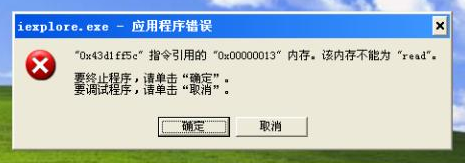
# Windbg抓取程序崩溃的dmp文件的方法

|  |  |  |
| --- | --- | --- |
| 日期 | 编写 |  |
| 2012/11/12 | 曾华伟 |  |

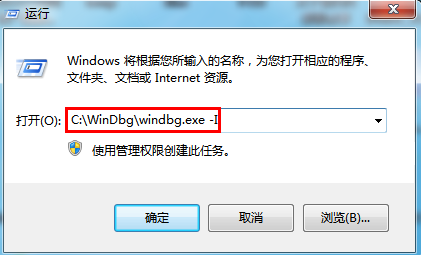
1. 简介

windbg是在windows平台下，强大的用户态和内核态调试工具。相比较于Visual Studio,它是一个轻量级的调试工具，所谓轻量级指的是它的安装文件大小较小，但是其调试功能，却比VS更为强大。它的另外一个用途是可以用来分析dump数据。

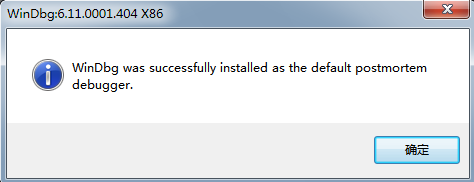
我们使用windbg的主要用途是来抓取IE崩溃产生的dmp文件，然后可以查看是哪个模块导致崩溃，从而协助开发判断分析问题所在。

1. 使用方法
2. **设置WinDbg抓取环境。**

WinDbg解压到任意盘符，例如C盘，使用下面的参数抓取Dump。C:\WinDbg\Windbg.exe –I



运行该参数时，WinDbg会弹出一个提示，点击确定后WinDbg界面会消失，如下图：  
此时就代表环境已经设置好，现在就需要你想方设法让程序崩溃，比如让IE崩溃。

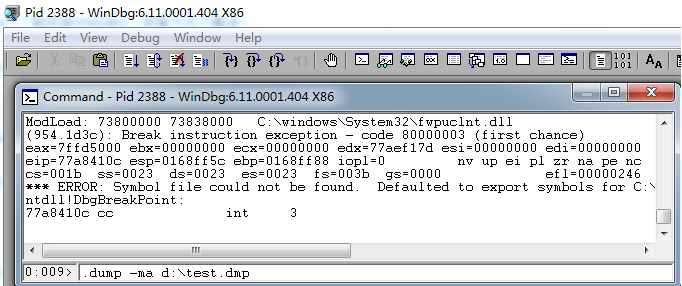


**WinDbg参数说明：**  
**-I：**将WinDbg作为默认的调试工具，注意I必须为大写，小写无效。

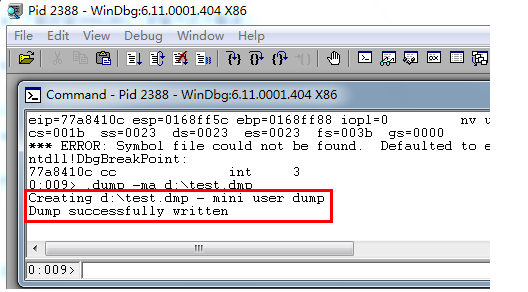
1. **收集Dump文件。**  
   在程序崩溃时，WinDbg窗口再次弹出来时，使用以下命令保存Dump文件。

.dump -ma d:\test.dmp

注意，带点, .



当开始保存Dump文件时，左下角的状态信息会变成**\*Busy\***，表示WinDbg正在工作，Dump保存完成后会出现“Dump successfully written”这个提示，如下图：



接下来就是等Dump保存好，然后把dump文件打包提供给开发即可。