dmp介绍

- dmp、pdb、exe确保是同一版本，即使代码未做任何修改，重新编译生成的新版exe不能与旧版exe产生的dmp文件一起调试
- dmp、pdb、exe最好放在同一目录下，方便设置vs设置符号文件（*.pdb）位置
- 尽量保证exe的源文件与上次发布exe的源文件一致

https://blog.csdn.net/hellokandy/article/details/107823320

winDbg调试DMP

WinDbg调试DMP格式文件
WinDbg可以用于Kernel模式调试和用户模式调试，还可以调试Dump文件。

打开WinDbg，通过菜单File - Open Crash dump 选择dump文件打开，也可通过CMD打开Dos命令窗口，切换到WinDbg所在目录，利用命令：

WinDbg –z “D:/Lines2009-7-25-22-20-33-900.dmp”

-z表示路径

分析dump文件
若生成的dump文件在本机，dump文件中将包含调试需要的PDB文件及源代码路径，若不在本机，可以通过WinDbg菜单File-Symbol File path 及 Source File Path 分别设置PDB文件路径和源代码路径。如果程序涉及到DLL，需要将EXE、DLL所有涉及的PDB、源代码路径都包括。使用命令：

!analyze –v

将分析dump文件，并显示程序崩溃处于的代码行

下载安装
https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/debugger-download-tools

https://developer.microsoft.com/zh-cn/windows/downloads/windows-sdk/
http://download.microsoft.com/download/A/6/A/A6AC035D-DA3F-4F0C-ADA4-37C8E5D34E3D/setup/WinSDKDebuggingTools_amd64/dbg_amd64.msi

WINDBG的安装、配置和功能

windbg介绍

用户成功安装微软Windows调试工具集后，能够在安装目录下发现四个调试器程序，分别是：cdb.exe、ntsd.exe、kd.exe和Windbg.exe。其中cdb.exe和ntsd.exe只能调试用户程序，Kd.exe主要用于内核调试，有时候也用于用户态调试，上述三者的一个共同特点是，都只有控制台界面，以命令行形式工作。

Windbg.exe在用户态、内核态下都能够发挥调试功能，尤其重要的是，它不再是命令行格式而是采用了可视化的用户界面。所以绝大部分情况下，我们在谈及Windows调试工具的时候，都直接指向

Windbg，而不大谈及前三者。

Windbg在用户态和内核态下，都支持两种调试模式，即“实时调试模式（Living）”和“事后调试模式（Postmortem）”。所谓实时模式，是被调试的目标对象（Target）当前正在运行当中，调试器可以实时分析、修改被调试目标的状态，如寄存器、内存、变量，调试exe可执行程序或~~双击~~双机实时调试都属于这种模式；所谓事后模式，是被调试的目标对象（Target）已经结束了，现在只是事后对它保留的快照进行分析，这个快照称为转储文件（Dump文件）。Windbg另一个重大优点，还在于它支持源码级的调试，就像VC自带的调试器一样。虽然提供了用户界面，但Windbg归根结底还是需要用户一个个地输入命令来指挥其行动。这就是他的Command窗口。每个调试命令都各有使用范围，有些命令只能用于内核调试，有些命令只能用于用户调试，有些命令只能用于活动调试。但用户也不必记得这许多，一旦在某个环境下，使用了不被支持的命令，都会显示“No export XXX found”的字样。

windbg的组要功能

功能	KD	NTSD	WinDbg	Visual Studio .NET
内核模式调试	Y	N	Y	N
用户模式调试		Y	Y	Y
非托管调试	Y	Y	Y	Y
托管调试		Y	Y	Y
远程调试	Y	Y	Y	Y
附加到进程	Y	Y	Y	Y
从进程分离	Y	Y	Y	Y
SQL调试	N	N	N	Y

内核调试方面

	WinDbg	**SoftICE**
原理	Windows 操作系统内置调试支持	Hook 中断，接管系统
系统和平台支持	x86、Itanium 和 x64 机器上的所有 NT 平台操作系统	x86，由于已停止更新，新版本操作系统中支持不佳，老系统中也常常遇到兼容性问题
符号和源码支持	完美支持符号调试和源码调试，可直接使用微软公共符号	支持符号调试和源码调试，但是需要先转换符号格式
远程调试	通过和远程工具、转发器的配合，实现各种灵活的远程调试方式，以支持不同的网络环境	通过 Virtual SoftICE 支持基于网络的远程调试
硬件需求	通过串口、1394、USB 2.0 接口的双机调试；通过 Pipe 连接的虚拟机调试；或者功能有诸多限制的本地内核调试	单机或者通过 Virtual SoftICE 的双机调试
用户界面	由于是双机调试，调试器只是主控机上运行的一个普通软件。拥有 GUI 界面，可以同时进行其他应用。	单机调试时完全接管系统，字符界面，操作不是很方便。
扩展性	支持脚本和插件，并且软件包本身提供了大量非常有用的插件	支持插件

用户调试方面

	Windows 调试工具包	OllyDbg	Visual Studio 调试器
原理	Windows 的用户程序调试支持	Windows的用户程序调试支持	Windows 的用户程序调试支持
系统和平台支持	主要基于 NT 系统，9x 内核下支持不佳并且需要安装附加模块	主要支持 NT 系统，9x 下也可以使用	新版本的 VisualStudio 不支持在 9x 系统下安装。VC6 之前可以在 9x 下调试
符号和源码支持	完美支持符号调试和源码调试，可直接使用微软公共符号	支持符号调试和源码调试	支持。VS2008 开始可以直接使用微软公共符号
远程调试	通过和远程工具、转发器的配合，实现各种灵活的远程调试方式，以支持不同的网络环境	不支持	较新版本 Visual Studio 中支持
无源码调试	反汇编分析能力较弱，GUI 界面偏弱，无源码时调试比较困难	强大的代码分析能力，无符号和源码时也能很好的进行调试	无源码调试的支持很弱，使用不便
用户界面	GUI 界面不是很丰富，大量操作需要通过命令	GUI 界面强大，能够实现大多数调试操作	介于 WinDbg 和 OllyDbg 之间。
扩展性	支持脚本和插件，并且软件包本身提供了大量非常有用的插件	支持脚本和插件，有大量可用的资源	支持插件扩展
Dump 文件调试	支持，分析功能强大	不支持	支持，但是不够强大
.NET 调试	通过 SOS.dll 支持，进行高级调试比较方便	不能直接支持	功能强大易用，绝大多数情况下都能解决问题

虽说WinDbg在无源码调试方面确实比较困难，但在调试内核方面却真的有独到之处

使用VS调试Dump文件

https://blog.csdn.net/u011726005/article/details/78484650