以notepad.exe为例进行调试

1. windbg加载notepad.exe
2. ctrl+s设置符号目录为以下值，用来设置pdb目录
   1. c:\mysymbols;cache\*c:\symbolcache;\\server\symbols;SRV\*c:\symbols\*http://msdl.microsoft.com/download/symbols
3. 输入.reload重新加载
4. 输入lmm notepad查看notepad被加载的进程地址
5. 使用dumpbin /headers notepad 查看notepad的OEP、RVA
6. 将进程起始地址加上RVA得出程序入口点，使用u addr查看反汇编代码
7. 使用bu notepad!winmain在winmain函数下断
8. 使用bl 查看断点列表
9. 使用g 使程序跑起来
10. 当程序断下来后，使用lm 查看程序加载的模块
11. 使用x notepad!\* 查看notepad的全部符号
12. 使用x notepad!\*main\* 查看notepad中包含main的符号
13. 使用dds addr L4查看符号表中的地址(符号也会被显示，L4表示显示前4条)
14. 使用k 查看调用堆栈
15. 使用~ 查看线程列表
16. 使用~0s 查看0号线程的调用栈
17. 使用qd 停止调试并使调试器与被调试程序分离

对有源码的c++程序进行调试，这里以手写的cppfordebug程序进行调试

1. windbg加载cppfordebug.exe
2. 输入以下命令，用来设置符号文件位置及源码位置
   1. **.sympath+ C:\MyApp\x64\Debug**
   2. [**.srcpath C:\MyApp\MyApp**](http://go.microsoft.com/fwlink/p?linkid=399395)
3. 输入.reload 重新加载程序
4. 输入bu cppfordebug!main 下断
5. 输入g 让程序跑起来
6. 程序断下后，源码窗口会显示来出，并在相应代码行处断下