[64位win7使用debug的方法](http://blog.csdn.net/jiajiayouba/article/details/8537986)

32位的Win7同志就不用看了 直接搜索C盘 debug就找到了 XP也一样  
  
主要说一下64位Win7使用debug程序的方法  
  
1，首先你要下载一个DOSBOX程序 这个程序是一个dos模拟器 这个程序的制作目的是运行经典的DOS游戏 -。-  
下载地址：<http://www.dosbox.com/download.php?main=1> 

安装的过程我就不写了，我想大家都会。

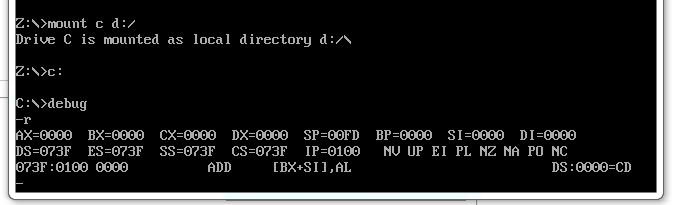
2，其次下载一个Win732位的debug程序

下载地址：<http://u.115.com/file/b3mmegwu>  
参见我的百度云

(以上两个资源，我打了个包，放在csdn上了：http://download.csdn[**.NET**](http://lib.csdn.net/base/dotnet)/detail/jiajiayouba/5025299 )

举例：将debug放到D盘的根目录 双击运行DOSBox 0.74  
在这个窗口输入：  
mount c d:/  
c:  
debug  
好啦 教程结束 Win7 64位运行debug调试程序

写几个命令试试



大家尽情享受汇编的乐趣吧。

DEBUG介绍：

DOS系统中的调试程序，程序名称就叫DEBUG。DEBUG在windows系统中也是极其重要的编译操作。

DOS中的Debug是为DOS提供的有力的侦错，跟踪程序运行，检查系统数据的工具程序，它是在字符界面下以单字符命令方式工作。要很好地使用它必须具备一定的汇编程序设计和硬件基本知识的能力，当然，它为[汇编语言](http://baike.baidu.com/view/49.htm)程序员提供了有效的调试手段，它的功能包括以下几个方面。

1. 直接输入、更改、跟踪、运行汇编程序；

2. 观察操作系统的内容；

3. 查看ROM BIOS的内容；

4. 观察更改RAM内部的设置值；

5. 以[扇区](http://baike.baidu.com/view/201129.htm)或文件的方式读写[软盘](http://baike.baidu.com/view/52940.htm)数据。

在DEBUG中地址用[段地址](http://baike.baidu.com/view/883213.htm)与段内地址来表示，而段地址可以明确地指出来，也可以用一个段指示器(段[寄存器](http://baike.baidu.com/view/6159.htm))来代表，用段寄存器表示时，其段地址就是此寄存器的内含值：

如：用段地址和段内地址表示FOFF：0100

用[段寄存器](http://baike.baidu.com/view/364403.htm)和段内地址表示CSF：0100←CS指向F000

下面列出了常用命令用法。

-A 地址 从指定地址开始编写小[汇编程序](http://baike.baidu.com/view/14850.htm)，按两个[回车键](http://baike.baidu.com/view/29849.htm)结束编辑

-U 地址 从指定地址开始[反汇编](http://baike.baidu.com/view/637356.htm)32字节的[机器指令](http://baike.baidu.com/view/2062994.htm)，缺省地址则从上一U命令继续

-D 始址 终址 以16进制/Asc[字符](http://baike.baidu.com/view/263416.htm)对照方式显示指定内存范围的数据，每行显示10H个[字节](http://baike.baidu.com/view/60408.htm)

-E 地址 值表 用给出的值表(空格分隔)替换指定地址开始的[内存单元](http://baike.baidu.com/view/5349463.htm)，例：-E 100 'v' 1F 'hello'

-N 文件名 为后续的L/W命令约定所操作的文件名

-L 地址 将N命令所指定文件的内容读入到指定内存位置。另，逻辑卷[扇区](http://baike.baidu.com/view/201129.htm)直接读：-L 地址 逻卷号 起始逻扇号 扇数

-W 地址 将BX-CX个字节的内存数据写入N命令指定的文件中。另，逻辑卷扇区直接写：-W 地址 逻卷号 起始逻扇号 扇数

-R[寄存器](http://baike.baidu.com/view/6159.htm)名 显示并允许修改指定寄存器的值

-G=始址 终址 执行指定内存中的机器指令程序

-T=地址 单步执行机器指令，缺省地址则从上一T命令继续。另，继续跟踪m条指令：-T m

例如：读取c:卷的[引导扇区](http://baike.baidu.com/view/409354.htm)，并保存到Boot.1文件中，并简单分析引导程序的前面几条指令：

-L 1000 2 0 1

-N boot.1

-R bx ;输入0000

-R cx ;输入0200

-W 1000

-U 1000

例如：读取第一个硬盘上的[主引导扇区](http://baike.baidu.com/view/418400.htm)，并保存到MB.1文件中，在屏幕上显示[硬盘分区表](http://baike.baidu.com/view/1385.htm)数据：

-A 100

yyyy:0100 mov dx，0080

yyyy:01xx mov cx，0001

yyyy:01xx mov ax，yyyy

yyyy:01xx mov es，ax

yyyy:01xx mov bx，1000

yyyy:01xx mov ax，0201

yyyy:01xx int 13

yyyy:01zz nop

-G=yyyy:0100 01zz

-N mb.1

-R bx ;输入0000

-R cx ;输入0200

-W 1000

-D 11be 11ff

以下是 Debug 子命令列表，

? 显示 Debug 详细命令列表。

Debug:A（汇编）—汇编 8086/8087/8088 记忆码

Debug:C（比较）—比较内存的两个部分

Debug：D（转储）—显示部分内存的内容

Debug:E（键入） —从指定地址开始，将数据输入到内存

Debug:F（填充）—使用指定值填充一段内存

Debug:G（转向）—运行在内存中的[可执行文件](http://baike.baidu.com/view/159830.htm)

Debug:H（十六进制）—执行十六进制运算

Debug:I（输入）—显示来自特定端口的 1 字节值

Debug:L（加载）—将文件或磁盘扇区内容加载到内存

Debug:M（移动）—复制内存块中的内容

Debug:N（名称）—为 l 或 w 命令指定文件，或者指定正在测试的文件的参数

Debug:O（输出）—向输出端口发送 1 个字节的值

Debug:P（执行）—执行循环、重复的字符串指令、软件中断或[子例程](http://baike.baidu.com/view/1191947.htm)

Debug:Q（退出）—停止 Debug 会话

Debug:r（[寄存器](http://baike.baidu.com/view/6159.htm)）—显示或改变一个或多个[寄存器](http://baike.baidu.com/view/6159.htm)

Debug:s（搜索）—在部分内存中搜索一个或多个字节值的模式

Debug:T（跟踪）—执行一条指令，然后显示所有寄存器的内容、所有标志的状态和 Debug 下一步要

执行的指令的解码形式

Debug:U（[反汇编](http://baike.baidu.com/view/637356.htm)）—[反汇编](http://baike.baidu.com/view/637356.htm)字节并显示相应的原语句

Debug:W（写入）—将被测试文件写入磁盘

Debug:XA（分配[扩展内存](http://baike.baidu.com/view/404404.htm)）

Debug:XD（取消分配扩展内存）

Debug:XM（映射扩展内存页）

Debug:XS（显示扩展内存状态）

**分隔命令参数：**

所有 Debug 命令都接受参数，除了 q 命令之外。可以用逗号或空格分隔参数，但是只有在两个十六进制值之间才需要这些[分隔符](http://baike.baidu.com/view/1268377.htm)。因此，以下命令等价：

dcs:100 110

d cs:100 110

d，cs:100，110

**指定有效地址项：**

Debug 命令中的 address 参数指定内存位置。Address 是一个包含字母段记录的二位名称或一个四位字段地址加上一个[偏移量](http://baike.baidu.com/view/1254177.htm)。可以忽略[段寄存器](http://baike.baidu.com/view/364403.htm)或[段地址](http://baike.baidu.com/view/883213.htm)。a，g，l，t，u 和 w 命令的默认段是 CS。所有其他命令的默认段是 DS。所有数值均为十六进制格式。

[有效地址](http://baike.baidu.com/view/1334477.htm)如下：

CS:0100

04BA:0100

在段名和偏移量之间要有冒号。

**指定有效范围项：**

Debug 命令中的 range 参数指定了内存的范围。可以为 range 选择两种格式：起始地址和结束地址，或者起始地址和长度范围（由 l 表示）。

例如，下面的两个语法都可以指定从 CS:100 开始的 16 字节范围：

cs:100 10f

cs:100 l 10

**更多内容可以以后学习**