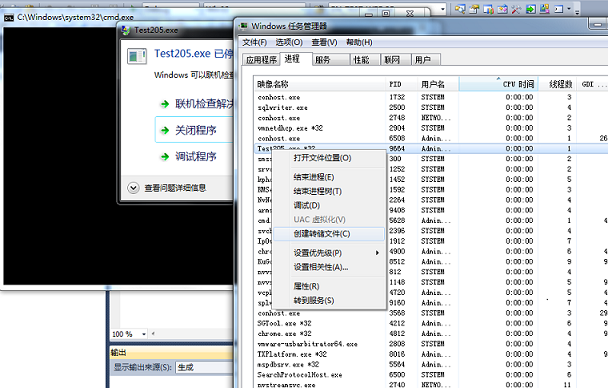
**Windows下dump文件生成与分析**

[news](http://www.taodudu.cc/news.html)2023/5/10 11:04:39

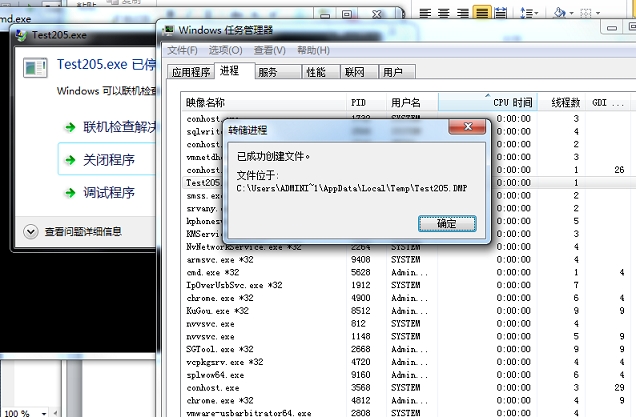
一、    生成Dump文件方式

1.1任务管理器

在程序崩溃后，先不关闭程序，在任务管理器中找到该程序对应的进程。右键—>创建转储文件。



此时会在默认的目录下创建出一个dump文件。

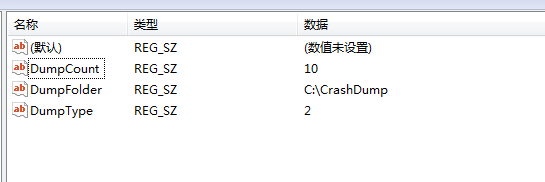


可以看出，此种方法只适用于程序崩溃但没有立即自行退出的情况。倘若程序故障后自行退出，则此方法就难以应用。不过，我们可以在注册表中添加如下信息已确保系统在程序崩溃后自行保存一个dump文件：

在注册表中找到

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\WindowsError Reporting\LocalDumps

添加项如下图：



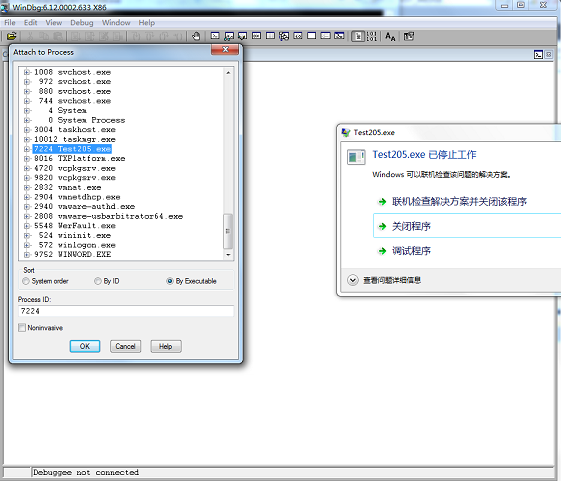
其中DumpType代表的含义是：

0 = Create a custom dump    
1 = Mini dump    
2 = Full dump

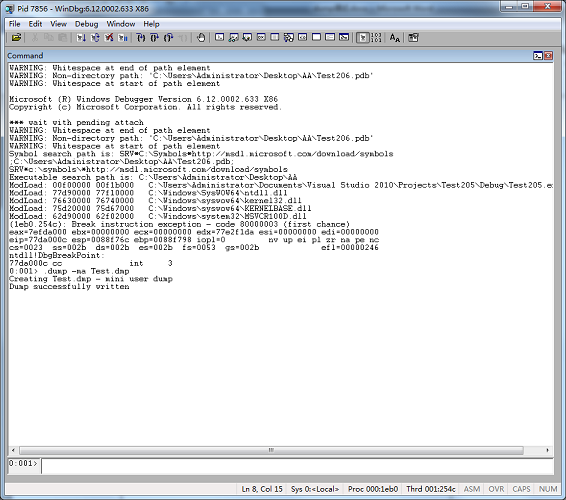
如此一来，一旦程序崩溃，系统会在C:\CrashDump下生成一个dump文件。

1.2WinDbg抓取

程序运行崩溃后，先不关闭程序，将WinDbg附加到改进程上。



执行命令：.dump –ma Test.dmp  ，则会产生一个Test.dmp的转储文件。



1.3程序中加入存储Dump的代码

通过SetUnhandledExceptionFilter设置捕获dump的入口，然后通过MiniDumpWriteDump生成dump文件。

如下程序在程序异常时会自行转储一个名为Test.dmp的dump文件。

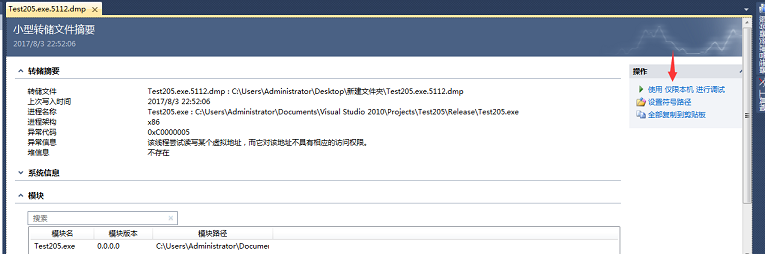
[cpp] view plain copy

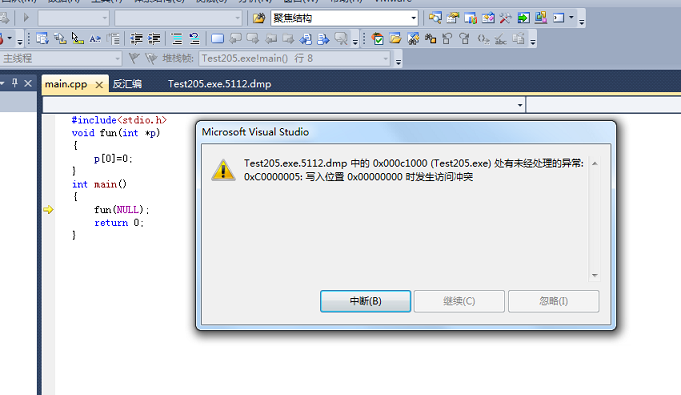
1. #include<Windows.h>
2. #include<DbgHelp.h>
3. #pragma comment(lib,"DbgHelp.lib")
4. // 创建Dump文件
5. void CreateDumpFile(LPCWSTR lpstrDumpFilePathName, EXCEPTION\_POINTERS \*pException)
6. {
7. HANDLE hDumpFile = CreateFile(lpstrDumpFilePathName, GENERIC\_WRITE, 0, NULL, CREATE\_ALWAYS, FILE\_ATTRIBUTE\_NORMAL, NULL);
8. // Dump信息
9. MINIDUMP\_EXCEPTION\_INFORMATION dumpInfo;
10. dumpInfo.ExceptionPointers = pException;
11. dumpInfo.ThreadId = GetCurrentThreadId();
12. dumpInfo.ClientPointers = TRUE;
13. // 写入Dump文件内容
14. MiniDumpWriteDump(GetCurrentProcess(), GetCurrentProcessId(), hDumpFile, MiniDumpNormal, &dumpInfo, NULL, NULL);
15. CloseHandle(hDumpFile);
16. }
17. // 处理Unhandled Exception的回调函数
18. LONG ApplicationCrashHandler(EXCEPTION\_POINTERS \*pException)
19. {
20. CreateDumpFile(L"Test.dmp",pException);
21. return EXCEPTION\_EXECUTE\_HANDLER;
22. }
24. void fun(int \*p)
25. {
26. p[0]=0;
27. }
28. int main(int argc, char \* argv[])
29. {
30. //注册异常处理函数
31. SetUnhandledExceptionFilter((LPTOP\_LEVEL\_EXCEPTION\_FILTER)ApplicationCrashHandler);
32. fun(NULL);
33. return 0;
35. }

二、调试Dump文件

2.1．VS调试

用VS打开dmp文件。测试时 dmp文件时本地产生的，因此VS会依据dmp文件自行找到exe，pdb和源代码的路径。因此直接点击调试，程序会出错代码行中断。

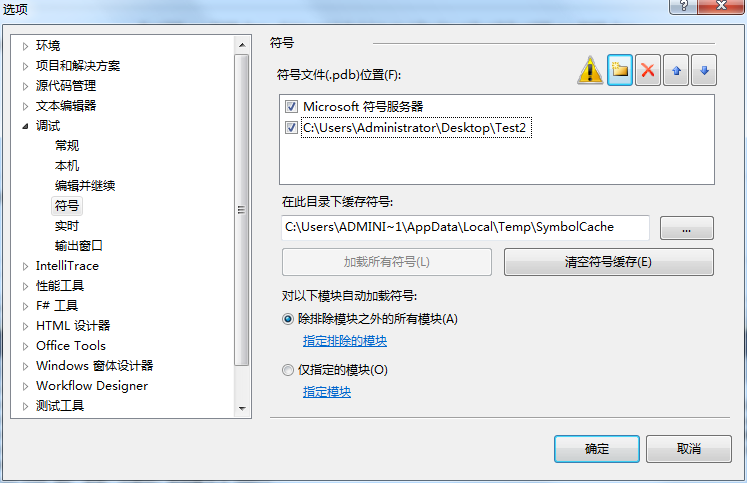




但若dmp文件是exe在另一台机器上产生的，则我们最好把exe,pdb,dmp放到同一文件夹下，必须保证pdb与出问题的exe是同一时间生成的，用VS打开dmp文件后还需要设置符号表文件路径和源代码路径：

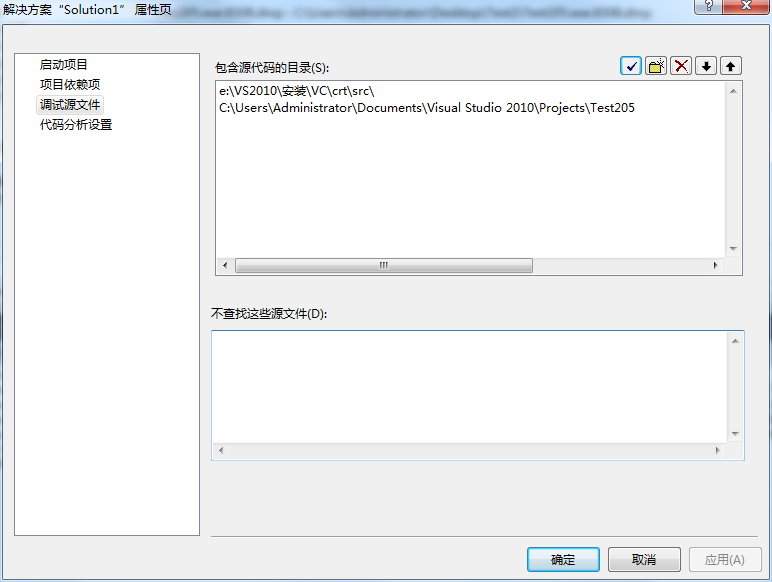
（1）  当把pdb文件与dmp文件放入同一目录下时，就不需设置其路径，否则需要设置

工具->选项->调试->符号：

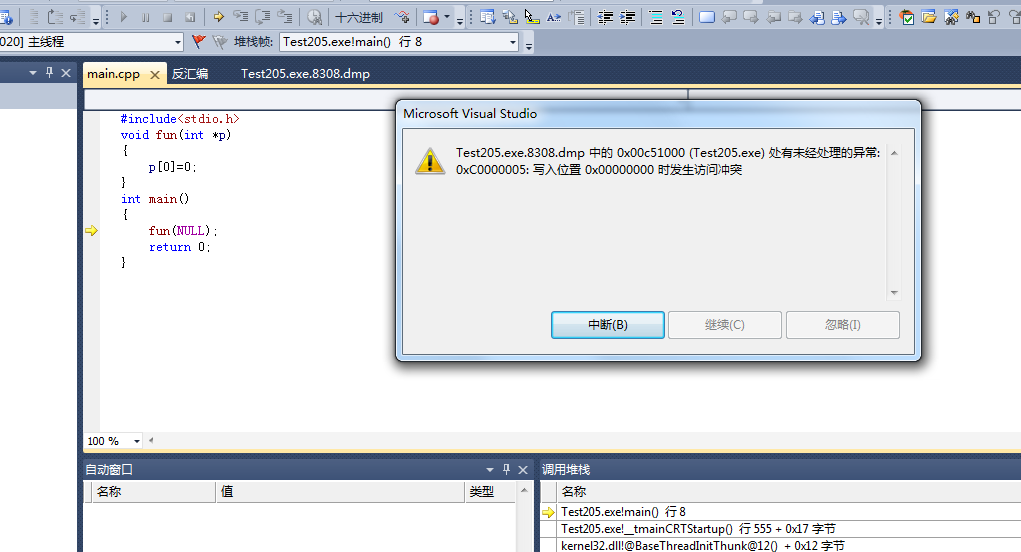


（2）还需设置源代码路径：

属性->调试源代码：

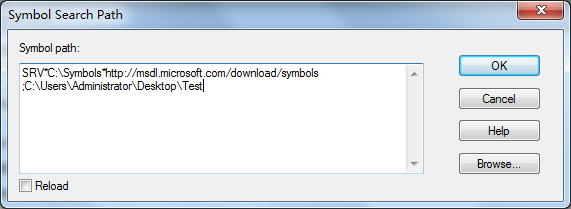


这样点击“使用仅限本机进行调试”，即可在出错代码行中断：

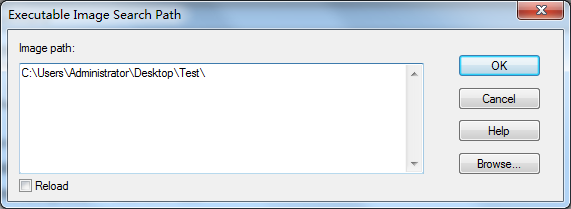


2.2 WinDbg调试

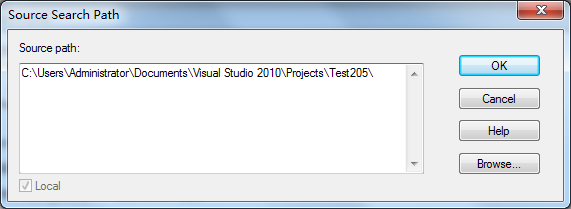
(1)设置pdb路径：File ->Symbol File Path



(2)设置exe路径：File -> Image File Path



(3)设置源代码路径：File -> Source File Path(指sln所在目录)



(4)打开dmp文件：File ->Open Crash Dump

(5)执行命令 !analyze –v





由分析结果可以看出，在main.cpp第7行出错，错误类型：NULL\_POINTER\_WRITE.

# 腾讯LiteAv TRTC 的 MFCDemo中的crashdump文件

可以参考下，挺好的

