

源码一:

```
.model small
.data
Hello      DB 'Hello world!',0dh,0ah,'$'
.code
START:     MOV AX,@DATA
           MOV DS,AX
           LEA DX,Hello
           MOV AH,9
           INT 21H

           MOV AX,4C00H
           INT 21h

END  START
```

汇编链接后:

```
D:\>debug hello.exe
-u
076A:0000 B86B07      MOV     AX,076B
076A:0003 8ED8          MOV     DS,AX
076A:0005 8D160200      LEA     DX,[0002]
076A:0009 B409          MOV     AH,09
076A:000B CD21          INT     21
076A:000D B8004C      MOV     AX,4C00
076A:0010 CD21          INT     21
076A:0012 4B           DEC     AX
```

源码二:

```
.model small
.data
Hello      DB 'Hello world!',0dh,0ah,'$'
.code
START:     MOV AX,@DATA
           MOV DS,AX
           MOV DX,offset Hello
           MOV AH,9
           INT 21H

           MOV AX,4C00H
           INT 21h

END  START
```

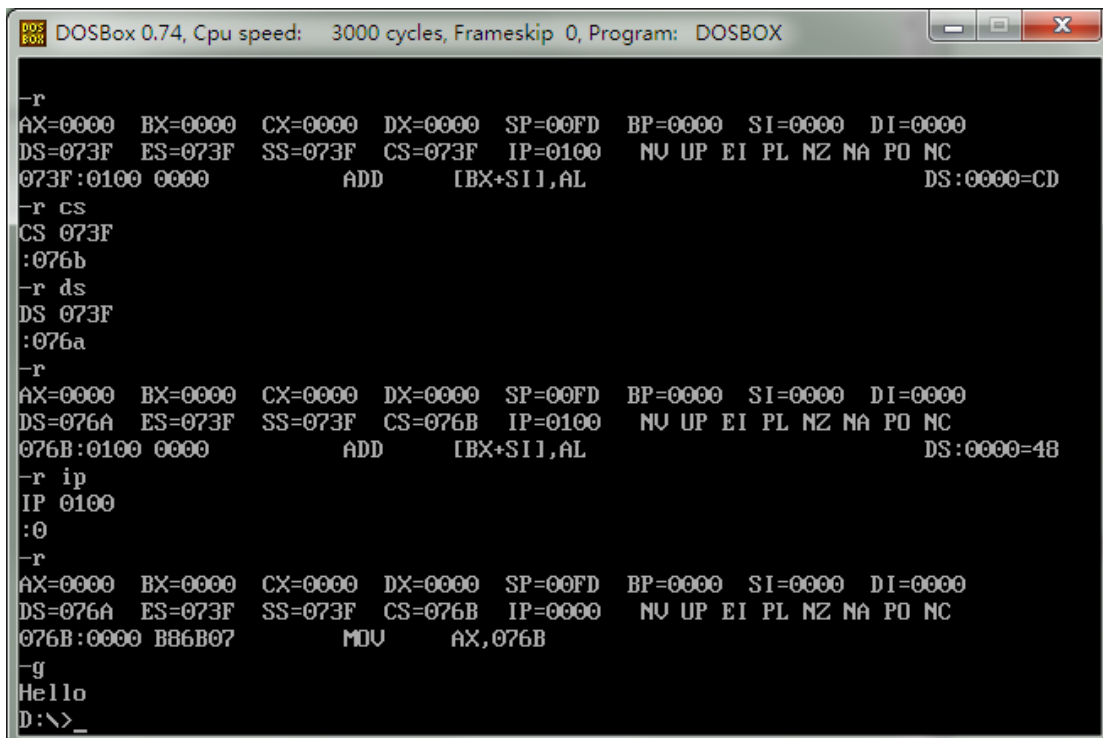
汇编链接后:

```
D:\>debug hello.exe
-u
076A:0000 B86B07      MOV     AX,076B
076A:0003 8ED8          MOV     DS,AX
076A:0005 BA0200      MOV     DX,0002
076A:0008 B409          MOV     AH,09
076A:000A CD21          INT     21
076A:000C B8004C      MOV     AX,4C00
076A:000F CD21          INT     21
076A:0011 004865      ADD     [BX+SI+6]
```

通过一、二，比较两种获取偏移地址的方式。

## Hello 的另类执行方式

- 1) 在汇编阶段选择生成列表文件 (\*.lst) --可直接用写字板打开 (显示地址、内容、源码等对应关系)
- 2) 在汇编阶段选择生成交叉引用文件 (\*.crf) --不能直接用写字板打开, 用 CREF 工具转成 \*.ref 文件后可用写字板浏览。(显示符号的定义及引用位置)
- 3) 直接写内存方式执行代码:
  - A) 写数据 "Hello\$" 对应的 ASCII 码 48 65 6c 6c 6f 24 写入内存  
Debug 下用 -e 076a: 0 回车 一次写入 (用空格自动分开了) -----相当于 DS: 076A
  - B) 写代码的机器码 b8 6b 07 be d8 ba 02 00 b4 09 cd 21 b8 00 4c cd 21 (17 个字节) 写入内存  
Debug 下用 -e 076b: 0 回车 一次写入 (用空格自动分开了) -----相当于 CS: 076B
  - C) 修改寄存器及执行, 如下图所示



```
-r
AX=0000 BX=0000 CX=0000 DX=0000 SP=00FD BP=0000 SI=0000 DI=0000
DS=073F ES=073F SS=073F CS=073F IP=0100  NU UP EI PL NZ NA PO NC
073F:0100 0000          ADD     [BX+SI],AL          DS:0000=CD
-r cs
CS 073F
:076b
-r ds
DS 073F
:076a
-r
AX=0000 BX=0000 CX=0000 DX=0000 SP=00FD BP=0000 SI=0000 DI=0000
DS=076A ES=073F SS=073F CS=076B IP=0100  NU UP EI PL NZ NA PO NC
076B:0100 0000          ADD     [BX+SI],AL          DS:0000=4B
-r ip
IP 0100
:0
-r
AX=0000 BX=0000 CX=0000 DX=0000 SP=00FD BP=0000 SI=0000 DI=0000
DS=076A ES=073F SS=073F CS=076B IP=0000  NU UP EI PL NZ NA PO NC
076B:0000 B86B07      MOV     AX,076B
-g
Hello
D:\>
```