第一步:首先编写源码

```
int Fun2(int x, int y, int z) //三个参数
{
int iTest4 = x + y * z;
    return iTest4;
}


int Fun1(int n, int m)    //两个参数
{
 int iTest3 = 0;
 iTest3 = n + m;
 iTest3 = Fun2(n,m,iTest3)
     return iTest3;
 }

 int main()
 {
 int iTest1 = 2;           //三个变量
 int iTest2 = 3;
 double iTest2 = 2.5;
 Fun1(iTest1, iTest2);
     return 0;
 }
```

第二步：按F9加断点，F5进行调试，查看内存变化。

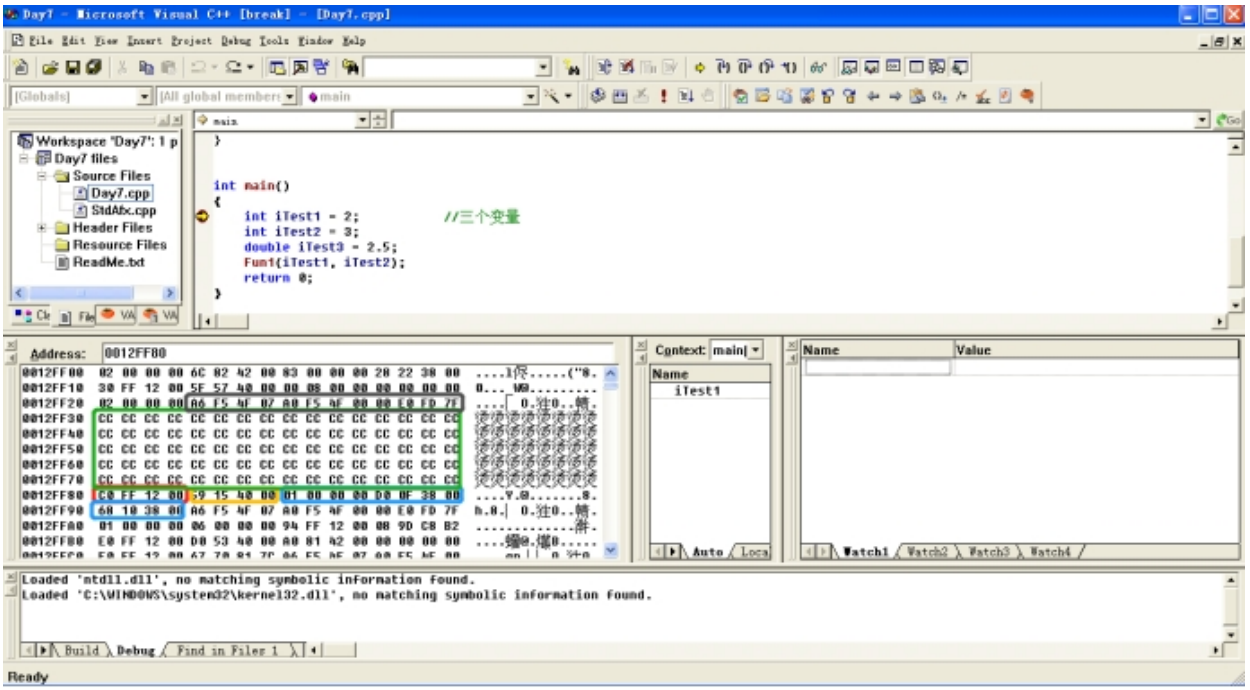
蓝色：main函数三个参数

黄色：main函数返回地址

红色：调用者的栈底

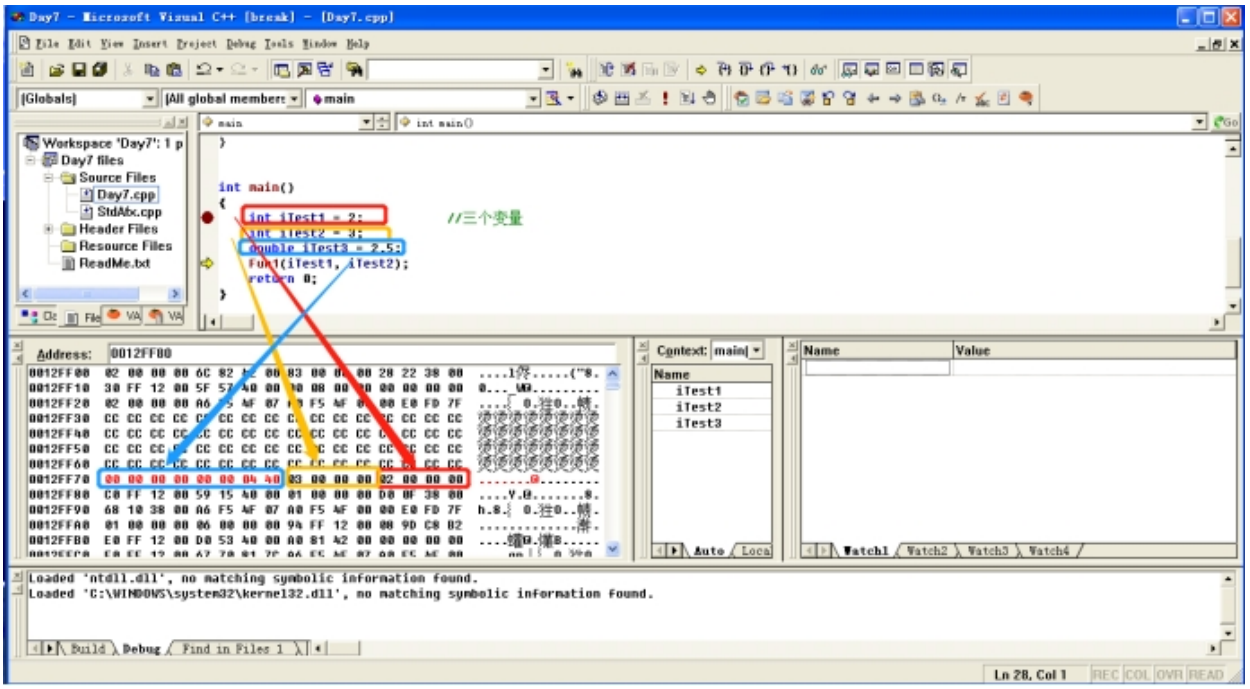
绿色：main函数申请的局部变量空间

黑色：保存的寄存器的环境



第三步：继续按F10进行调试，查看内存变化。

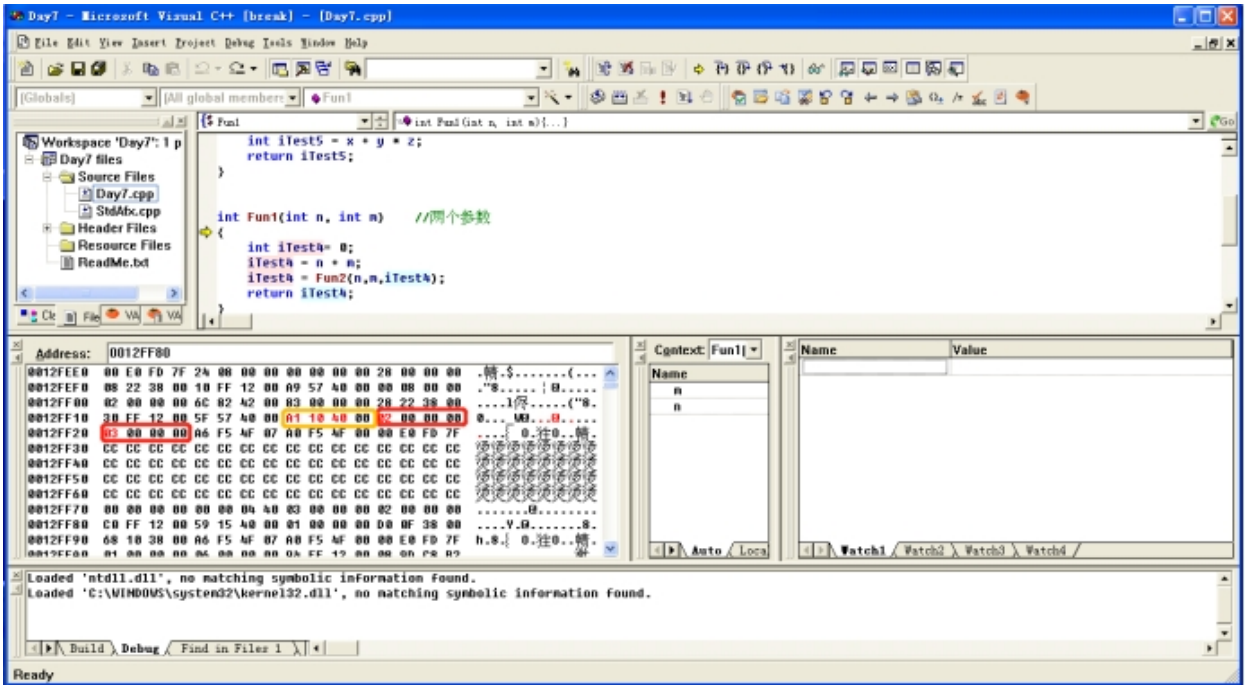
main函数当中的局部变量储存到申请的地址当中



第四步：继续按F11进入到Fun1函数当中，查看内存变化。

红色：Fun1的2个参数

黄色：Fun1的返还地址

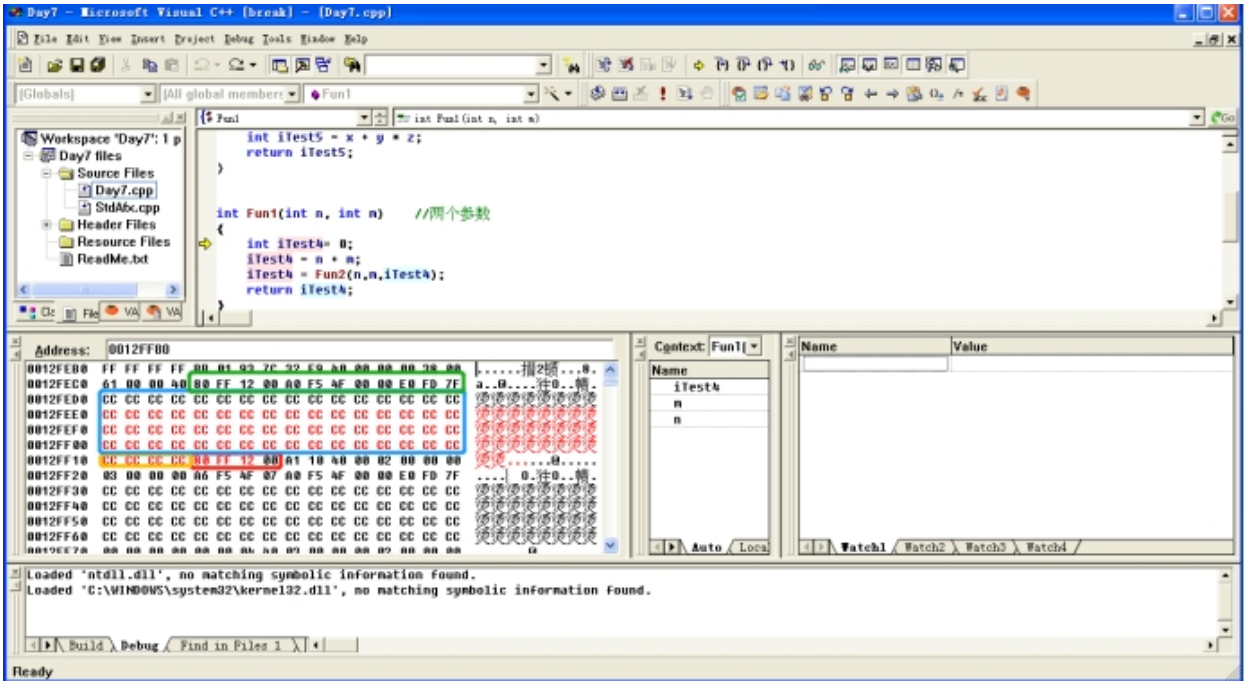


第五步：继续按F11，查看内存变化。

红色：main函数的栈底地址

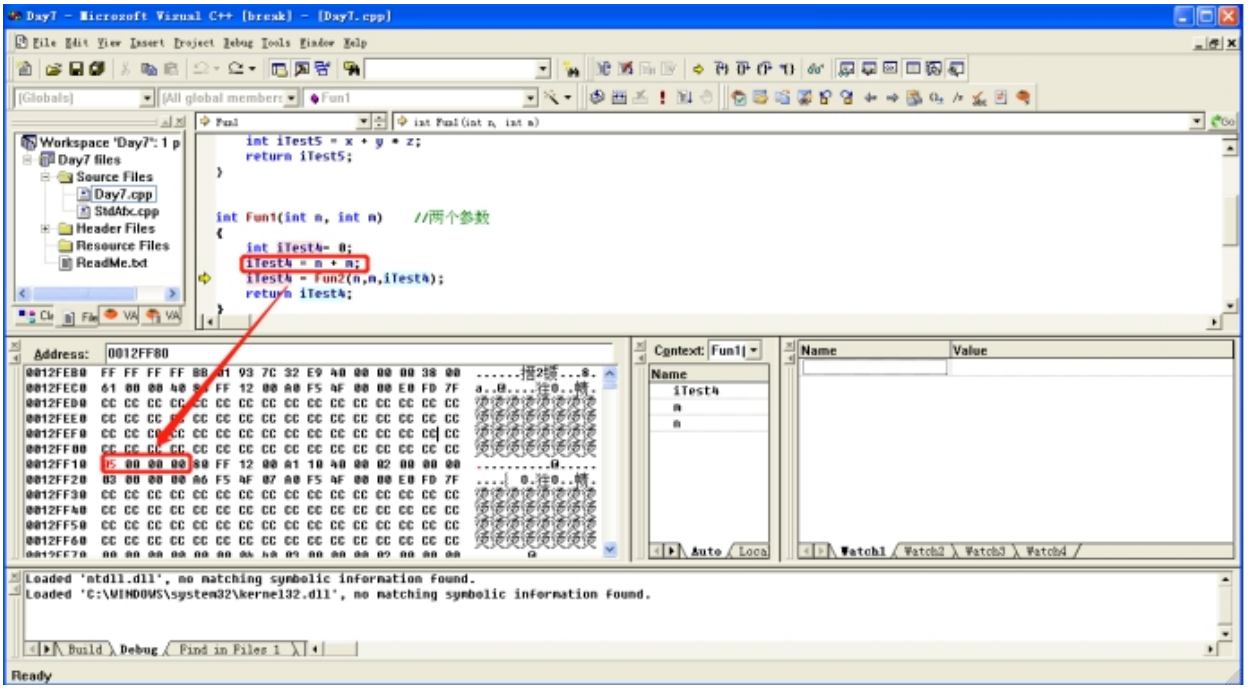
绿色：寄存器的保存

黄色、蓝色：申请的Fun1的变量空间



第五步：继续按F10，进程进行到 iTest4 = Fun2(n,m,iTest4)；查看内存变化。

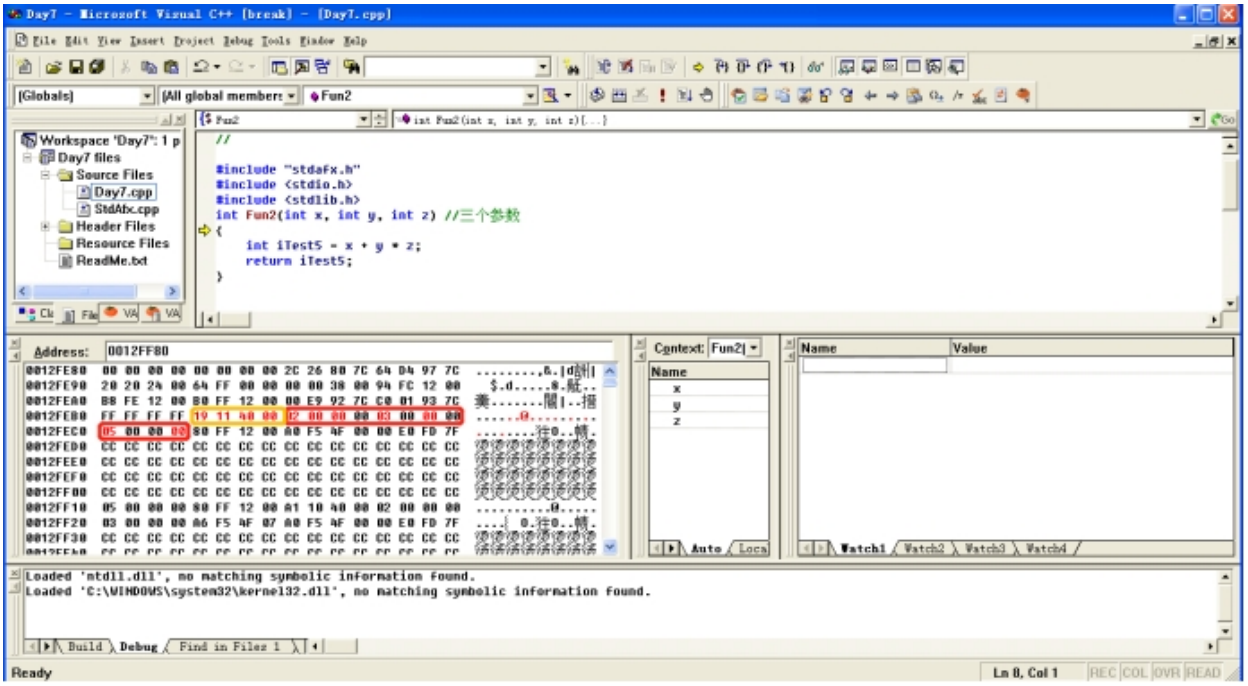
变量从0变为5



第六步：继续按F11，进程进入到Fun2函数当中；查看内存变化。

红色：Fun2的3个参数

黄色：Fun2的返还地址

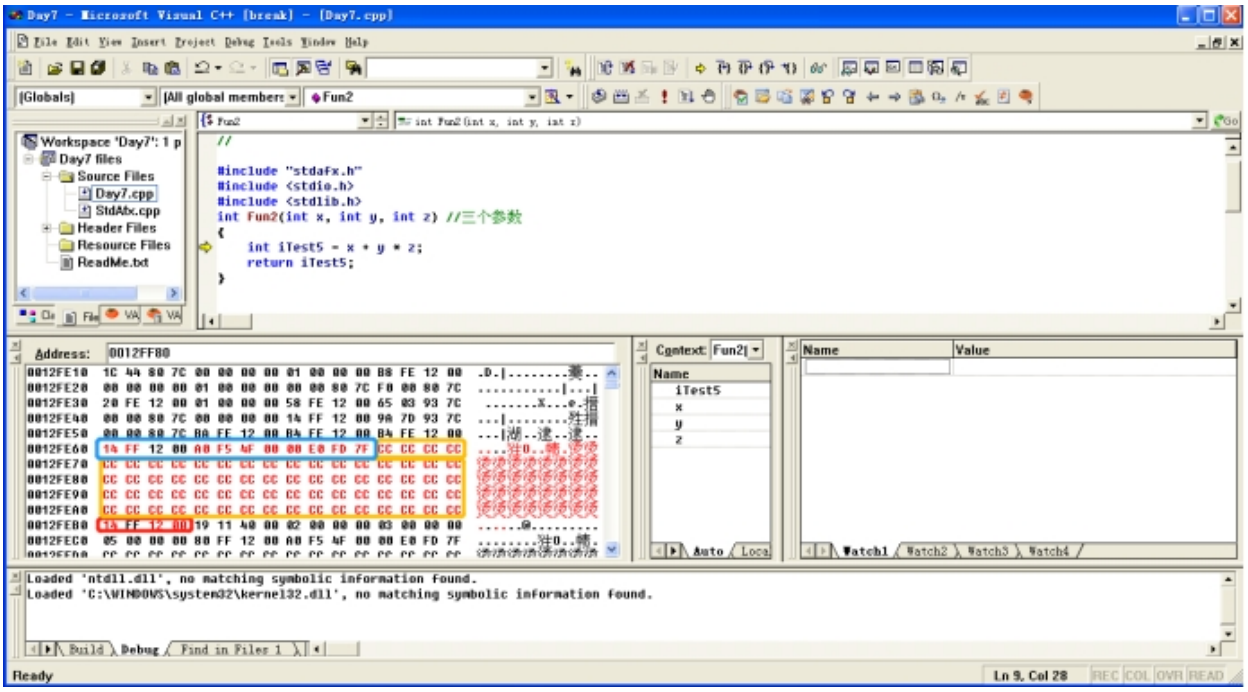


第七步：继续按F10，查看内存变化。

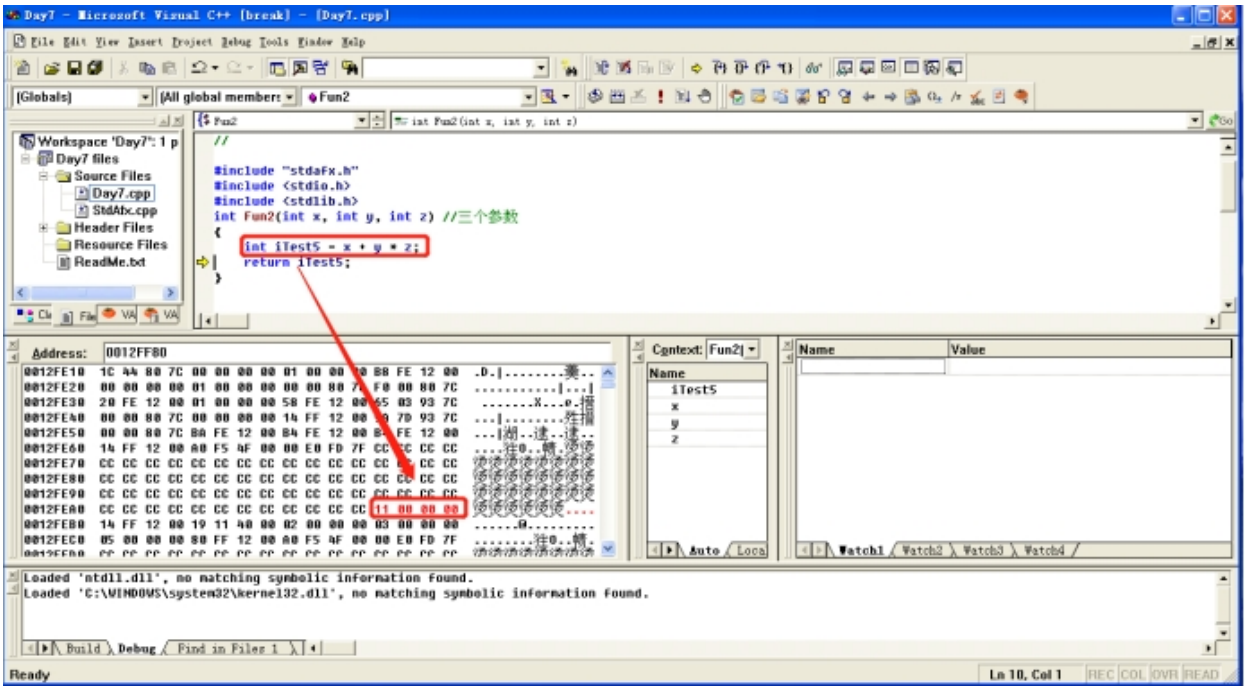
红色：Fun1函数的栈底地址

蓝色：保存寄存器的环境

黄色：Fun2申请的变量内存

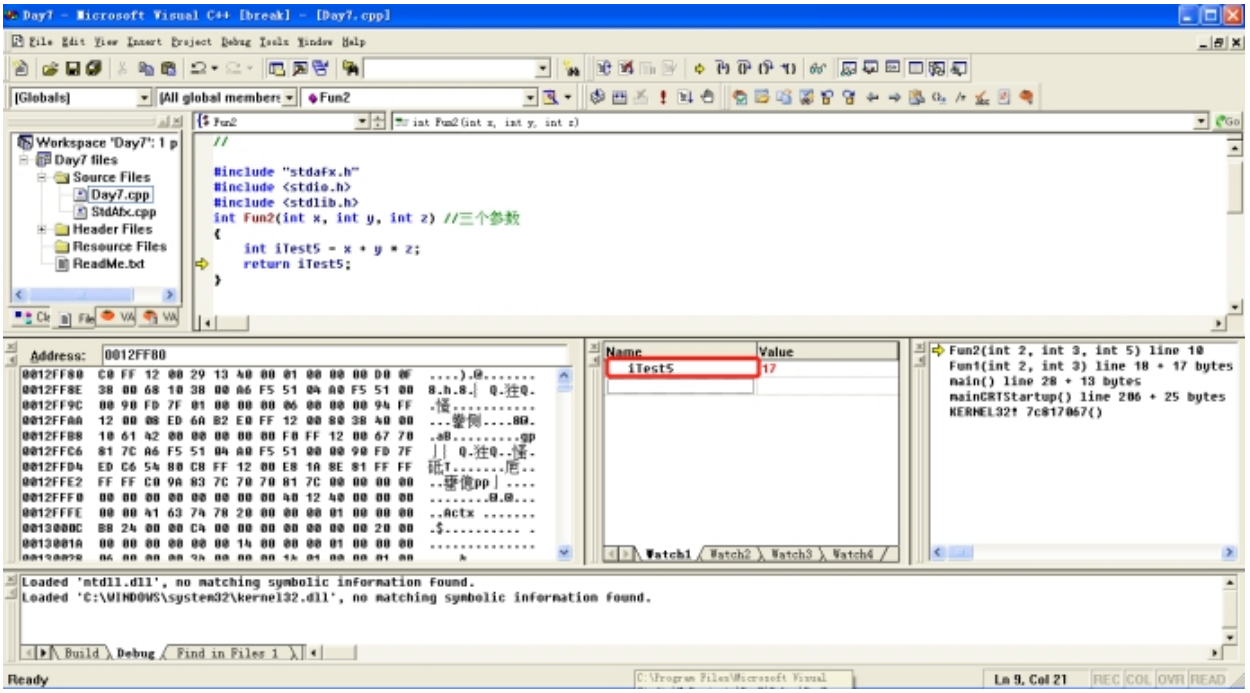


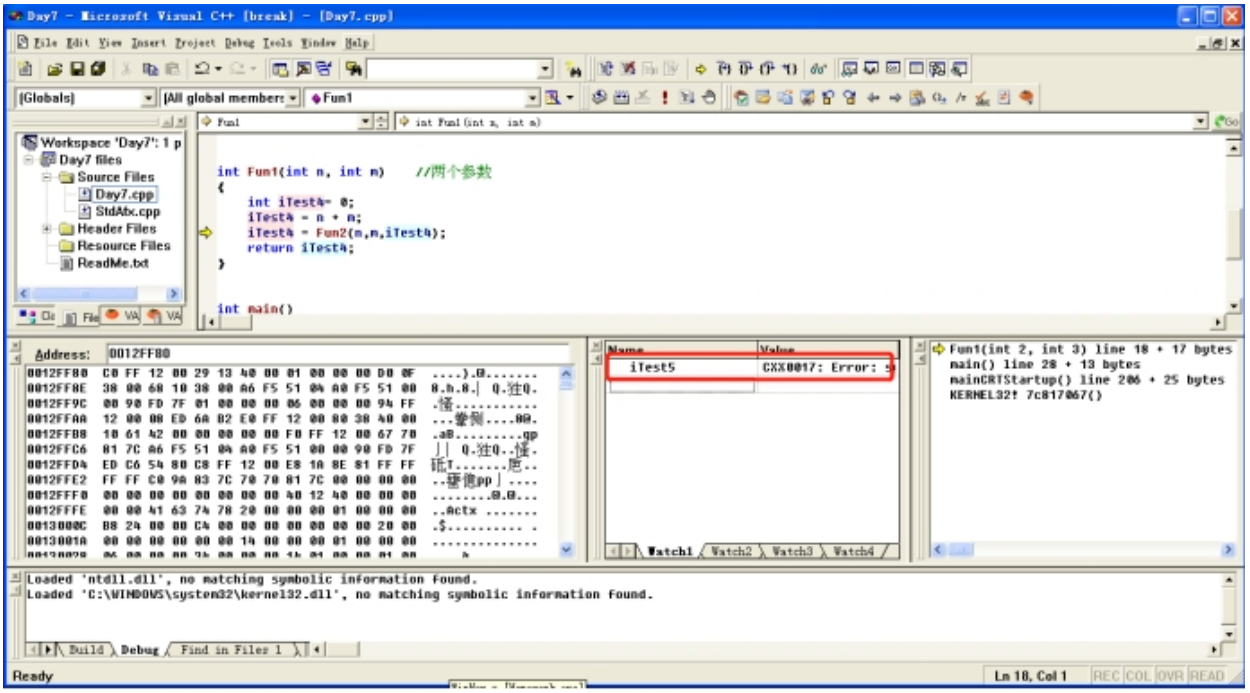
可以观察到iTest5的值为11。

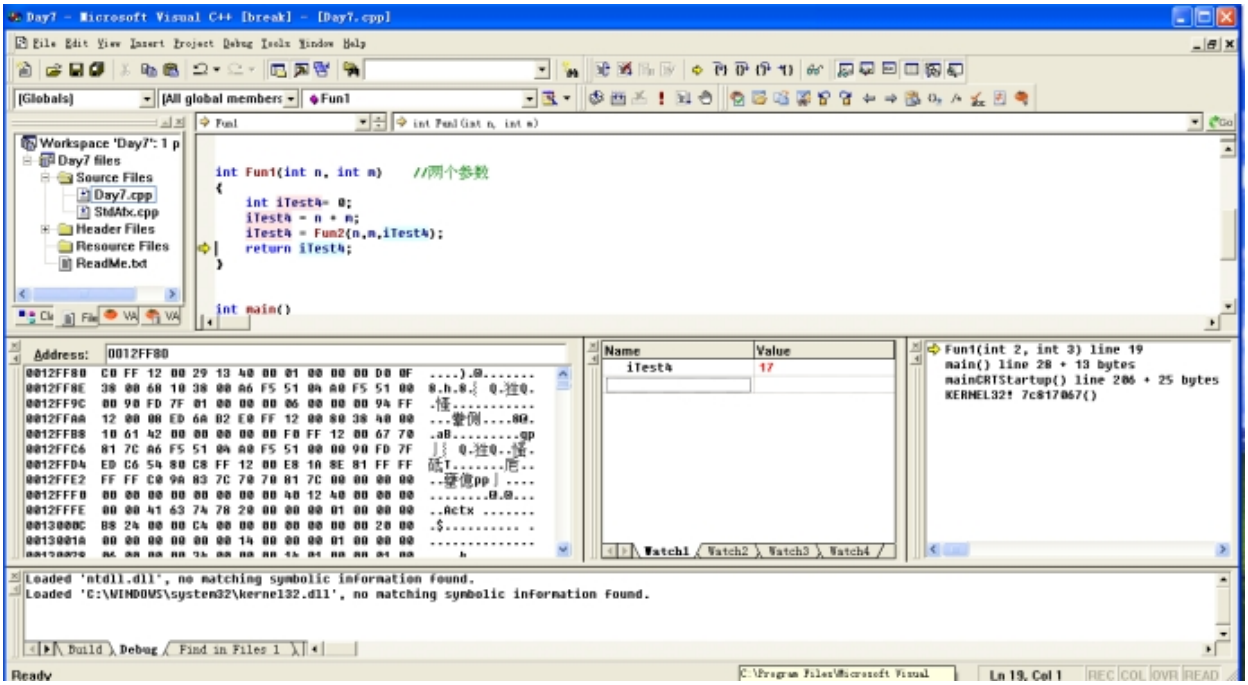


第八步：函数开始返回

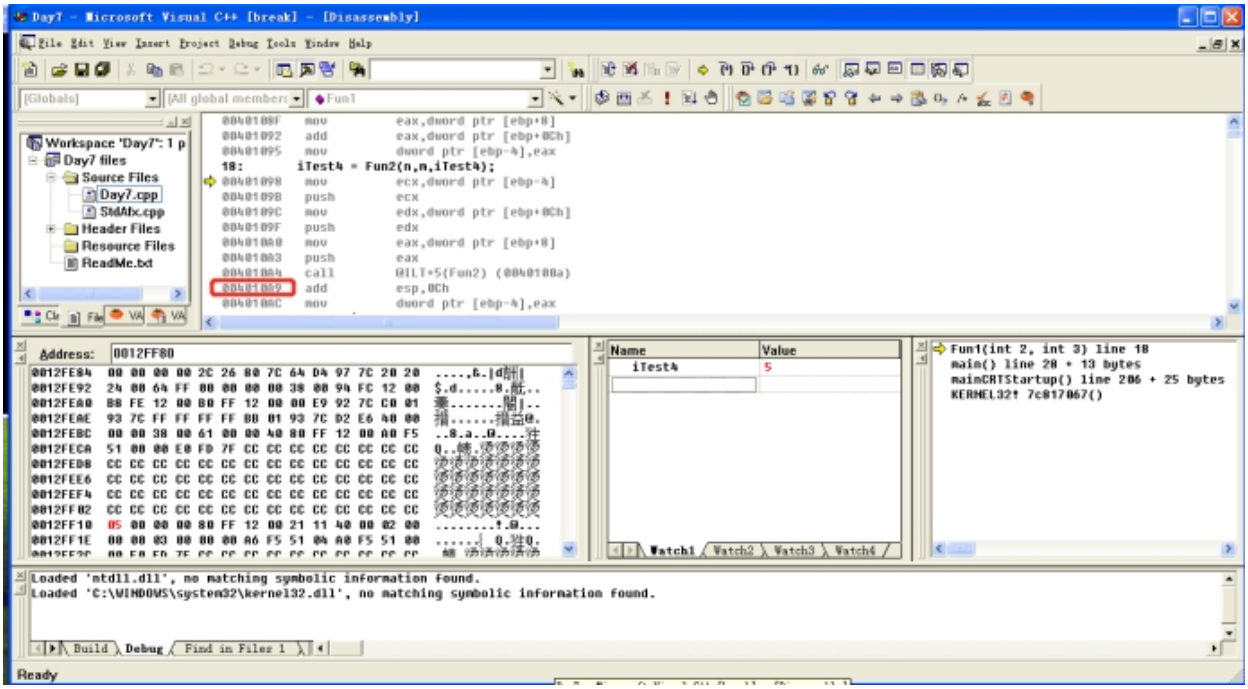
释放局部变量的空间


Day7 - Microsoft Visual C++ [break] - [Day7.cpp]
Workspace 'Day7': 1 p
Day7 files
Source Files
Day7.cpp
StdAfx.cpp
Header Files
Resource Files
ReadMe.txt
//
#include "stdafx.h"
#include <stdio.h>
#include <stdlib.h>
int Fun2(int x, int y, int z) //三个参数
{
int iTest5 = x + y * z;
return iTest5;
}
Name
Value
iTest5
17
Fun2(int 2, int 3, int 5) line 10
Fun1(int 2, int 3) line 18 + 17 bytes
main() line 28 + 13 bytes
mainCRTStartup() line 206 + 25 bytes
KERNEL32! 7c817067()
Loaded 'ntdll.dll', no matching symbolic information found.
Loaded 'C:\WINDOWS\system32\kernel32.dll', no matching symbolic information found.
Ready

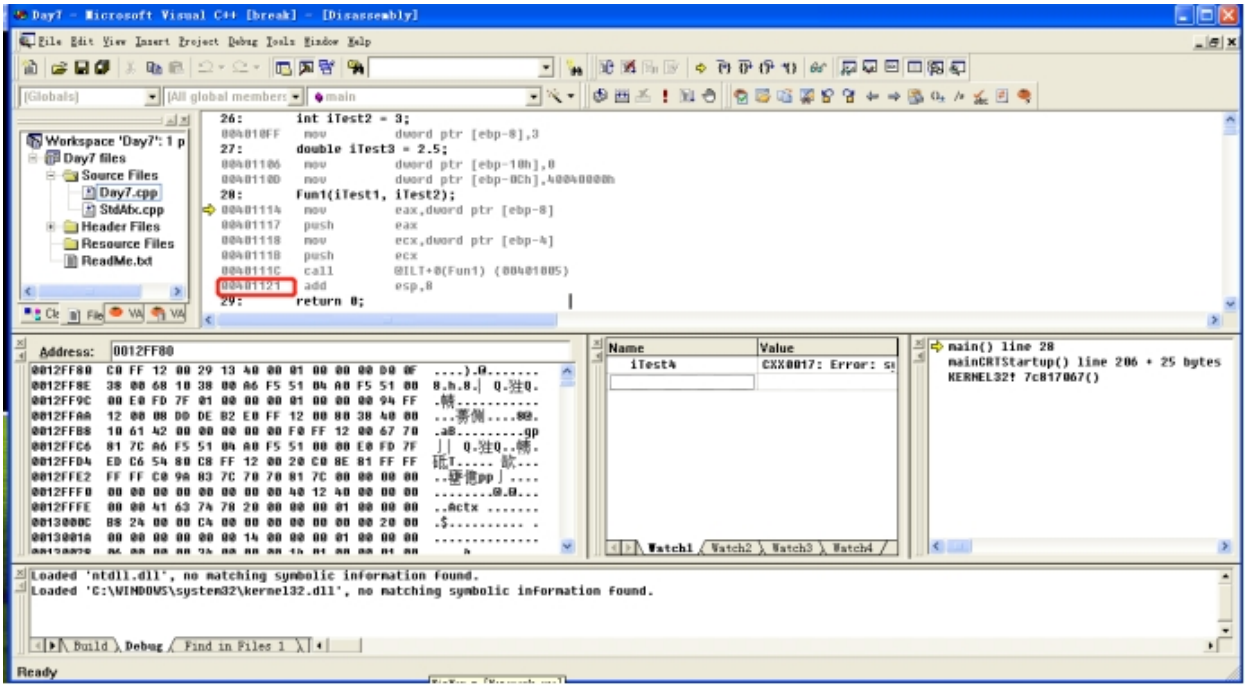

Day7 - Microsoft Visual C++ [break] - [Day7.cpp]
Workspace 'Day7': 1 p
Day7 files
Source Files
Day7.cpp
StdAfx.cpp
Header Files
Resource Files
ReadMe.txt
int Fun1(int n, int m) //两个参数
{
int iTest4= 0;
iTest4 = n + m;
iTest4 = Fun2(m,m,iTest4);
return iTest4;
}
int main()
Name
Value
iTest5
CXX0017: Error: s
Fun1(int 2, int 3) line 18 + 17 bytes
main() line 28 + 13 bytes
mainCRTStartup() line 206 + 25 bytes
KERNEL32! 7c817067()
Loaded 'ntdll.dll', no matching symbolic information found.
Loaded 'C:\WINDOWS\system32\kernel32.dll', no matching symbolic information found.
Ready



Fun2返回到Fun1的位置



Fun1函数返回到main函数的位置


Day7 - Microsoft Visual C++ [break] - [Disassembly]
File Edit View Insert Project Debug Tools Window Help
Workspace 'Day7': 1 p
Day7 files
Source Files
Day7.cpp
StdAfx.cpp
Header Files
Resource Files
ReadMe.txt
26: int iTest2 = 3;
00401000 mov dword ptr [ebp-8],3
27: double iTest3 = 2.5;
00401007 mov dword ptr [ebp-10h],0
0040100E mov dword ptr [ebp-0Ch],40040000h
28: Fun1(iTest1, iTest2);
00401015 mov eax,dword ptr [ebp-8]
00401018 push eax
00401019 mov ecx,dword ptr [ebp-4]
0040101B push ecx
0040101C call @ILT+0(Fun1) (00401005)
00401021 add esp,8
29: return 0;
Address: 0012FF80
0012FF80 C0 FF 12 00 29 13 40 00 01 00 00 00 D0 0F
0012FF8E 38 00 68 10 38 00 A6 F5 51 04 A0 F5 51 00
0012FF9C 00 E0 FD 7F 01 00 00 00 01 00 00 00 94 FF
0012FFAA 12 00 00 DD DE B2 E0 FF 12 00 00 38 40 00
0012FFB8 10 61 42 00 00 00 00 00 F0 FF 12 00 67 70
0012FFC6 01 7C A6 F5 51 04 A0 F5 51 00 00 E0 FD 7F
0012FFD4 ED C6 54 80 C8 FF 12 00 20 C0 8E 01 FF FF
0012FFE2 FF FF C0 9A 83 7C 70 78 01 7C 00 00 00 00
0012FFF0 00 00 00 00 00 00 00 00 40 12 40 00 00 00
0012FFFE 00 00 41 63 74 78 20 00 00 00 01 00 00 00
Name
Value
iTest4
CXX0017: Error: s
Watch1
Watch2
Watch3
Watch4
main() line 28
mainCRTStartup() line 206 + 25 bytes
KERNEL32! 7c817067()
Loaded 'ntdll.dll', no matching symbolic information found.
Loaded 'C:\WINDOWS\system32\kernel32.dll', no matching symbolic information found.
Build
Debug
Find in Files 1
Ready

执行完毕。