pdb设置：

;srv\*D:\symbols\* http://msdl.microsoft.com/download/symbols

\\10.0.1.150\PCClient\Builds\PC2012\V5Symbols

表示从D:\symbols这个目录去加载pdb，如果pdb不存在，则从<http://mdsl.microsoft.com/download/symbols>这个地址下载，加到D:\symbols，同时加载进调试器。

;表示后面还有一个符号信息

如何生成一个dump文件：

打开windbg，按F6 attach到目标进程，然后：

.dump /ma C:\dump\xxx.dmp

不要直接退出WINDBG，先detach再退出WINDBG，否则目标进程会被关闭。

dump不是崩溃的时候才能产生，而是随时可以产生。

!sym noisy 打开符号加载详细模式

!analyze –v 用于分析挂掉线程的详细情形，错误原因。

!cs xxxx 查看某个临界区里面的内容

~\* 打印出当前所有的线程

~\*kb 打印出所有线程的堆栈

~0s 切换到0号线程

!runaway 查看所有线程的用户态运行时间，后面加个 f，可以查看内核态运行时间

kv 显示当前线程的堆栈

kvn 显示当前线程的堆栈当显示每一行的序号

.frame x 关联显示第x行序号堆栈的代码

lm 列出所有加载的模块，同时会显示是否加载了pdb

lmf 列出所有模式的路径

.exr ?? 显示异常记录

!handle 显示一个handle的信息

.thread 切换current thread

!locks 检查有无死锁

d db dd 显示指定地址的内存

bp bc bd 下断点，清断点，禁断点

ba 下内存断点

dv 查看某个变量的值

dt 查看某个变量的结构，如 dt this

sxe 0x... 设置异常通知，但发生该异常（first chance）会中断

为什么analyze –v 能看到堆栈，但kv却看不到堆栈？

这是因为原线程已经走过去了，windbg是将堆栈转储到别的地方，在analyze的堆栈下面会显示这么一句话：

STACK\_COMMAND: ~9s; .ecxr ; kb

这个时候要运行一下.ecxr命令就能正常显示了。这条命令要求调试器把当前的内容切换到保存在故障转储里的异常信息。我们执行这条命令后，将能访问异常抛出时调用栈和局部变量的值。