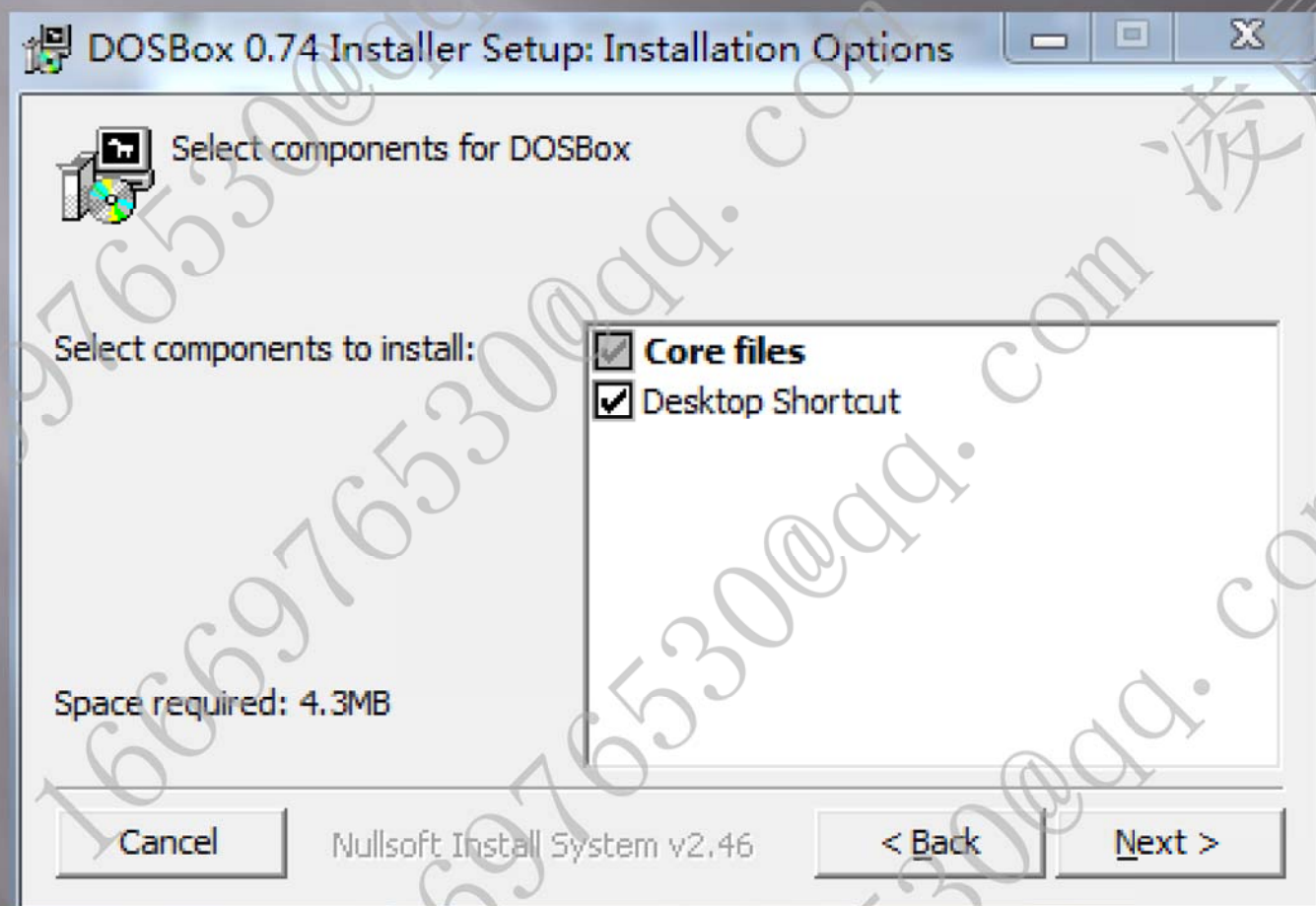
安装：DOSBox0.74-win32（1）

- ▣ 双击安装，并点击next



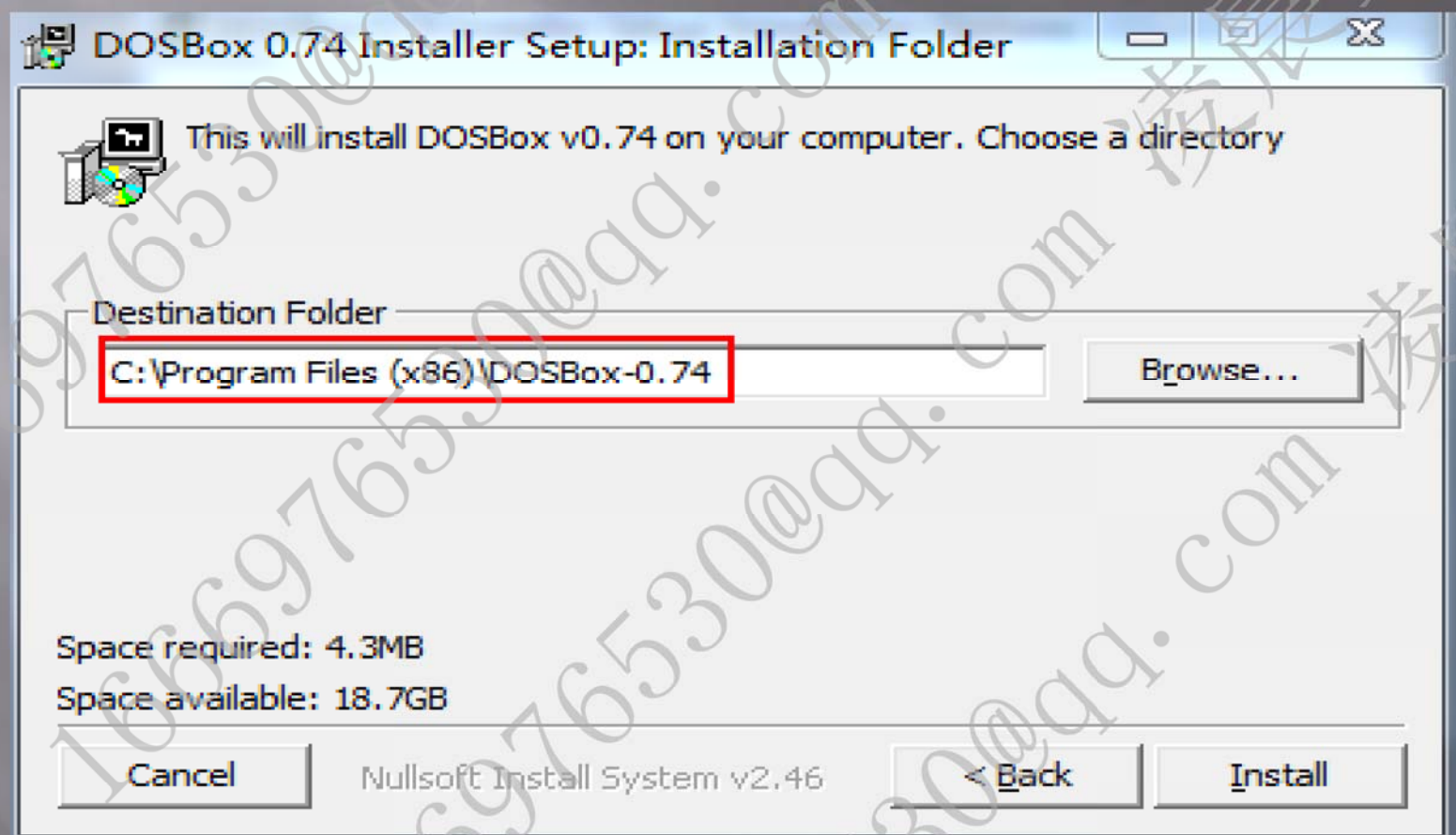
安装：DOSBox0.74-win32（2）

▣ 点击next



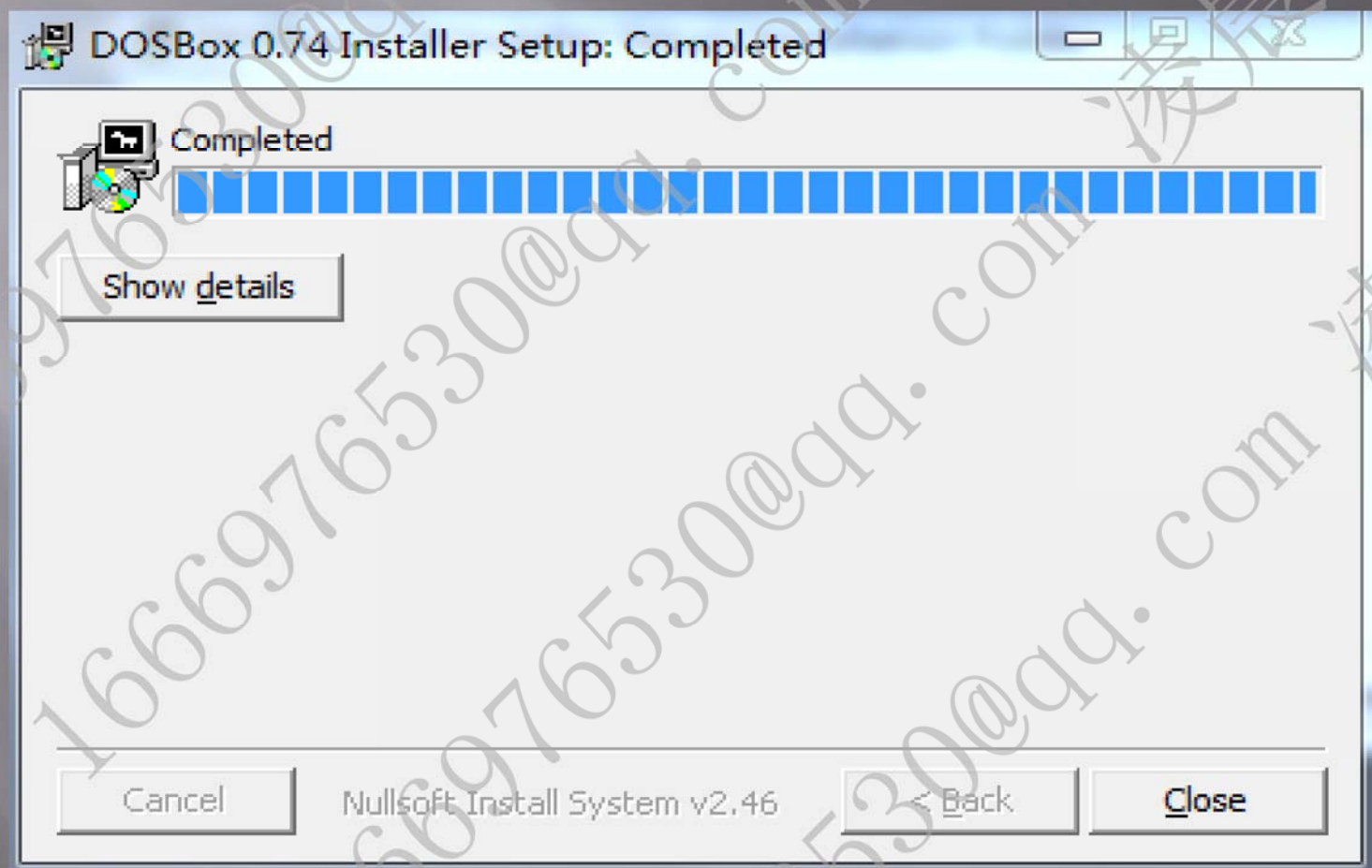
安装：DOSBox0.74-win32（3）

- 可以修改安装路径，点击Install



安装：DOSBox0.74-win32（4）

- ▣ 安装完成，点击Close



配置DOSBox操作目录

配置：DOSBox0.74-win32（1）

- 在安装目录C:\Program Files (x86)\DOSBox-0.74中，打开DOSBox 0.74 Options.bat



配置：DOSBox0.74-win32 (2)

- ▣ 在弹出配置选项文本文件，找到[autoexec]选项
- ▣ 在下面添加如下字段：

```
MOUNT C D:\masmprom  
set PATH=$PATH%;D:\masmprom
```

```
[autoexec]  
# Lines in this section will be run at startup.  
# You can put your MOUNT lines here.  
MOUNT C D:\masmprom  
set PATH=$PATH%;D:\masmprom
```

注：在d盘下创建masmprom目录



配置：DOSBox0.74-win32（3）

- ▣ 如到主载
- ▣ 当入力输
- ▣ 效

```
DOS BOX DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip: 0, Program:
Welcome to DOSBox v0.74
For a short introduction for new users type: INT
For supported shell commands type: HELP
To adjust the emulated CPU speed, use ctrl-F11 a
To activate the keymapper ctrl-F1.
For more information read the README file in the
HAVE FUN!
The DOSBox Team http://www.dosbox.com
Z:\>SET BLASTER=A220 I7 D1 H5 T6
Z:\>MOUNT C D:\masmpo
Drive C is mounted as local directory D:\masmpo\
Z:\>set PATH=%PATH%;D:\masmpo
Z:\>
```

配置：DOSBox0.74-win32（4）

- ▣ 接下来输入C:

```
Z:\>set PATH=%PATH%;D:\masmprom
```

```
Z:\>C:
```

```
C:\>dir
```

```
Directory of C:\
```

```
.<DIR>  
.<DIR>
```

```
0 File(s)
```

```
2 Dir(s)
```

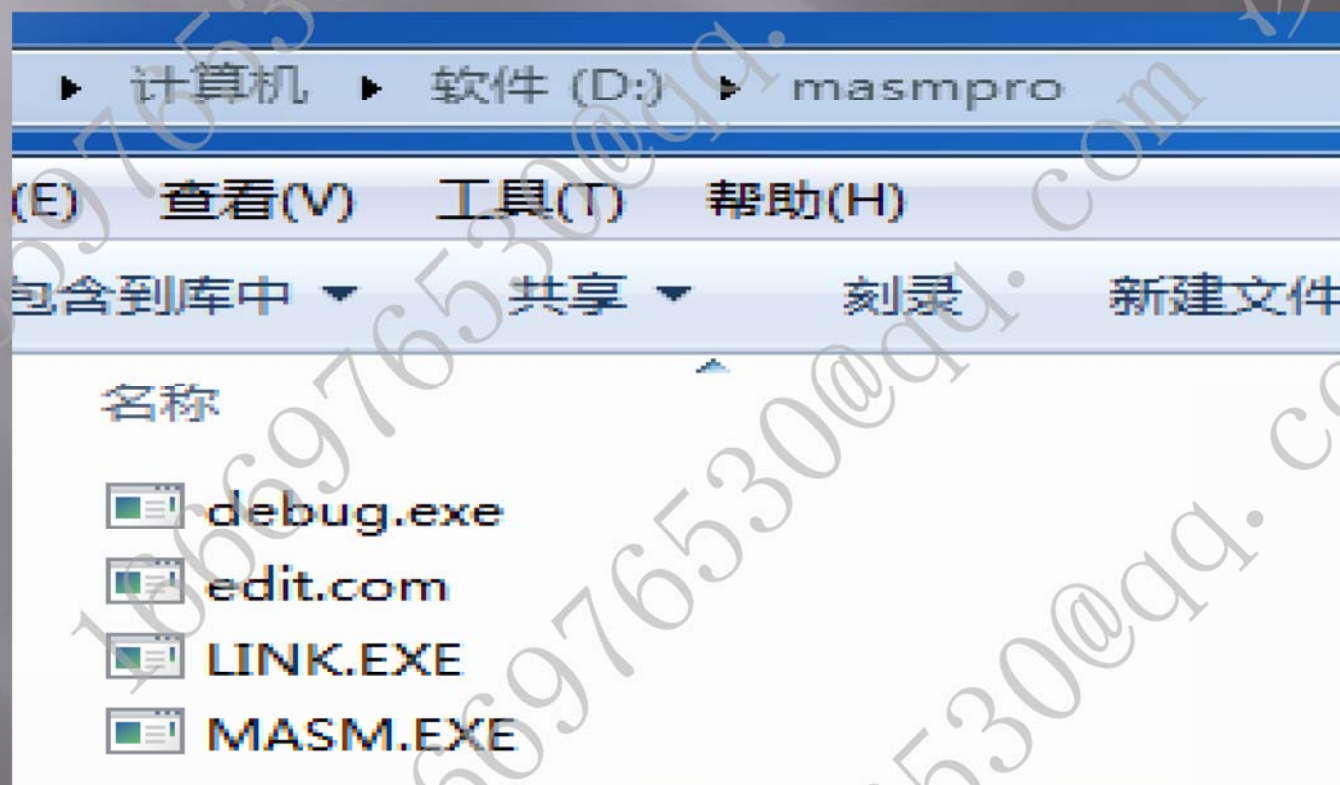
```
262,111,744
```

```
C:\>
```

注：切换到C: 目录下，此时输入dir可以看到D:\masmprom里的文件

配置DOSBox操作目录 (1)

- ▣ 下面配置masmprom
- ▣ 将文件夹“工具a 在DOSBOX 下使用”内的内容拷贝到D:\masmprom里



使用debug查看CPU、内存

debug

- ▣ debug简介:

- ▣ debug是Dos、Windows提供的实模式（8086方式）程序的调试工具。

- ▣ debug功能:

- ▣ 可以查看CPU各种寄存器的内容
- ▣ 可以查看内存的情况
- ▣ 可以在机器码级别跟踪程序的运行

debug

▣ 常用操作:

- ▣ (1) R: 查看更改cpu寄存器内容
- ▣ (2) D: 查看内存中内容
- ▣ (3) E: 改写内存中内容
- ▣ (4) U: 将内存中机器指令翻译成汇编指令
- ▣ (5) T: 执行一条机器指令
- ▣ (6) A: 以汇编格式在内存中写入一条指令

操作：R查看更改cpu寄存器内容

▣ 查看内容：

```
-R
AX=0000 BX=0000 CX=0000 DX=0000 SP=00FD BP=0000 SI=0000 DI=0000
DS=0740 ES=0740 SS=0740 CS=0740 IP=0100  NV UP EI PL NZ NA PO NC
0740:0100 0000          ADD     [BX+SI],AL          DS:0000=CD
```

▣ 注意CS和IP的值，CS=0740，IP=0100。内存0740和0100处的指令为CPU当前要读取、执行的指令。

▣ 指令的内容为：0000

操作：R查看更改cpu寄存器内容

▣ 修改内容：

```
-R
AX=0000 BX=0000 CX=0000 DX=0000 SP=00FD BP=0000 SI=0000 DI=0000
DS=0740 ES=0740 SS=0740 CS=0740 IP=0100  NV UP EI PL NZ NA PO NC
0740:0100 0000          ADD     [BX+SI],AL          DS:0000=CD
```

- ▣ 若修改一个寄存器中的值，比如AX中的值，可用“R AX”然后回车，将出现“:”作为输入提示，在后面输入要写入的数据后回车，即完成了对AX内容的修改。可以通过R键查看

```
-R ax
AX 0000
:1111
-R
AX=1111 BX=0000 CX=0000 DX=0000 SP=00FD
DS=0740 ES=0740 SS=0740 CS=0740 IP=0100
0740:0100 0000          ADD     [BX+SI],AL
```

操作：D：查看内存中内容

- ▣ 查看内容：
- ▣ d 段地址: 偏移地址

```
-d
1000:0080  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
1000:0090  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
1000:00A0  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
1000:00B0  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
1000:00C0  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
1000:00D0  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
1000:00E0  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
1000:00F0  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
-d 3000:10
3000:0010  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
3000:0020  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
3000:0030  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
3000:0040  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
3000:0050  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
3000:0060  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
3000:0070  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
3000:0080  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
```

▣ 参考：王爽老师的《汇编语言 第3版 》第35页

实验 1 查看 CPU 和内存，用机器指令和汇编指令编程

谢谢



看雪公众号: [ikanxue](#)