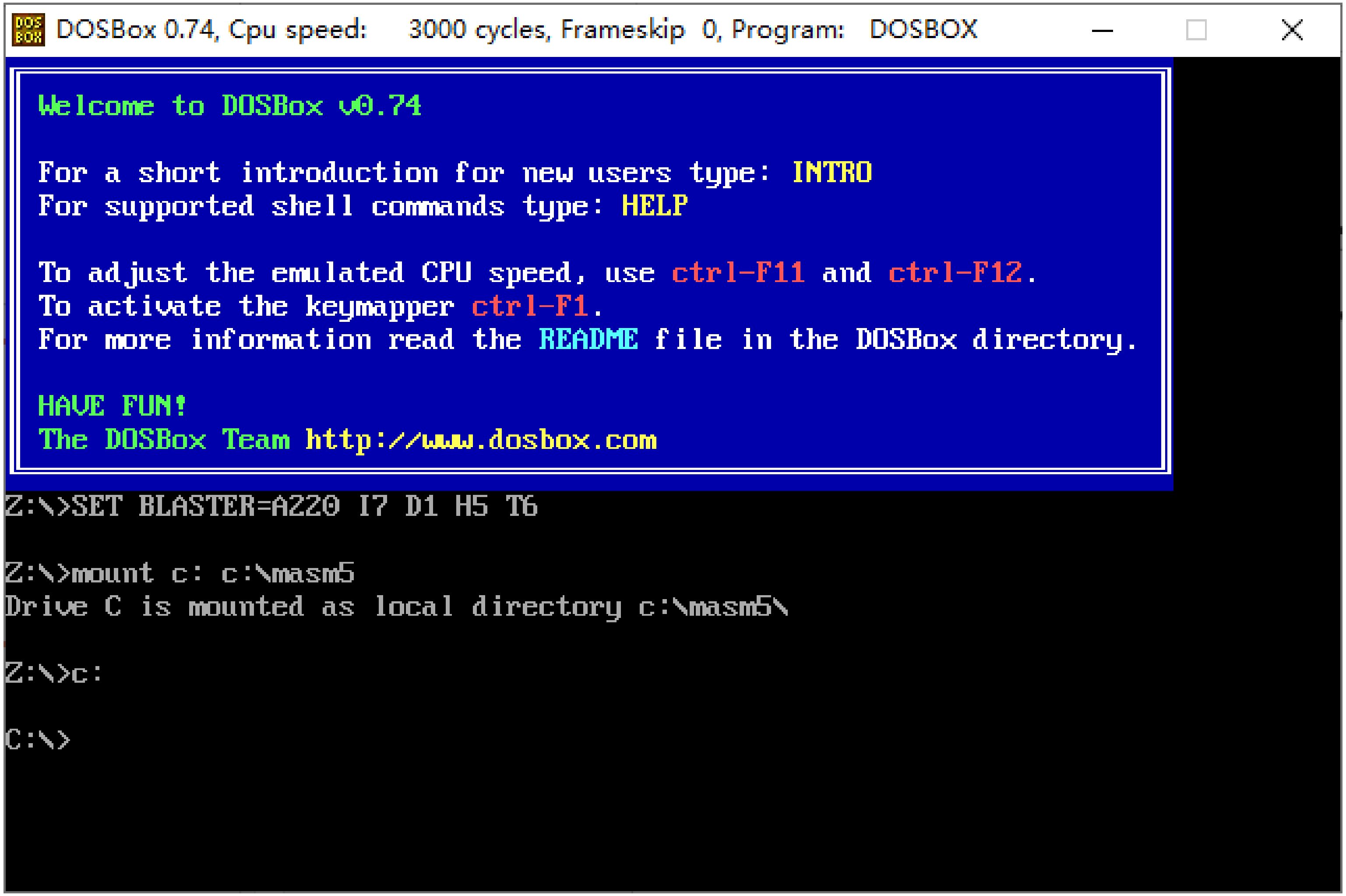
编写和调试汇编程序

DOSBox的使用方法

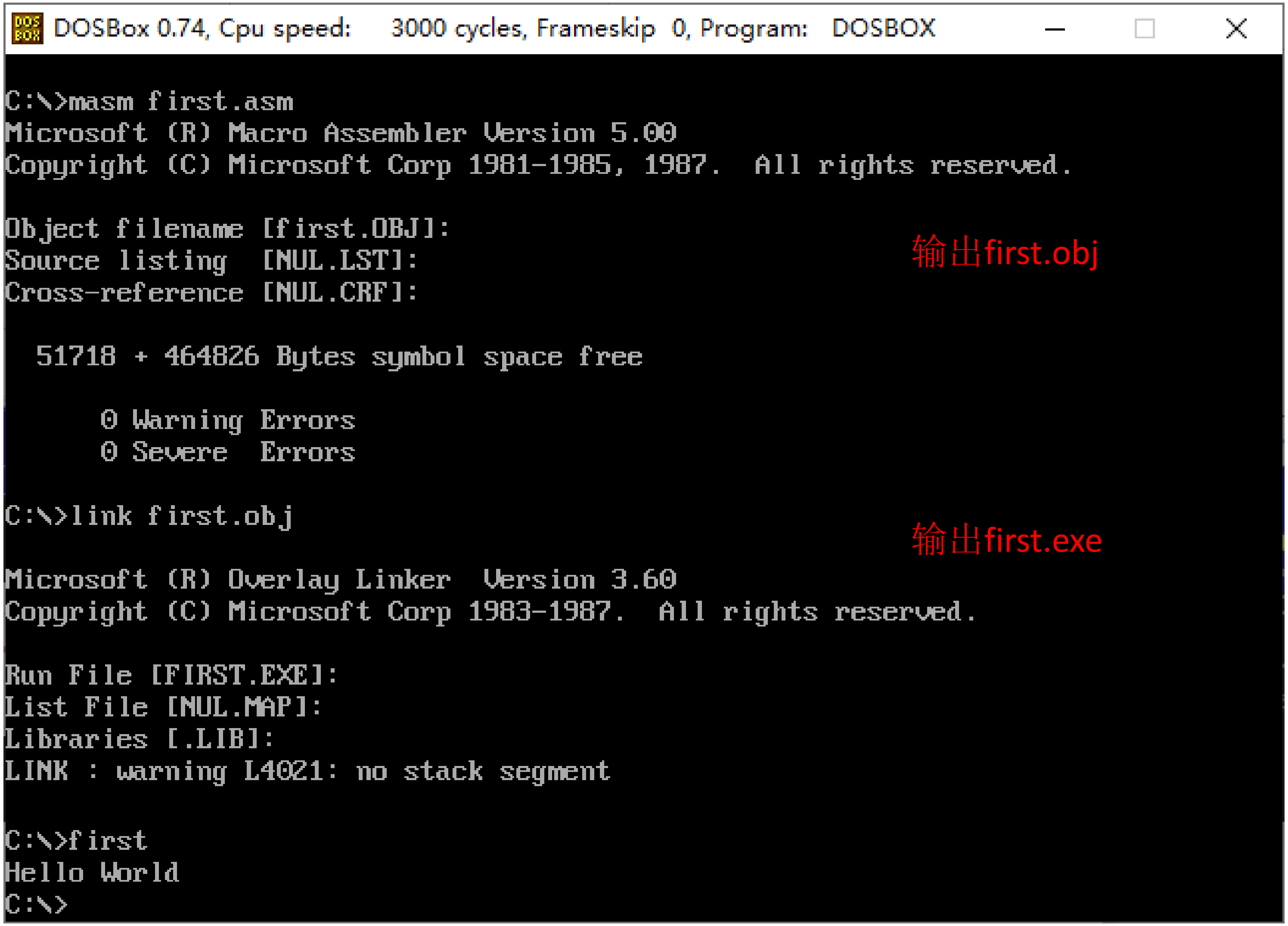

DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX

```
Welcome to DOSBox v0.74

For a short introduction for new users type: INTRO
For supported shell commands type: HELP

To adjust the emulated CPU speed, use ctrl-F11 and ctrl-F12.
To activate the keymapper ctrl-F1.
For more information read the README file in the DOSBox directory.

HAVE FUN!
The DOSBox Team http://www.dosbox.com
Z:\>SET BLASTER=A220 I7 D1 H5 T6

Z:\>mount c: c:\masm5
Drive C is mounted as local directory c:\masm5\

Z:\>c:

C:\>
```

显示字符串程序

```
;first.asm
data segment
   s1 db 'Hello World','$'
data ends

code segment
     assume cs:code, ds:data
start:
    mov ax,data
    mov ds, ax
    mov ah,09h           ; 功能：显示字符串
    mov dx,offset s1     ; ds:dx指向字符串的起始地址
    int 21h              ; DOS功能调用

   mov ah,4ch            ; 功能：结束程序，返回DOS系统
    int 21h              ; DOS功能调用
code  ends
   end start
```

MASM和DEBUG参考


DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX

```
C:\>masm first.asm
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987.  All rights reserved.

Object filename [first.OBJ]:
Source listing  [NUL.LST]:
Cross-reference [NUL.CRF]:

  51718 + 464826 Bytes symbol space free

      0 Warning Errors
      0 Severe  Errors

C:\>link first.obj

Microsoft (R) Overlay Linker  Version 3.60
Copyright (C) Microsoft Corp 1983-1987.  All rights reserved.

Run File [FIRST.EXE]:
List File [NUL.MAP]:
Libraries [.LIB]:
LINK : warning L4021: no stack segment

C:\>first
Hello World
C:\>
```

汇编

输出first.obj

链接

输出first.exe

运行

DOS功能调用

DOS功能调用

AH	功能	调用参数	返回参数
00	程序终止(同INT 20H)	CS=程序段前缀	
01	键盘输入并回显		AL=输入字符
02	显示输出	DL=输出字符	

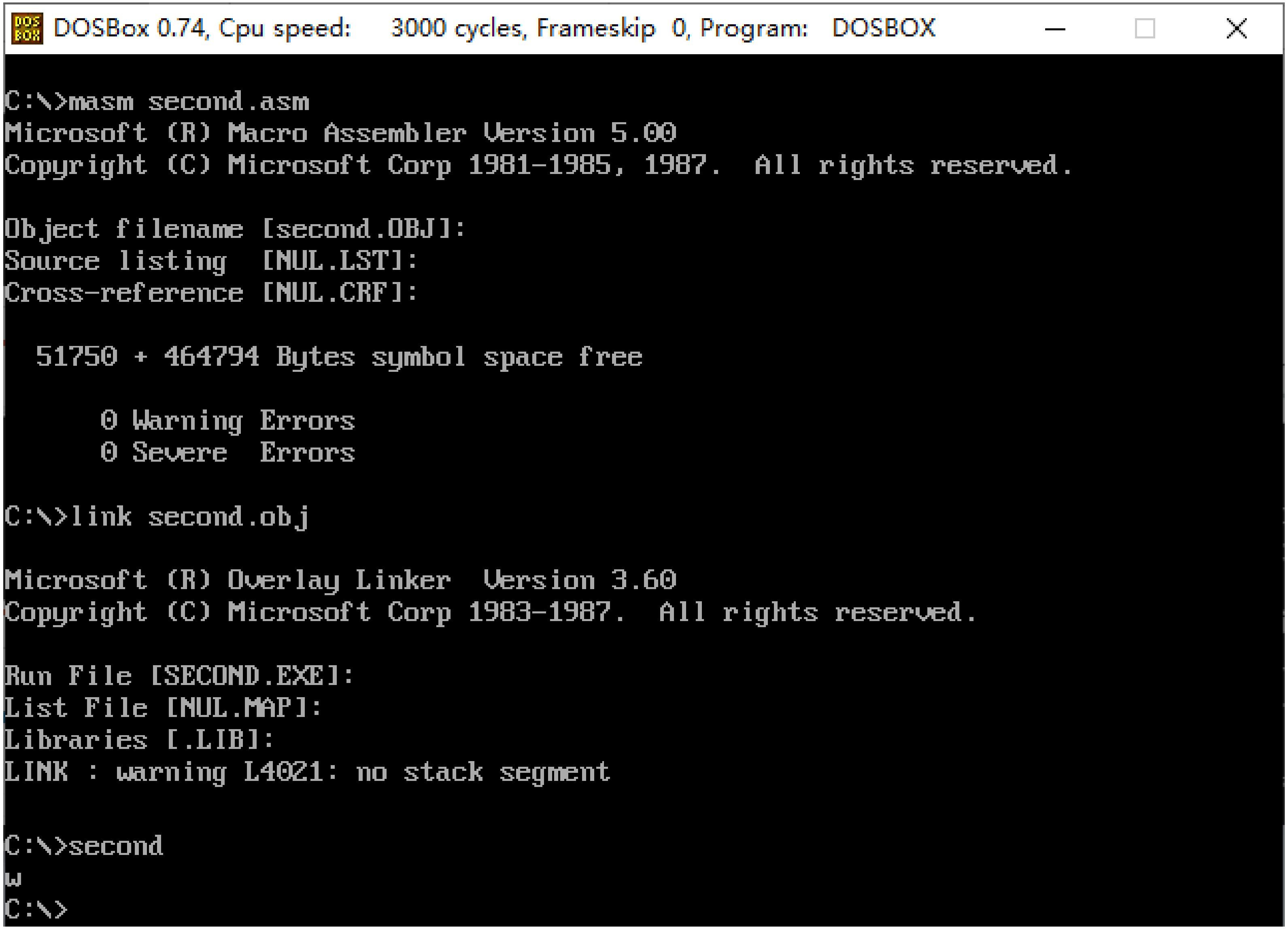
06	直接控制台I/O	DL=FF(输入)
		DL=字符(输出)
			AL=输入字符

07	键盘输入(无回显)		AL=输入字符
08	键盘输入(无回显) 检测Ctrl-Break		AL=输入字符
09	显示字符串	DS:DX=串地址 '$'结束字符串	
0A	键盘输入到缓冲区	DS:DX=缓冲区首地址 (DS:DX)=缓冲区最大字符数	(DS:DX+1)=实际输入的字符数

0B	检验键盘状态		AL=00 有输入
			AL=FF 无输入

键盘输入程序

```
;second.asm
code segment
     assume cs:code

start:
      mov ah,07h        ; 功能：键盘输入
      int 21h           ; DOS功能调用

      mov dl, al
      mov ah,02h        ; 功能：显示输出
      int 21h           ; DOS功能调用

      mov ah,4ch        ; 功能：返回DOS系统
      int 21h           ; DOS功能调用
code  ends
     end start
```

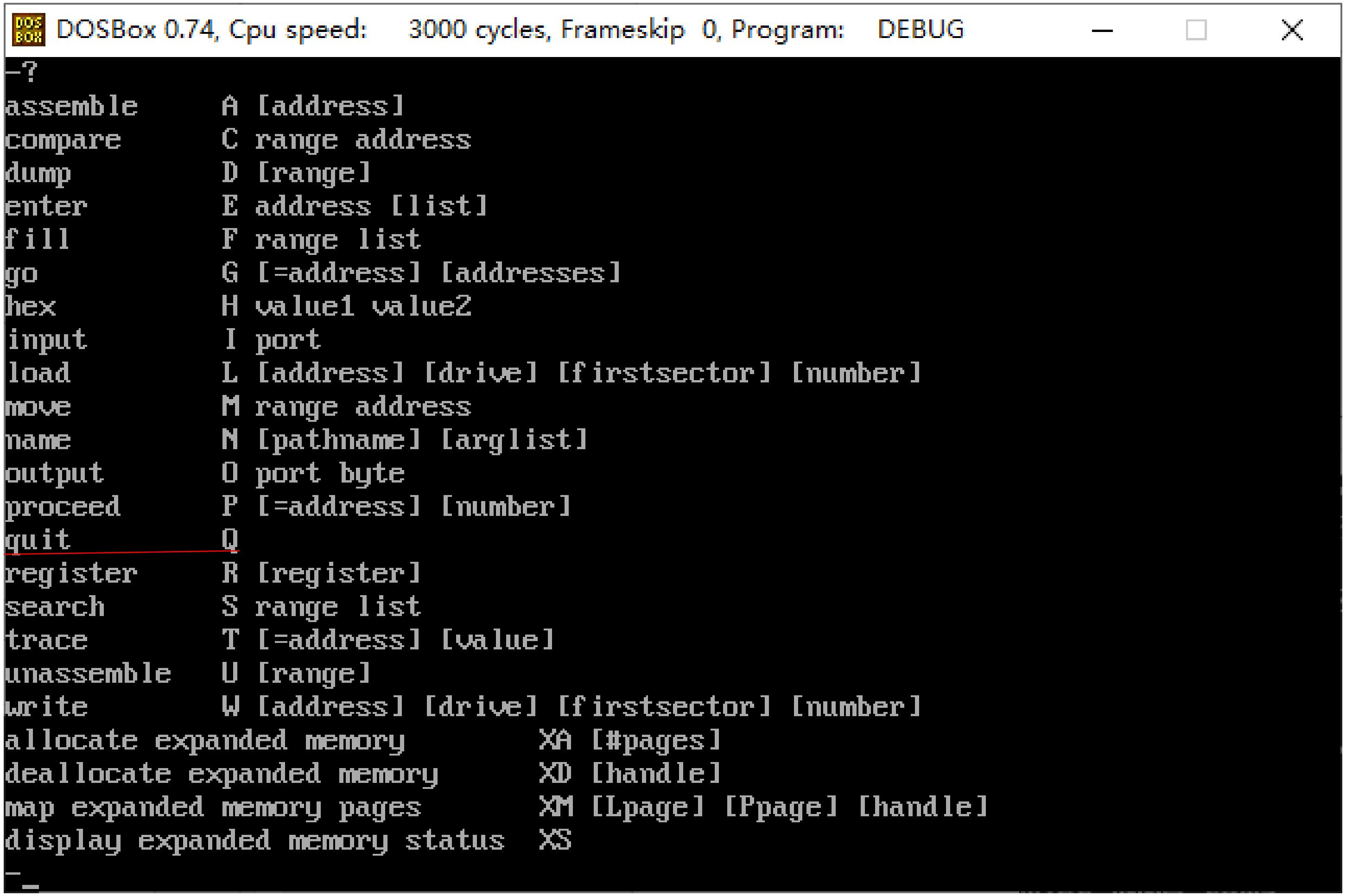


DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX

```
C:\>masm second.asm
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987.  All rights reserved.

Object filename [second.OBJ]:
Source listing  [NUL.LST]:
Cross-reference [NUL.CRF]:

  51750 + 464794 Bytes symbol space free

      0 Warning Errors
      0 Severe  Errors

C:\>link second.obj

Microsoft (R) Overlay Linker  Version 3.60
Copyright (C) Microsoft Corp 1983-1987.  All rights reserved.

Run File [SECOND.EXE]:
List File [NUL.MAP]:
Libraries [.LIB]:
LINK : warning L4021: no stack segment

C:\>second
w
C:\>
```

debug

（1）命令


DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG

```
-?
assemble      A [address]
compare       C range address
dump          D [range]
enter         E address [list]
fill          F range list
go            G [=address] [addresses]
hex           H value1 value2
input         I port
load          L [address] [drive] [firstsector] [number]
move          M range address
name          N [pathname] [arglist]
output        O port byte
proceed       P [=address] [number]
quit          Q
register      R [register]
search        S range list
trace         T [=address] [value]
unassemble    U [range]
write         W [address] [drive] [firstsector] [number]
allocate expanded memory        XA [#pages]
deallocate expanded memory      XD [handle]
map expanded memory pages       XM [Lpage] [Ppage] [handle]
display expanded memory status  XS
-_
```

A （Assemble）逐行汇编 a [address]

C （Compare）比较两内存块 c range address

D （Dump）内存16进制显示 d [address]或 d [range]

E （Enter）修改内存字节 e address [list]

F （fin）预置一段内存 f range list

G （Go）执行程序 g [=address][address...]

H （Hexavithmetic）制算术运算 h value value

I （Input）从指定端口地址输入 i pataddress

L （Load）读盘 l [address [driver sector]

M （Move）内存块传送 m range address

N （Name）置文件名 n filespec [filespec...]

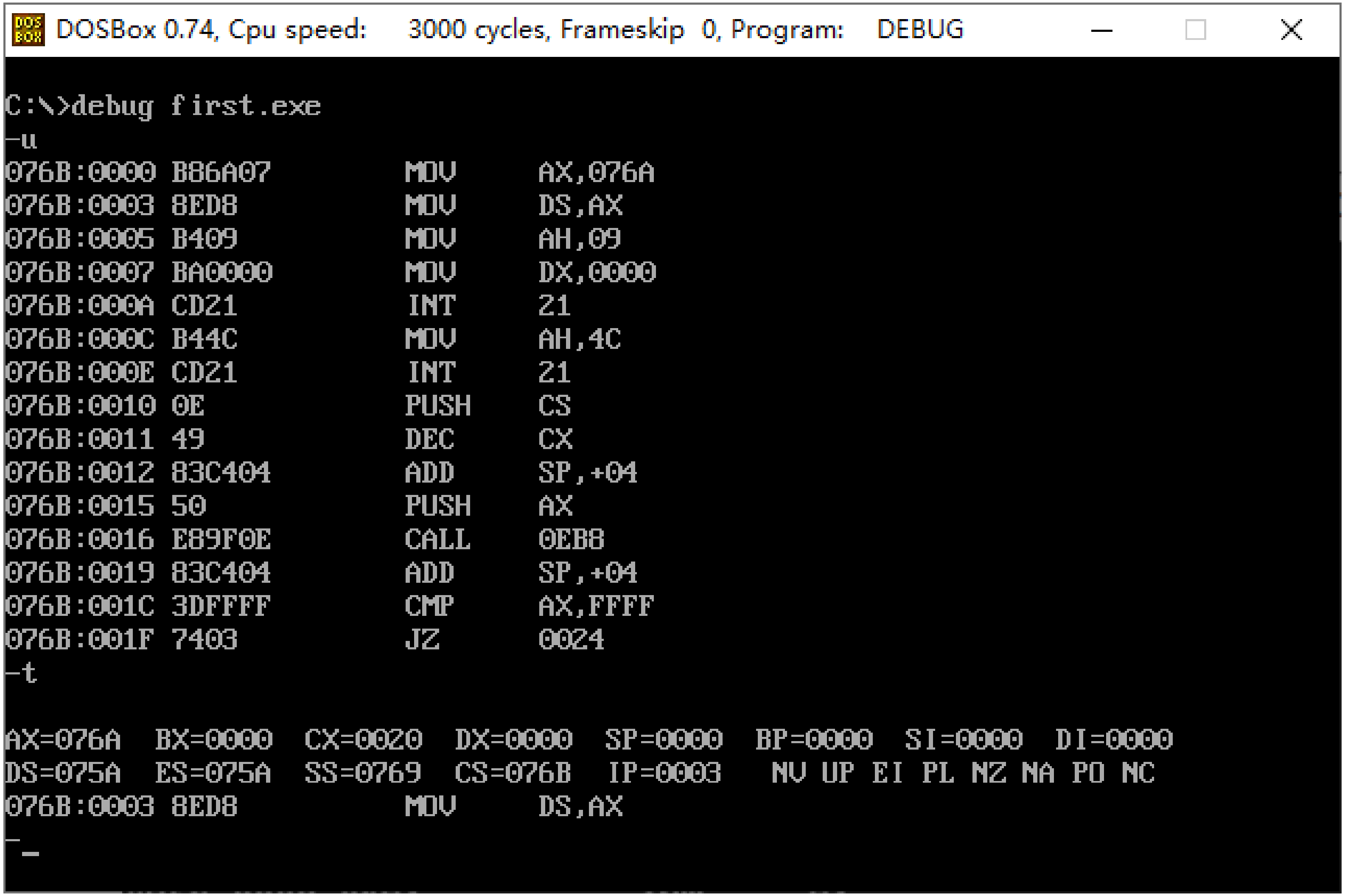
O （Output）从指定端口地址输出 o portadress byte

Q （Quit）结束 q

R （Register）显示和修改寄存器 r [register name]

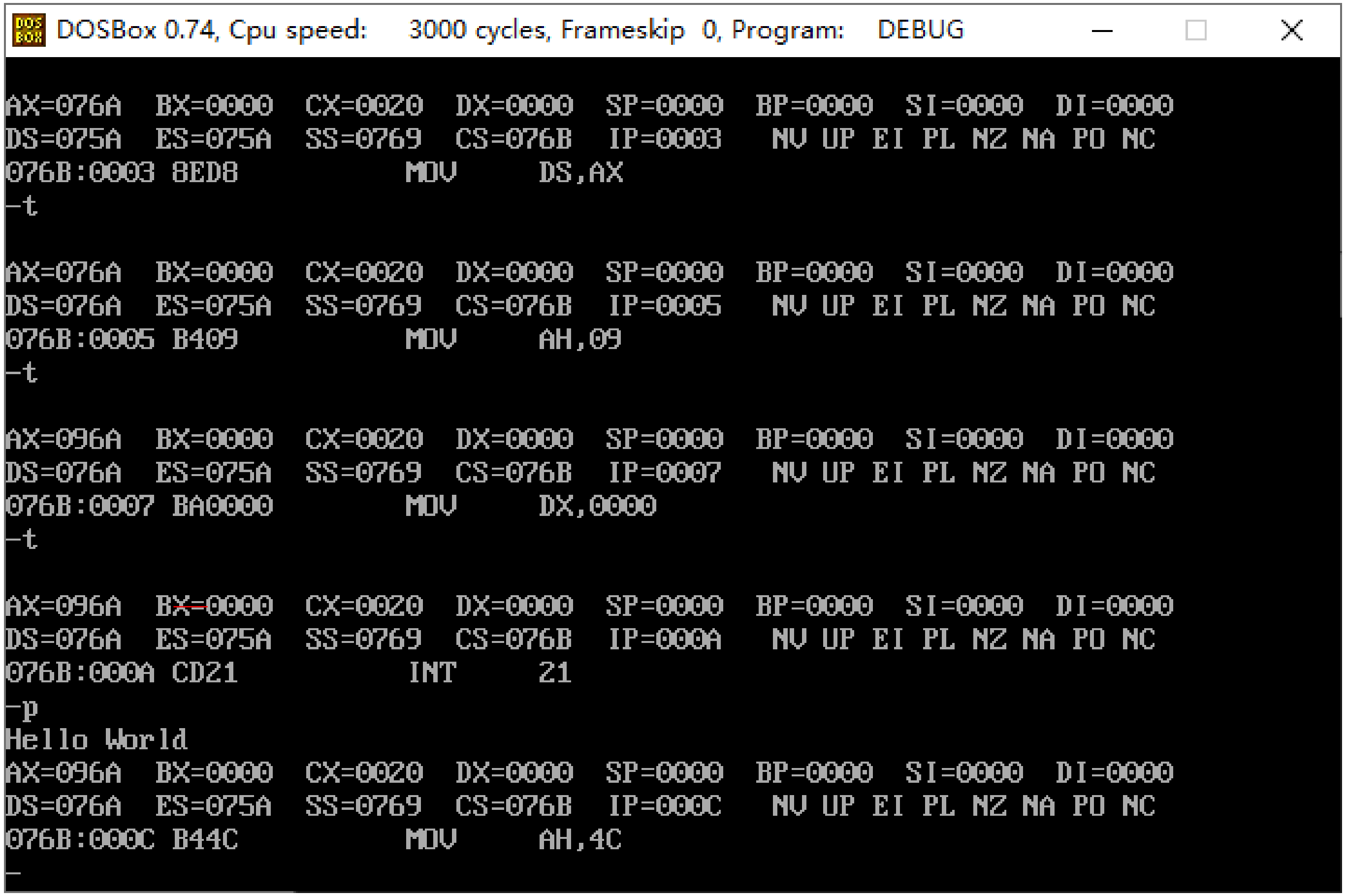
S （Search）查找字节串 s range list

（2）U 反汇编 T 单步执行(逐语句) P(逐过程)


DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG

```
C:\>debug first.exe
-u
076B:0000 B86A07        MOV     AX,076A
076B:0003 8ED8          MOV     DS,AX
076B:0005 B409          MOV     AH,09
076B:0007 BA0000        MOV     DX,0000
076B:000A CD21          INT     21
076B:000C B44C          MOV     AH,4C
076B:000E CD21          INT     21
076B:0010 0E            PUSH    CS
076B:0011 49            DEC     CX
076B:0012 83C404        ADD     SP,+04
076B:0015 50            PUSH    AX
076B:0016 E89F0E        CALL    0EB8
076B:0019 83C404        ADD     SP,+04
076B:001C 3DFFFF        CMP     AX,FFFF
076B:001F 7403          JZ      0024
-t

AX=076A  BX=0000  CX=0020  DX=0000  SP=0000  BP=0000  SI=0000  DI=0000
DS=075A  ES=075A  SS=0769  CS=076B  IP=0003   NV UP EI PL NZ NA PO NC
076B:0003 8ED8          MOV     DS,AX
-_
```

T 单步执行(逐语句) P(逐过程)


DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG

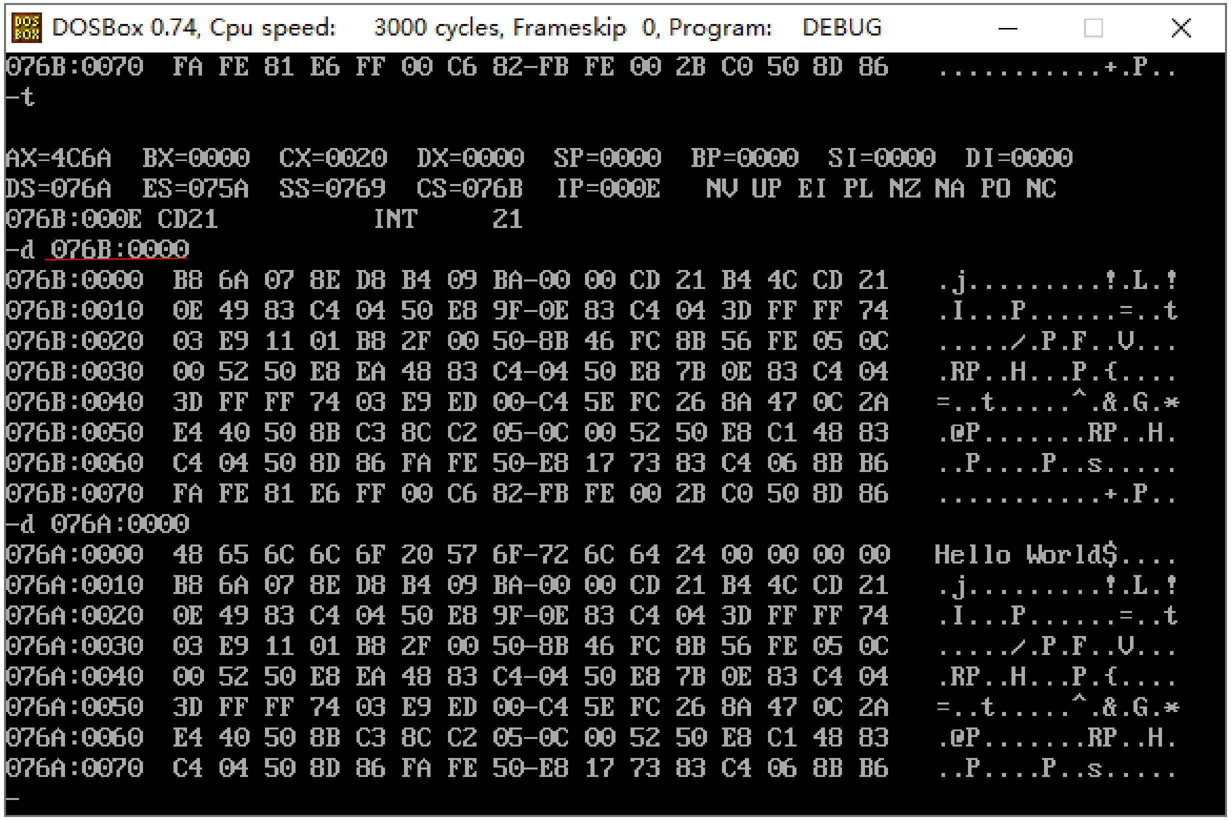
```
AX=076A  BX=0000  CX=0020  DX=0000  SP=0000  BP=0000  SI=0000  DI=0000
DS=075A  ES=075A  SS=0769  CS=076B  IP=0003   NV UP EI PL NZ NA PO NC
076B:0003 8ED8          MOV     DS,AX
-t

AX=076A  BX=0000  CX=0020  DX=0000  SP=0000  BP=0000  SI=0000  DI=0000
DS=076A  ES=075A  SS=0769  CS=076B  IP=0005   NV UP EI PL NZ NA PO NC
076B:0005 B409          MOV     AH,09
-t

AX=096A  BX=0000  CX=0020  DX=0000  SP=0000  BP=0000  SI=0000  DI=0000
DS=076A  ES=075A  SS=0769  CS=076B  IP=0007   NV UP EI PL NZ NA PO NC
076B:0007 BA0000        MOV     DX,0000
-t

AX=096A  BX=0000  CX=0020  DX=0000  SP=0000  BP=0000  SI=0000  DI=0000
DS=076A  ES=075A  SS=0769  CS=076B  IP=000A   NV UP EI PL NZ NA PO NC
076B:000A CD21          INT     21
-p
Hello World
AX=096A  BX=0000  CX=0020  DX=0000  SP=0000  BP=0000  SI=0000  DI=0000
DS=076A  ES=075A  SS=0769  CS=076B  IP=000C   NV UP EI PL NZ NA PO NC
076B:000C B44C          MOV     AH,4C
-
```

连续执行3条指令
T 3

从CS:0100H开始连续执行3条指令
T =0100 3

（3）D 查看内存单元

D 段地址:起始偏移地址 [结尾偏移地址]


DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG

```
076B:0070  FA FE 81 E6 FF 00 C6 82-FB FE 00 2B C0 50 8D 86   ...........+.P..
-t

AX=4C6A  BX=0000  CX=0020  DX=0000  SP=0000  BP=0000  SI=0000  DI=0000
DS=076A  ES=075A  SS=0769  CS=076B  IP=000E   NV UP EI PL NZ NA PO NC
076B:000E CD21          INT     21
-d 076B:0000
076B:0000  B8 6A 07 8E D8 B4 09 BA-00 00 CD 21 B4 4C CD 21   .j.........!.L.!
076B:0010  0E 49 83 C4 04 50 E8 9F-0E 83 C4 04 3D FF FF 74   .I...P......=..t
076B:0020  03 E9 11 01 B8 2F 00 50-8B 46 FC 8B 56 FE 05 0C   ...../.P.F..V...
076B:0030  00 52 50 E8 EA 48 83 C4-04 50 E8 7B 0E 83 C4 04   .RP..H...P.{....
076B:0040  3D FF FF 74 03 E9 ED 00-C4 5E FC 26 8A 47 0C 2A   =..t.....^.&.G.*
076B:0050  E4 40 50 8B C3 8C C2 05-0C 00 52 50 E8 C1 48 83   .@P.......RP..H.
076B:0060  C4 04 50 8D 86 FA FE 50-E8 17 73 83 C4 06 8B B6   ..P....P..s.....
076B:0070  FA FE 81 E6 FF 00 C6 82-FB FE 00 2B C0 50 8D 86   ...........+.P..
-d 076A:0000
076A:0000  48 65 6C 6C 6F 20 57 6F-72 6C 64 24 00 00 00 00   Hello World$....
076A:0010  B8 6A 07 8E D8 B4 09 BA-00 00 CD 21 B4 4C CD 21   .j.........!.L.!
076A:0020  0E 49 83 C4 04 50 E8 9F-0E 83 C4 04 3D FF FF 74   .I...P......=..t
076A:0030  03 E9 11 01 B8 2F 00 50-8B 46 FC 8B 56 FE 05 0C   ...../.P.F..V...
076A:0040  00 52 50 E8 EA 48 83 C4-04 50 E8 7B 0E 83 C4 04   .RP..H...P.{....
076A:0050  3D FF FF 74 03 E9 ED 00-C4 5E FC 26 8A 47 0C 2A   =..t.....^.&.G.*
076A:0060  E4 40 50 8B C3 8C C2 05-0C 00 52 50 E8 C1 48 83   .@P.......RP..H.
076A:0070  C4 04 50 8D 86 FA FE 50-E8 17 73 83 C4 06 8B B6   ..P....P..s.....
-
```

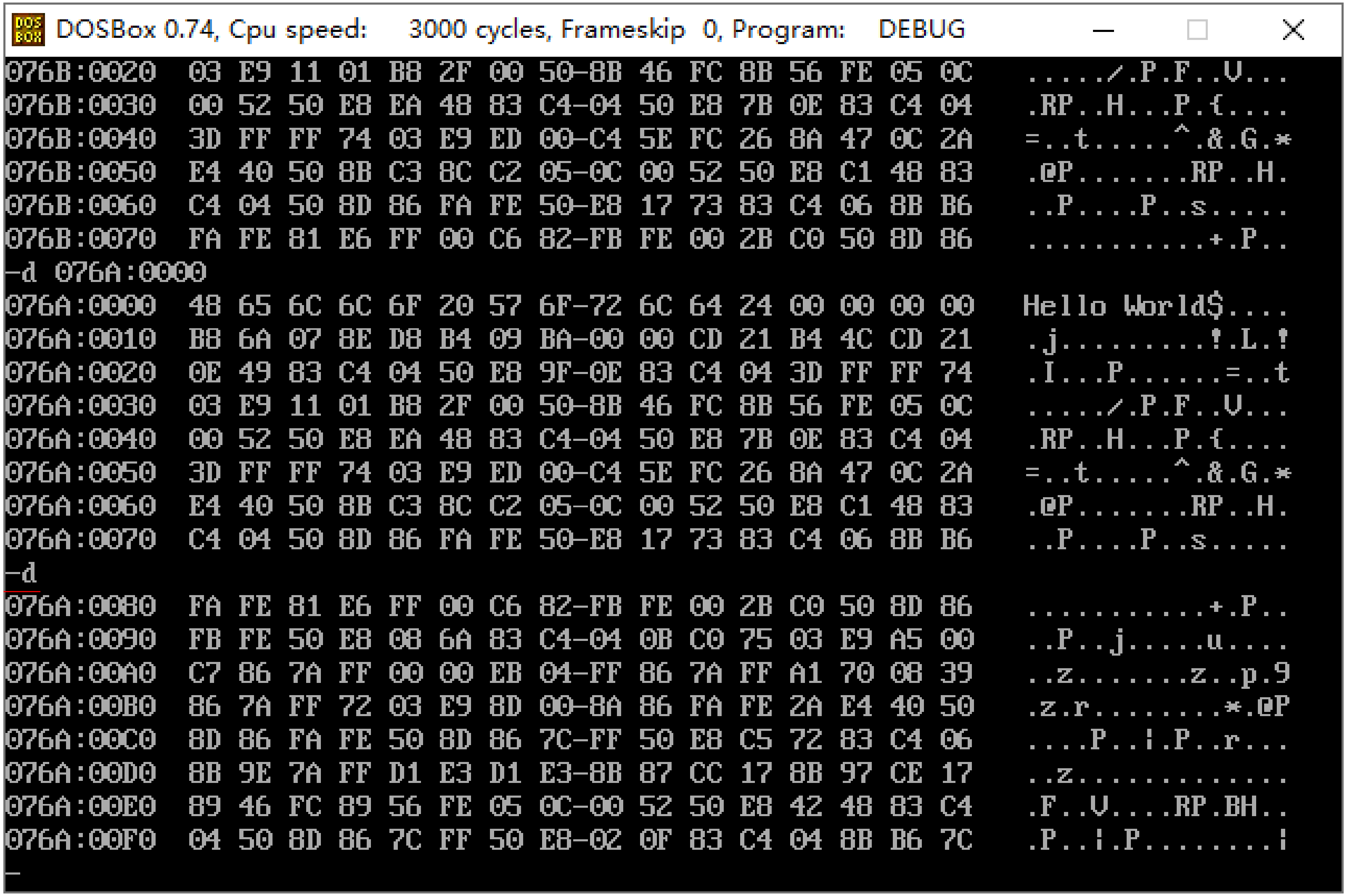
查看数据段
D DS:100

查看附加段
D ES:0

查看0200H段的5号到15H号单元
D 0200:5 15

从数据段100H号单元开始显示
D100

//多次键入D，可连续显示后面的单元内容。


DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG

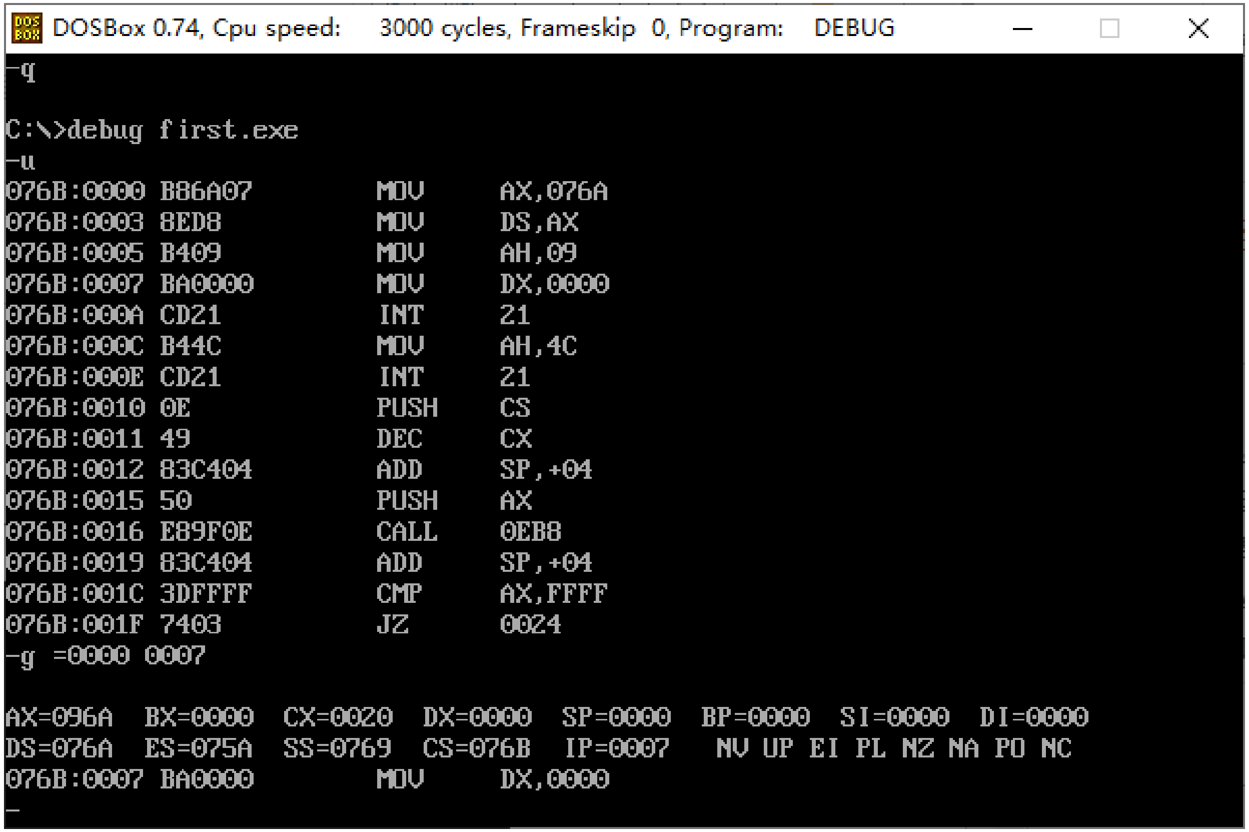
```
076B:0020  03 E9 11 01 B8 2F 00 50-8B 46 FC 8B 56 FE 05 0C   ...../.P.F..V...
076B:0030  00 52 50 E8 EA 48 83 C4-04 50 E8 7B 0E 83 C4 04   .RP..H...P.{....
076B:0040  3D FF FF 74 03 E9 ED 00-C4 5E FC 26 8A 47 0C 2A   =..t.....^.&.G.*
076B:0050  E4 40 50 8B C3 8C C2 05-0C 00 52 50 E8 C1 48 83   .@P.......RP..H.
076B:0060  C4 04 50 8D 86 FA FE 50-E8 17 73 83 C4 06 8B B6   ..P....P..s.....
076B:0070  FA FE 81 E6 FF 00 C6 82-FB FE 00 2B C0 50 8D 86   ...........+.P..
-d 076A:0000
076A:0000  48 65 6C 6C 6F 20 57 6F-72 6C 64 24 00 00 00 00   Hello World$....
076A:0010  B8 6A 07 8E D8 B4 09 BA-00 00 CD 21 B4 4C CD 21   .j.........!.L.!
076A:0020  0E 49 83 C4 04 50 E8 9F-0E 83 C4 04 3D FF FF 74   .I...P......=..t
076A:0030  03 E9 11 01 B8 2F 00 50-8B 46 FC 8B 56 FE 05 0C   ...../.P.F..V...
076A:0040  00 52 50 E8 EA 48 83 C4-04 50 E8 7B 0E 83 C4 04   .RP..H...P.{....
076A:0050  3D FF FF 74 03 E9 ED 00-C4 5E FC 26 8A 47 0C 2A   =..t.....^.&.G.*
076A:0060  E4 40 50 8B C3 8C C2 05-0C 00 52 50 E8 C1 48 83   .@P.......RP..H.
076A:0070  C4 04 50 8D 86 FA FE 50-E8 17 73 83 C4 06 8B B6   ..P....P..s.....
-d
076A:0080  FA FE 81 E6 FF 00 C6 82-FB FE 00 2B C0 50 8D 86   ...........+.P..
076A:0090  FB FE 50 E8 08 6A 83 C4-04 0B C0 75 03 E9 A5 00   ..P..j.....u....
076A:00A0  C7 86 7A FF 00 00 EB 04-FF 86 7A FF A1 70 08 39   ..z.......z..p.9
076A:00B0  86 7A FF 72 03 E9 8D 00-8A 86 FA FE 2A E4 40 50   .z.r........*.@P
076A:00C0  8D 86 FA FE 50 8D 86 7C-FF 50 E8 C5 72 83 C4 06   ....P..¦.P..r...
076A:00D0  8B 9E 7A FF D1 E3 D1 E3-8B 87 CC 17 8B 97 CE 17   ..z.............
076A:00E0  89 46 FC 89 56 FE 05 0C-00 52 50 E8 42 48 83 C4   .F..V....RP.BH..
076A:00F0  04 50 8D 86 7C FF 50 E8-02 0F 83 C4 04 8B B6 7C   .P..¦.P........¦
-
```

（4）G 执行指令

格式：G [=address][breakpoints]

参数：=address：指定当前在内存中开始执行的内存地址。

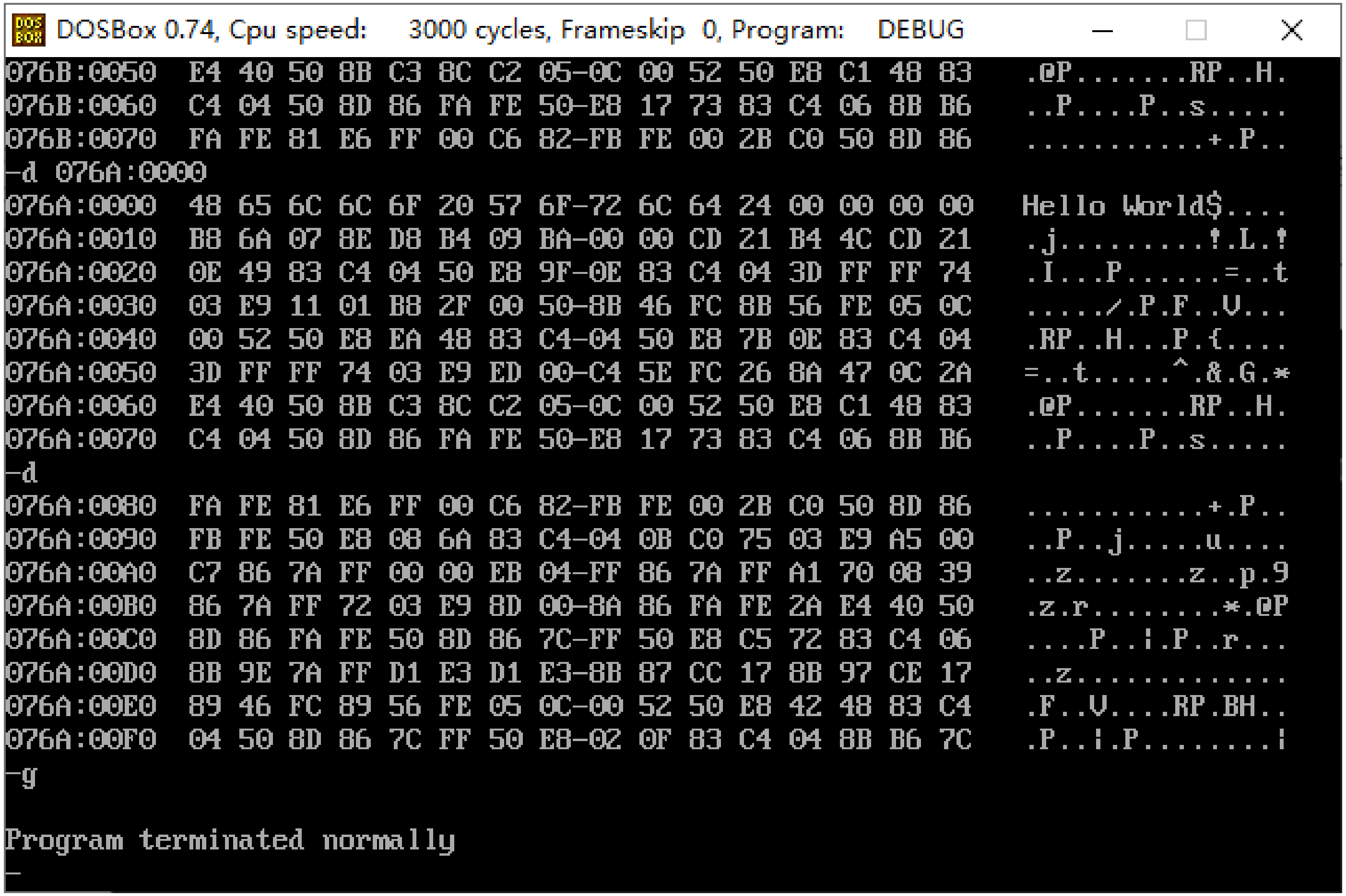
breakpoints：为G命令设置的临时断点



DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG

```
-q

C:\>debug first.exe
-u
076B:0000 B86A07        MOV     AX,076A
076B:0003 8ED8          MOV     DS,AX
076B:0005 B409          MOV     AH,09
076B:0007 BA0000        MOV     DX,0000
076B:000A CD21          INT     21
076B:000C B44C          MOV     AH,4C
076B:000E CD21          INT     21
076B:0010 0E            PUSH    CS
076B:0011 49            DEC     CX
076B:0012 83C404        ADD     SP,+04
076B:0015 50            PUSH    AX
076B:0016 E89F0E        CALL    0EB8
076B:0019 83C404        ADD     SP,+04
076B:001C 3DFFFF        CMP     AX,FFFF
076B:001F 7403          JZ      0024
-g =0000 0007

AX=096A  BX=0000  CX=0020  DX=0000  SP=0000  BP=0000  SI=0000  DI=0000
DS=076A  ES=075A  SS=0769  CS=076B  IP=0007   NV UP EI PL NZ NA PO NC
076B:0007 BA0000        MOV     DX,0000
-
```

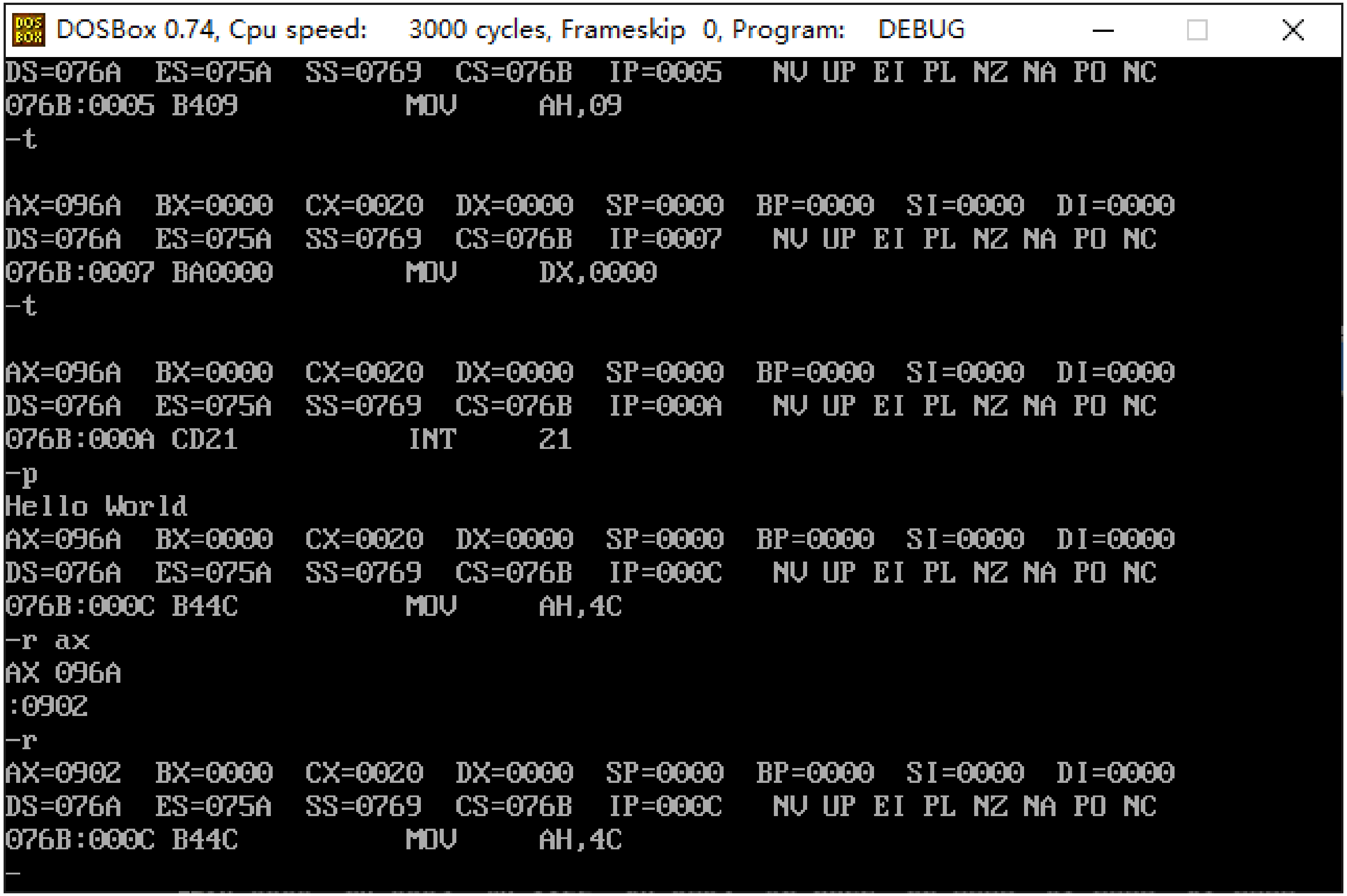
如果不指定参数，将从CS:IP寄存器中当前地址中开始执行程序



DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG

```
076B:0050  E4 40 50 8B C3 8C C2 05-0C 00 52 50 E8 C1 48 83   .@P.......RP..H.
076B:0060  C4 04 50 8D 86 FA FE 50-E8 17 73 83 C4 06 8B B6   ..P....P..s.....
076B:0070  FA FE 81 E6 FF 00 C6 82-FB FE 00 2B C0 50 8D 86   ...........+.P..
-d 076A:0000
076A:0000  48 65 6C 6C 6F 20 57 6F-72 6C 64 24 00 00 00 00   Hello World$....
076A:0010  B8 6A 07 8E D8 B4 09 BA-00 00 CD 21 B4 4C CD 21   .j.........!.L.!
076A:0020  0E 49 83 C4 04 50 E8 9F-0E 83 C4 04 3D FF FF 74   .I...P......=..t
076A:0030  03 E9 11 01 B8 2F 00 50-8B 46 FC 8B 56 FE 05 0C   ...../.P.F..V...
076A:0040  00 52 50 E8 EA 48 83 C4-04 50 E8 7B 0E 83 C4 04   .RP..H...P.{....
076A:0050  3D FF FF 74 03 E9 ED 00-C4 5E FC 26 8A 47 0C 2A   =..t.....^.&.G.*
076A:0060  E4 40 50 8B C3 8C C2 05-0C 00 52 50 E8 C1 48 83   .@P.......RP..H.
076A:0070  C4 04 50 8D 86 FA FE 50-E8 17 73 83 C4 06 8B B6   ..P....P..s.....
-d
076A:0080  FA FE 81 E6 FF 00 C6 82-FB FE 00 2B C0 50 8D 86   ...........+.P..
076A:0090  FB FE 50 E8 08 6A 83 C4-04 0B C0 75 03 E9 A5 00   ..P..j.....u....
076A:00A0  C7 86 7A FF 00 00 EB 04-FF 86 7A FF A1 70 08 39   ..z.......z..p.9
076A:00B0  86 7A FF 72 03 E9 8D 00-8A 86 FA FE 2A E4 40 50   .z.r........*.@P
076A:00C0  8D 86 FA FE 50 8D 86 7C-FF 50 E8 C5 72 83 C4 06   ....P..¦.P..r...
076A:00D0  8B 9E 7A FF D1 E3 D1 E3-8B 87 CC 17 8B 97 CE 17   ..z.............
076A:00E0  89 46 FC 89 56 FE 05 0C-00 52 50 E8 42 48 83 C4   .F..V....RP.BH..
076A:00F0  04 50 8D 86 7C FF 50 E8-02 0F 83 C4 04 8B B6 7C   .P..¦.P........¦
-g

Program terminated normally
-
```

（5）R 查看和修改寄存器内容



DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG

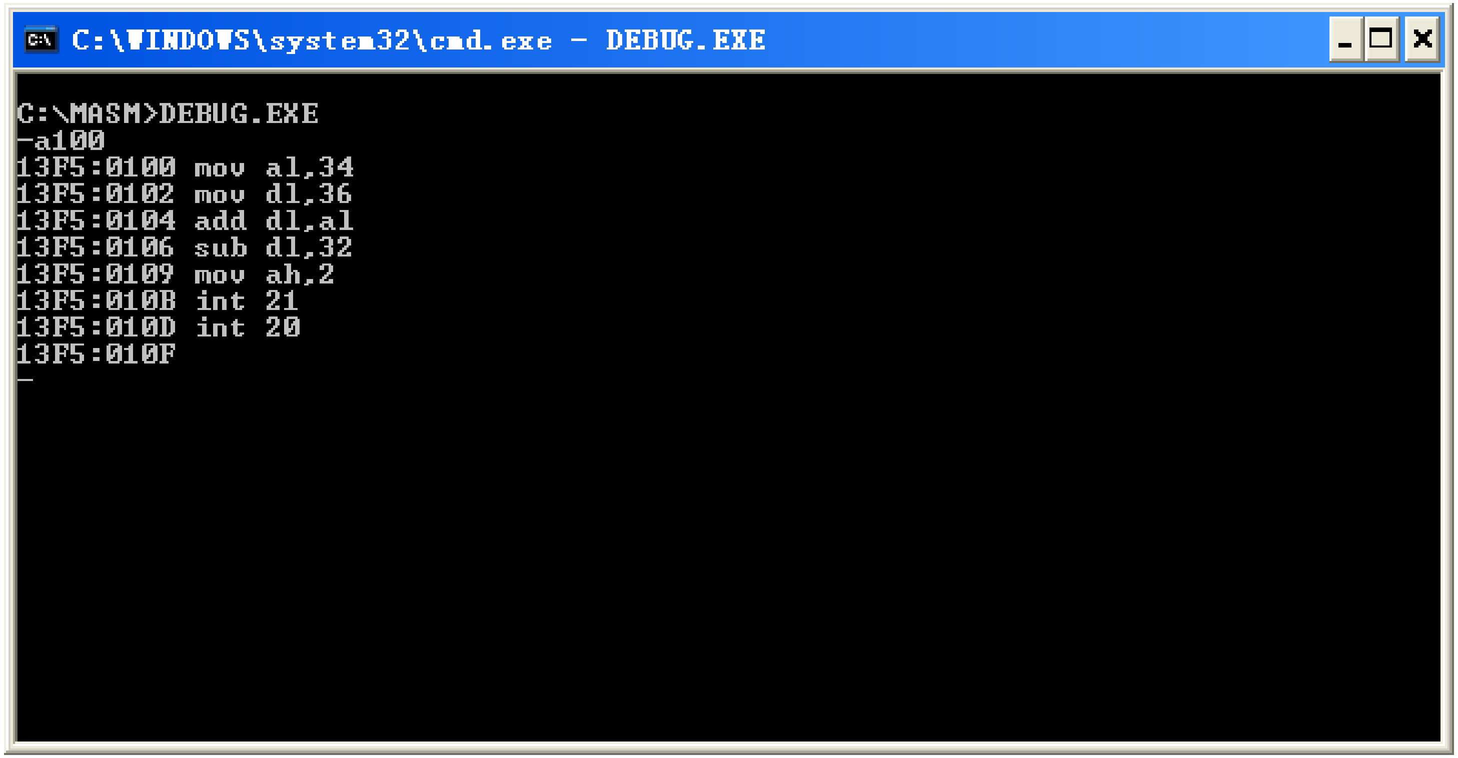
```
DS=076A  ES=075A  SS=0769  CS=076B  IP=0005   NV UP EI PL NZ NA PO NC
076B:0005 B409          MOV     AH,09
-t

AX=096A  BX=0000  CX=0020  DX=0000  SP=0000  BP=0000  SI=0000  DI=0000
DS=076A  ES=075A  SS=0769  CS=076B  IP=0007   NV UP EI PL NZ NA PO NC
076B:0007 BA0000        MOV     DX,0000
-t

AX=096A  BX=0000  CX=0020  DX=0000  SP=0000  BP=0000  SI=0000  DI=0000
DS=076A  ES=075A  SS=0769  CS=076B  IP=000A   NV UP EI PL NZ NA PO NC
076B:000A CD21          INT     21
-p
Hello World
AX=096A  BX=0000  CX=0020  DX=0000  SP=0000  BP=0000  SI=0000  DI=0000
DS=076A  ES=075A  SS=0769  CS=076B  IP=000C   NV UP EI PL NZ NA PO NC
076B:000C B44C          MOV     AH,4C
-r ax
AX 096A
:0902
-r
AX=0902  BX=0000  CX=0020  DX=0000  SP=0000  BP=0000  SI=0000  DI=0000
DS=076A  ES=075A  SS=0769  CS=076B  IP=000C   NV UP EI PL NZ NA PO NC
076B:000C B44C          MOV     AH,4C
-
```

（5）A（汇编命令）

功能：从汇编语言程序创建可以执行的机器码

格式：A address

如果不制定位置，它会从上次停止处得地址开始汇编。

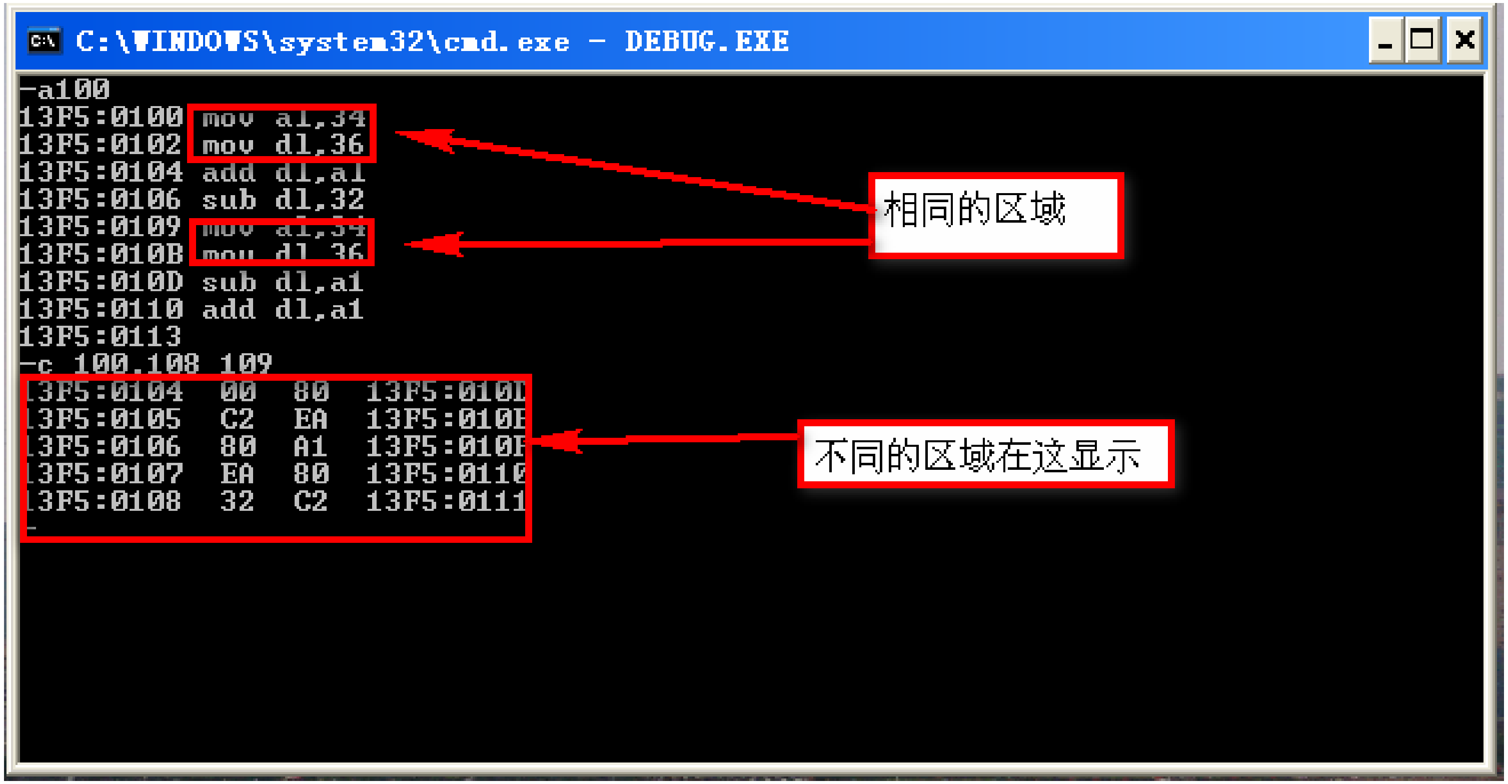


```
C:\MASM>DEBUG.EXE
-a100
13F5:0100 mov al,34
13F5:0102 mov dl,36
13F5:0104 add dl,al
13F5:0106 sub dl,32
13F5:0109 mov ah,2
13F5:010B int 21
13F5:010D int 20
13F5:010F
-
```

（6） C（表命令）

功能：比较内存的两个区域存放的内容

命令格式：C range address



```
-a100
13F5:0100 mov al,34
13F5:0102 mov dl,36
13F5:0104 add dl,al
13F5:0106 sub dl,32
13F5:0109 mov al,34
13F5:010B mov dl,36
13F5:010D sub dl,al
13F5:0110 add dl,al
13F5:0113
-c 100,108 109
13F5:0104  00  80  13F5:010D
13F5:0105  C2  EA  13F5:010E
13F5:0106  80  A1  13F5:010F
13F5:0107  EA  80  13F5:0110
13F5:0108  32  C2  13F5:0111
-
```

相同的区域

不同的区域在这显示