WinDbg 分析 DMP 文件方法完全攻略

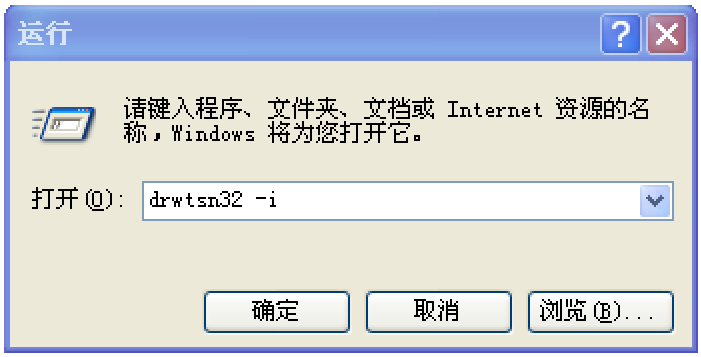
(2012-07-17 20:49:35)

前言：在 C++实际开发过程中，开发出来的程序，一般情况下由开发人员进行单元测试，然后移交给测试人员进行测试。在开发人员测试出现的 bug，我们可以直接在本地进行调试。如果测试人员测试出崩溃级别的 bug，如果我们需要调试往往借助于 vs 提供的 Remote Debugger 工具进行远程调试（关于 vs2010 远程调试的方法，请参考 http://blog.sina.com.cn/s/blog_a459dcf5010153o7.html),然是当程序在用户手中出现崩溃此时我们可以采用 Remote Debugger 进行调试，但是如果此时开发人员无法直接去用户现场调试，此时就需要用户生成 DMP 文件，以便开发人员使用 DMP 文件进行分析。

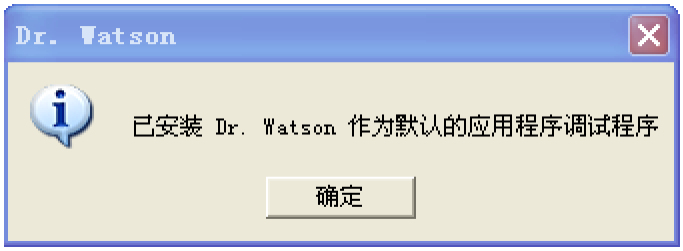
本文主要介绍 C++开发过程中出现程序崩溃后，如何进行分析定位 bug（基于 xp 系统）。

一、DMP 文件获取设置

（1）在运行窗口中输入 drwtsn32 -i ，并且点击确定

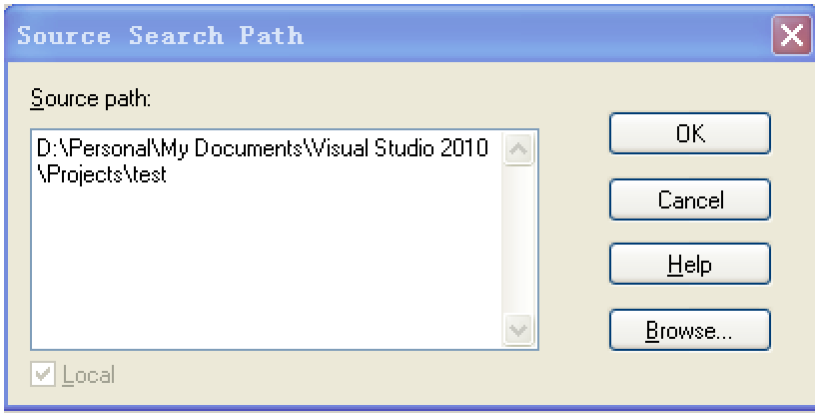


（2）在（1）确定后弹出如下对话框

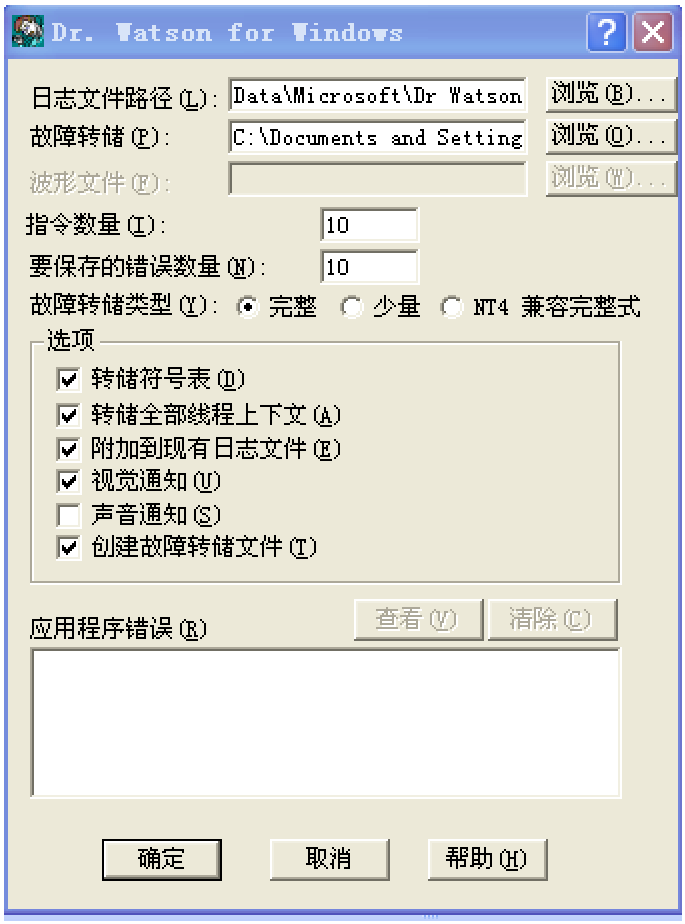


（3）在（2）弹出的确定框后点击确定按钮完成，将 Dr.Watson 设置为默认应用程序调试程序。Dr.Watson 系统自带的程序。

（4）再次在运行窗口中输入：drwtsn32，如下图：



（5）点击确定按钮，在弹出的对话框中按照下列方式设置

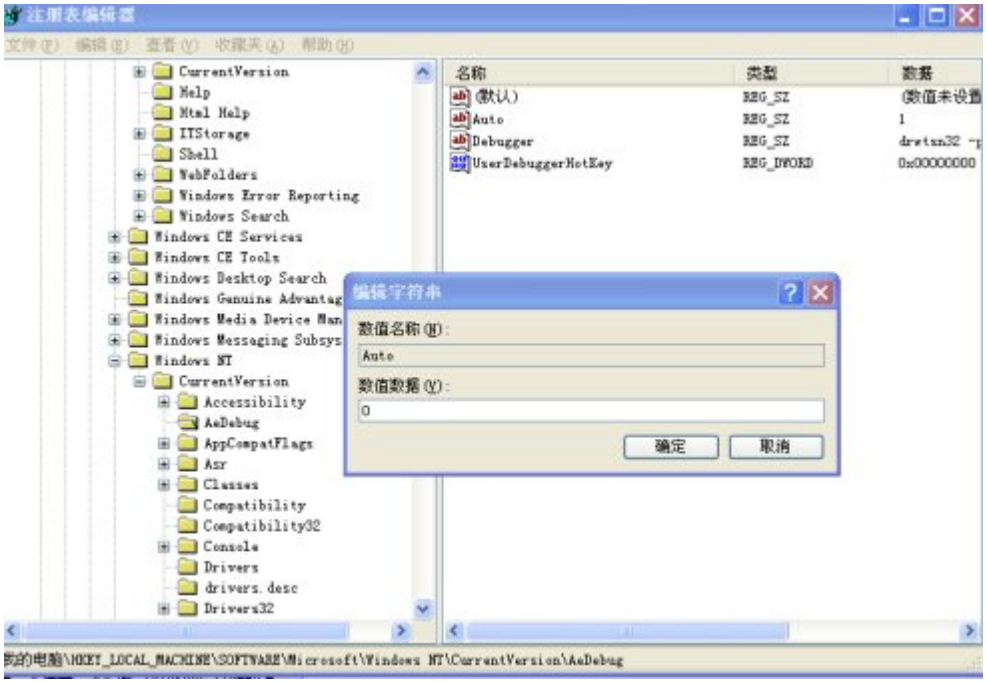


(6) 点击确定按钮完成 DMP 文件设置。

二、关闭 Dr.Watson 方法

（1）打开注册表

（2）在注册表中进入主键 [HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\WindowsNT\CurrentVersion\AeDebug]，然后将“AUTO”键值设置为 0 如下图：



三、Windbg 下载地址

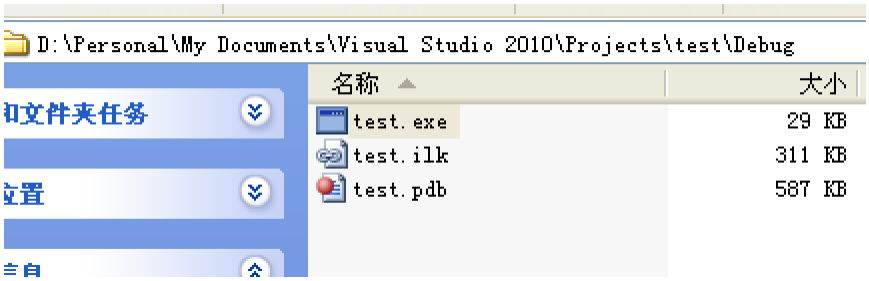
http://msdn.microsoft.com/en-us/windows/hardware/gg463009.aspx，下载完成后安装

四、DMP 文件获取

(1) 用 vs2010 创建一个基于 win32 的程序，其源码如下：

```
1  // test.cpp : Defines the entry point for the console application.
2  //
3
4  #include "stdafx.h"
5  #include <string>
6  #include <stdlib.h>
7
8  void Crash(void)
9  {
10     int i = 1;
11     int j = 0;
12     i /= j;
13 }
14
15
16 int _tmain(int argc, _TCHAR* argv[])
17 {
18     char buf[10];
19     memset(buf,0,10);
20
21     Crash();
22
23     strcpy(buf,"123456789123");
24     system("pause");
25
26     return 0;
27 }
```

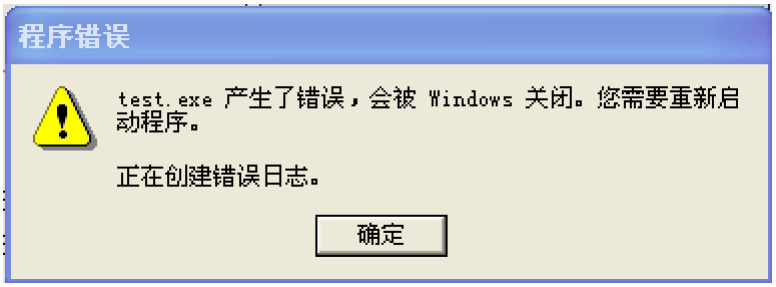
(2)我们知道在学习 C++中整数不能跟 0 进行除运算，否则会引起程序崩溃。而（1）中就是编写能触发 0 的异常，导致程序结束运行的程序。编译（1）中的程序，结果如下：



（3）运行（2）中 test.exe 程序 ，程序崩溃。如下图：

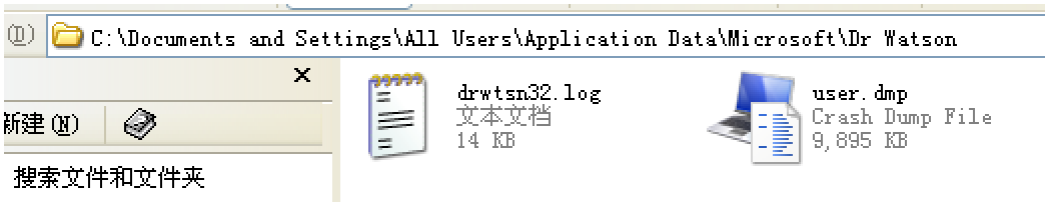
(4) 按照《一、DMP 文件获取设置》步骤实现 Dr.Watson 设置为默认应用程序调试程序。

(5)再次运行运行（2）中 test.exe 程序 如下图：



点击确定完成 dmp 文件的生成。

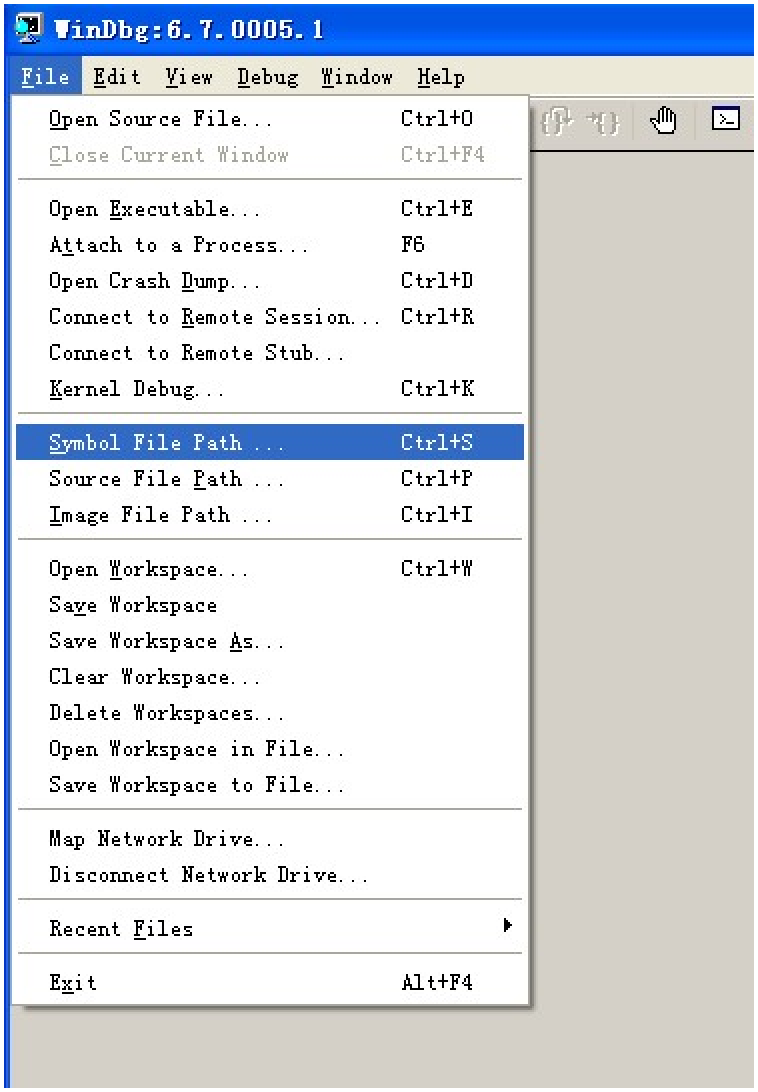
（6）打开在（4）中设置 dmp 文件路径。（本例中默认地址为：C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson）如下图：



其中 user.dmp 就是我们需要的 dmp 文件。

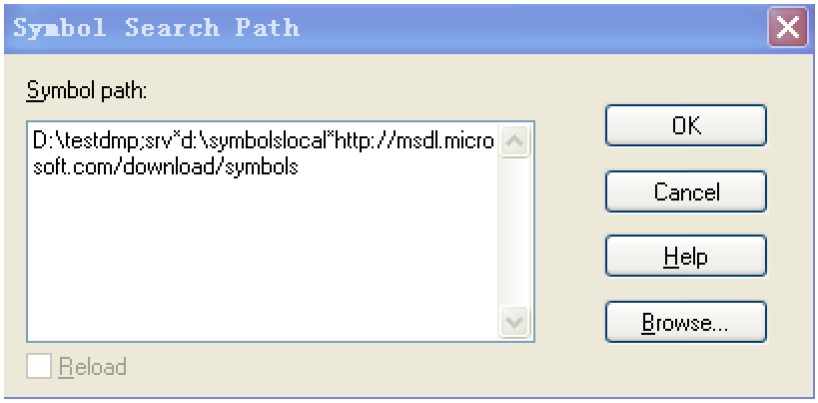
五、分析《四、DMP 文件获取》中获取的 DMP 文件

（1）符号表路径设置（参考下图）



(2)在弹出对话框中输入：

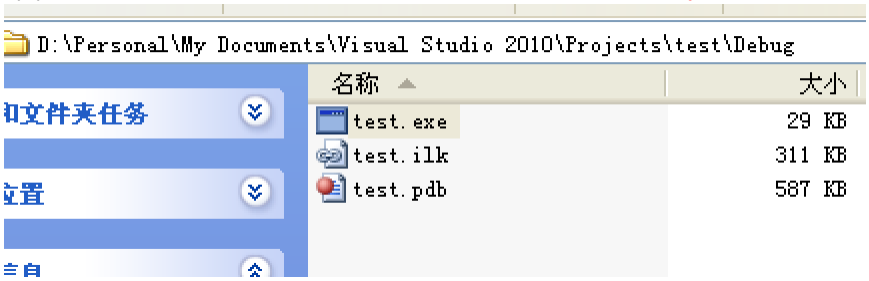
D:\testdmp;srv*d:\symbolslocal*http://msdl.microsoft.com/download/symbols 点击 ok 按钮



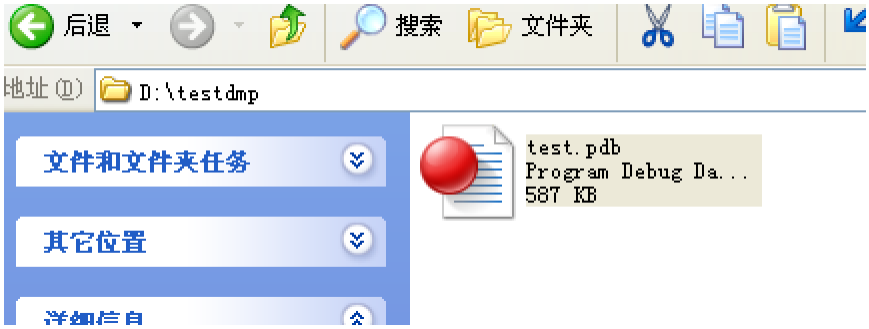
注意：D:\testdmp；这个是我们存放符号的文件夹，在进行此步骤前创建。

其中;srv*d:/symbolslocal*http://msdl.microsoft.com/download/symbols 设置的目的是下载该程序用到的操作系统相关的库函数的符号表到本地

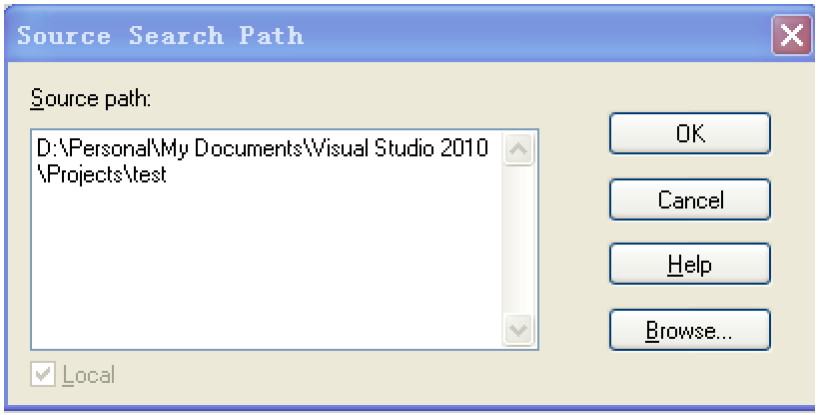
(3) 将前面《四、DMP 文件获取》中程序生成的符号 test.pdb（下图）拷贝到 D:\testdmp 中



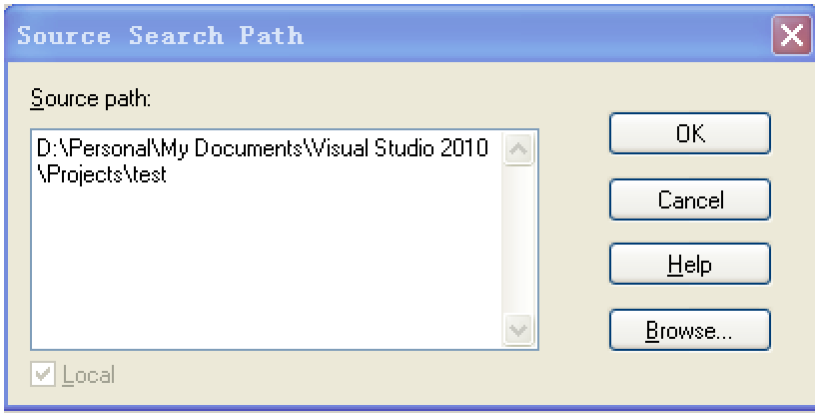
拷贝后结果如下



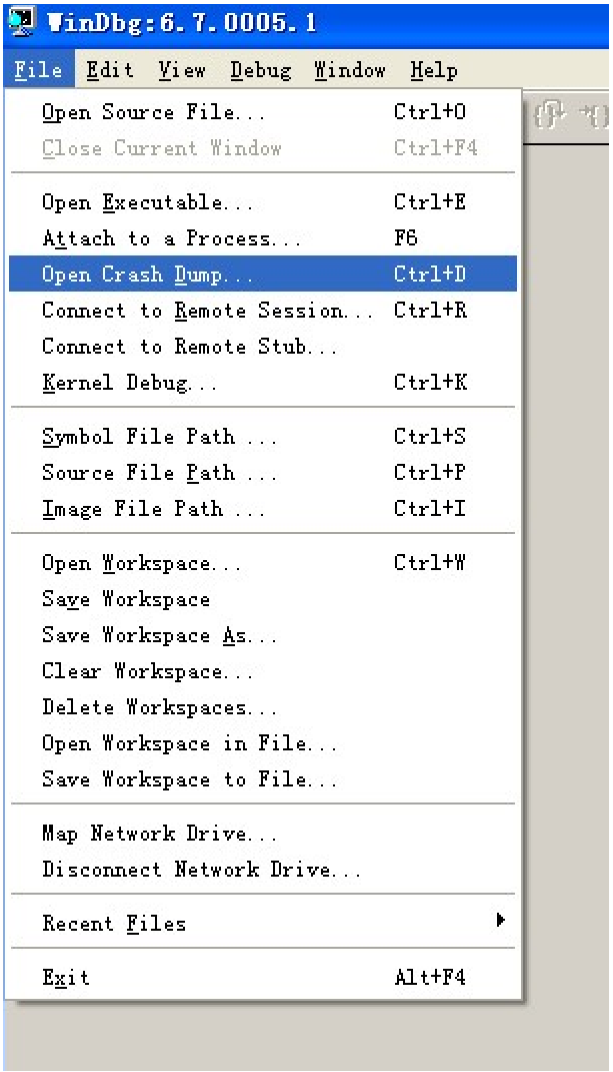
(4) 源代码路径设置（参考下图）

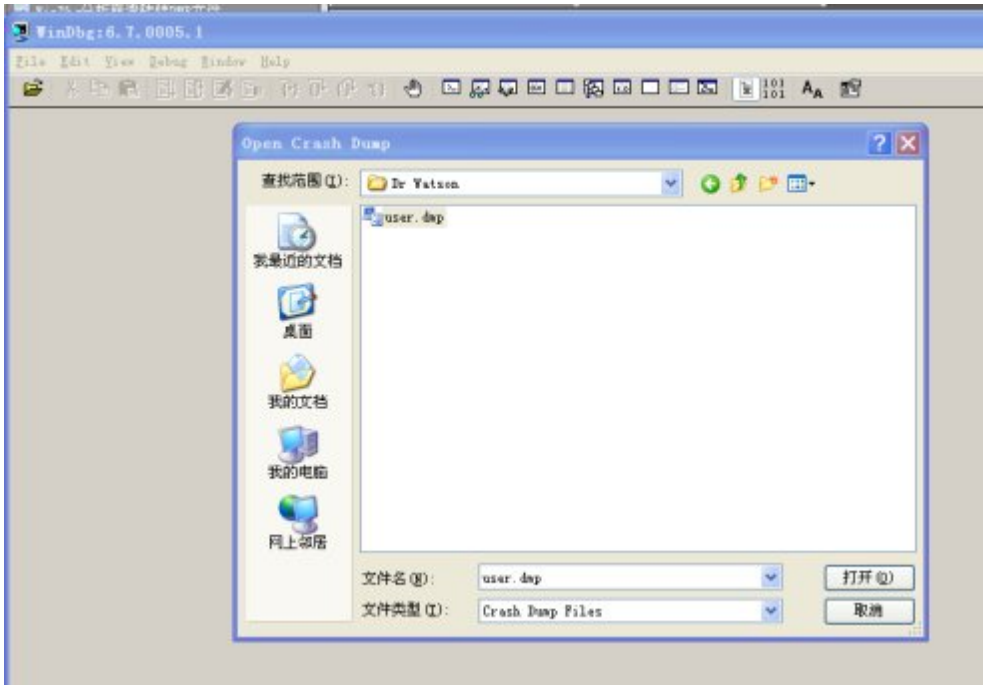


(5)在弹出对话框中输入：D:\Personal\My Documents\Visual Studio 2010\Projects\test 点击 ok 按钮



(6)DMP 文件导入（参考下图）





点击打开，完成 dmp 导入。导入后自动定位错误的行，并在 command 中给出崩溃的原因，如下如：