

当配置好开发环境后，就要配置测试环境了。不瞒大家说，写这章的心里压力最大，如果后面的章节没写好，大家也就是一个知识点没学会，如果这章没写好，大家肯定要骂我了。因为这章的内容是讲解如何在 WIN64 系统上玩驱动，如果没搞好，就彻底没法玩了。

废话不多说，先说今天的各个主角：

1. VMWARE。VMWARE 是虚拟机软件，相信这个大家都知道，因为版权的关系，我不能把它的下载地址和注册码等信息放在文章里，这个可以大家去各种知名软件站点搜索。建议下载 VMWARE 9.0（虽然最近已经出到了 10.0）。

2. WINDBG。WINDBG 是微软出品的调试器，比起 OD 等常用调试器，就是支持内核调试。它的下载地址是：http://www.windbg.org/X64%20Debuggers%20And%20Tools-x64_en-us.msi（不过其实大家不用下载，因为安装 WDK 时已经自带了）。

3. VirtualKD。方便与进行虚拟机双机调试的工具，免去手动设置的麻烦。下载地址：<http://virtualkd.sysprogs.org>

接下来分别说『安装虚拟机』、『进行双机内核调试』和『进行本地内核调试』的步骤。请大家一步一步进行操作，顺序绝对不能弄乱，否则必定失败。

『安装虚拟机』的步骤：

1. 安装 VMWARE。
2. 安装 WIN7X64 虚拟机（当然你也可以把其他 WIN64 系统都安装好）。
3. 在虚拟机里关闭 UAC（方便测试驱动！这一步一定要做，否则后续步骤会失败）。
4. 在虚拟机里安装 VMware Tools。
5. 在虚拟机里安装 [.NET FRAMEWORK4](#)（如果是 WIN7X64 以后的系统则跳过这步）。
6. 备份虚拟机的当前状态。

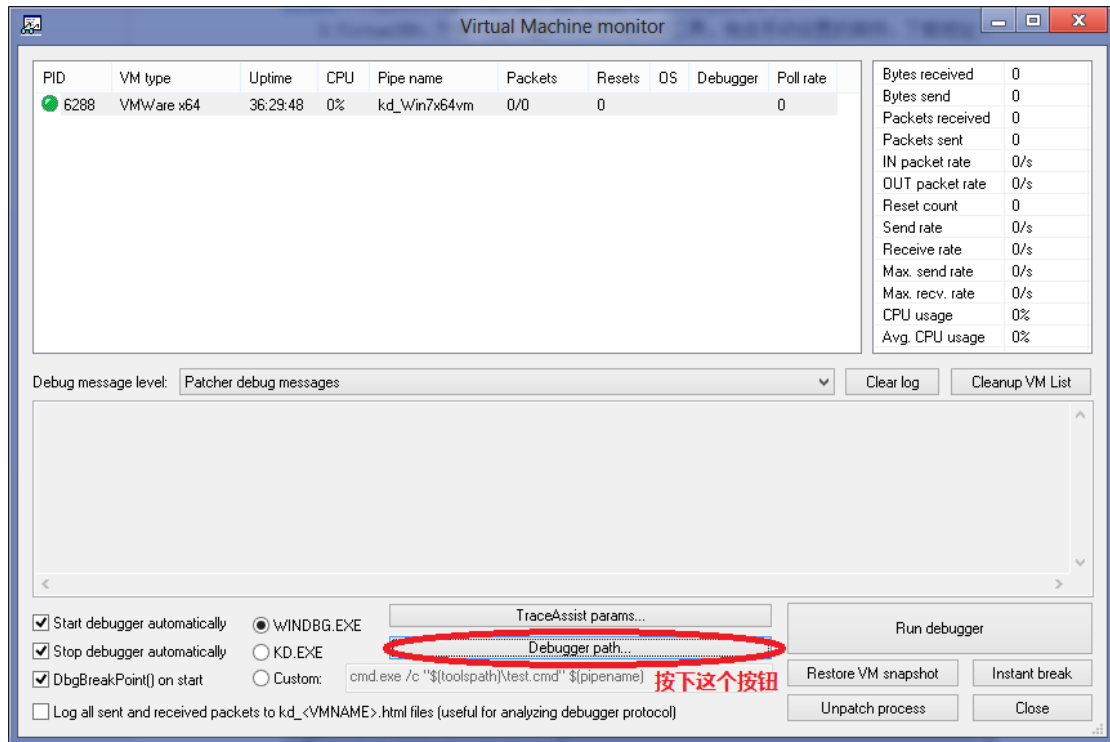
如果不了解虚拟机的使用，请自行百度，讲解虚拟机的使用方法不是课程重点。

『进行双机内核调试』的步骤：

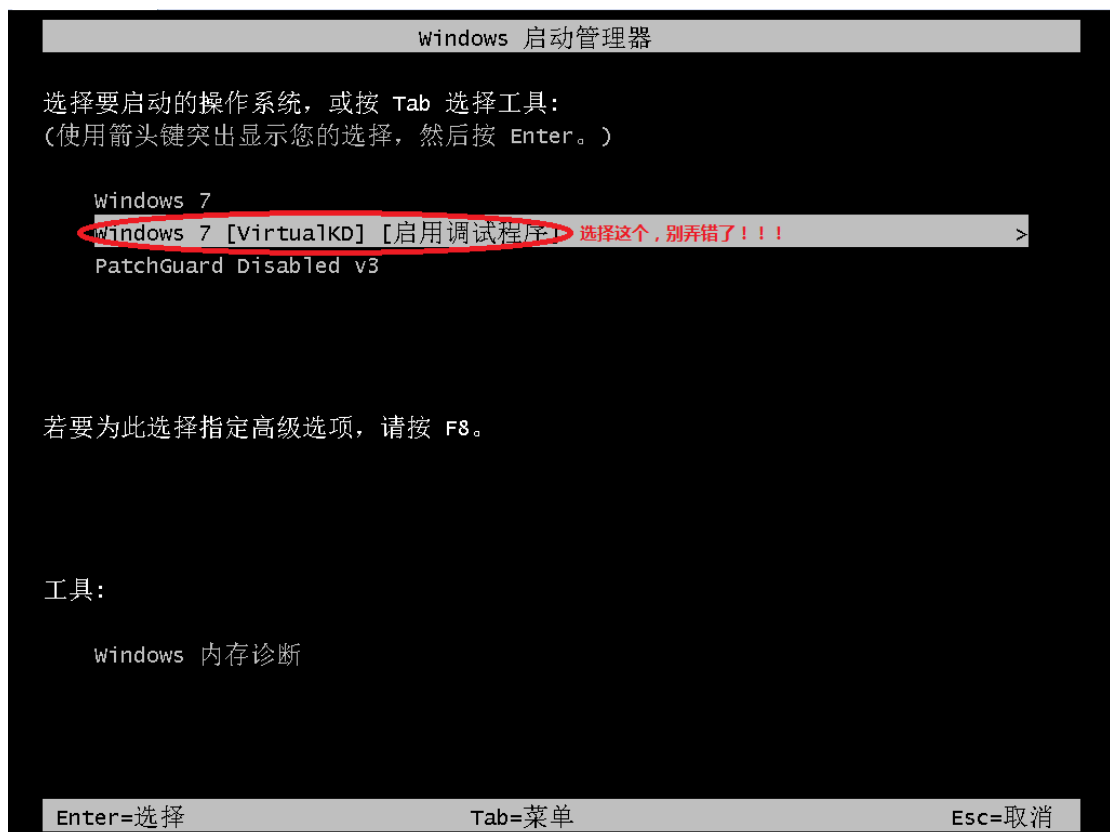
1. 把 VirtualKD 的 target 文件夹弄进虚拟机里。
2. 在虚拟机里安装 VirtualKD（打开 VirtualKD 目录下的 target 文件夹，以管理员权限运行 vminstall.exe）。【见下图】



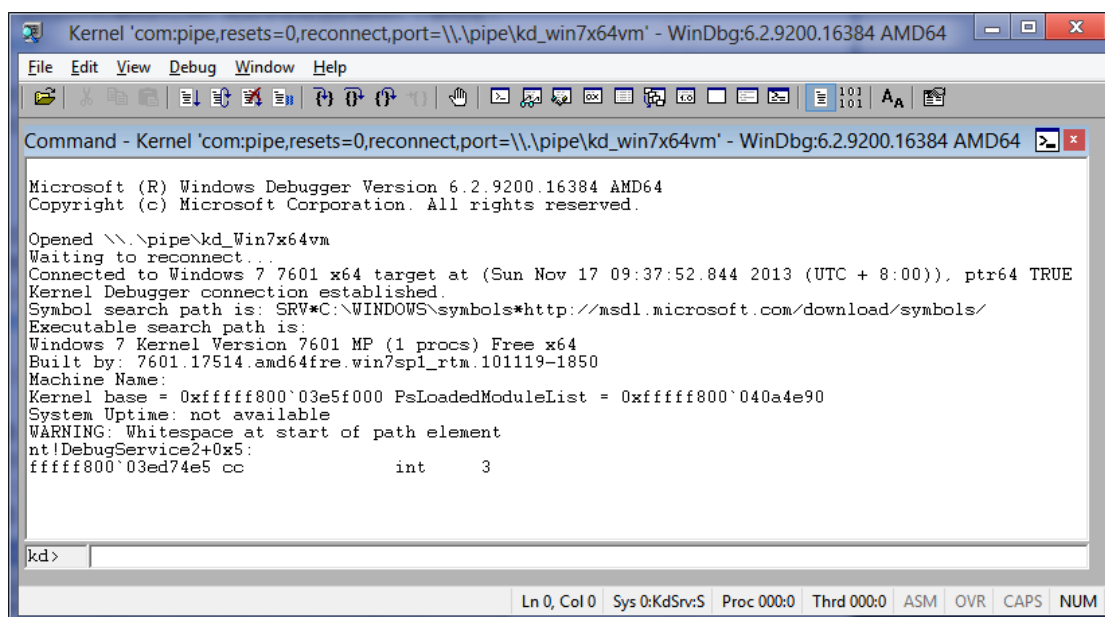
3. 在真机运行 VMMON64.exe，设置调试器路径。点击 VMMON 界面下面的『Debugger path』按钮，选择 WINDBG 路径。一般路径是：C:\WinDDK\7600.16385.1\Debuggers\windbg.exe。【见下图】



4. 重启虚拟机，进入这个内核启动项。【见下图】



5. 进入不久之后，WINDBG 会自动启动（实际上是 VMMON.EXE 启动的），出现类似这样的画面（见下图）。按下 F5，继续让系统运行。



```

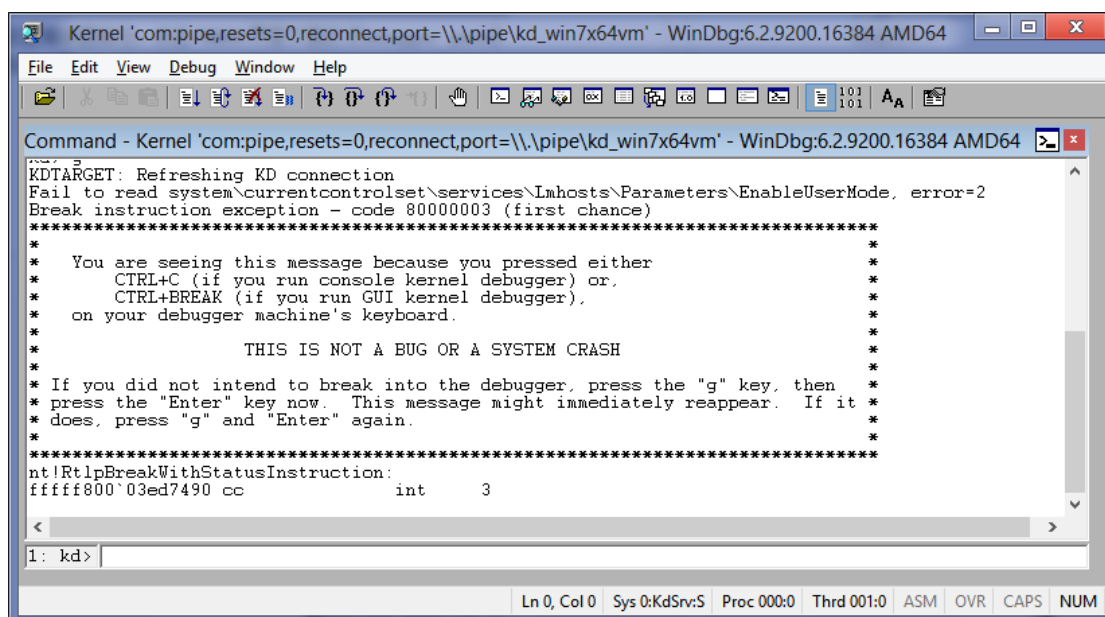
Kernel 'com:pipe,reset=0,reconnect,port=\\.\pipe\kd_win7x64vm' - WinDbg:6.2.9200.16384 AMD64
File Edit View Debug Window Help
Command - Kernel 'com:pipe,reset=0,reconnect,port=\\.\pipe\kd_win7x64vm' - WinDbg:6.2.9200.16384 AMD64
Microsoft (R) Windows Debugger Version 6.2.9200.16384 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.

Opened \\.\pipe\kd_Win7x64vm
Waiting to reconnect...
Connected to Windows 7 7601 x64 target at (Sun Nov 17 09:37:52.844 2013 (UTC + 8:00)), ptr64 TRUE
Kernel Debugger connection established.
Symbol search path is: SRV*C:\WINDOWS\symbols*http://msdl.microsoft.com/download/symbols/
Executable search path is:
Windows 7 Kernel Version 7601 MP (1 procs) Free x64
Built by: 7601.17514.amd64fre.win7spl_rtm.101119-1850
Machine Name:
Kernel base = 0xfffff800`03e5f000 PsLoadedModuleList = 0xfffff800`040a4e90
System Uptime: not available
WARNING: Whitespace at start of path element
nt!DebugService2+0x5:
fffff800`03ed74e5 cc          int     3

kd>
Ln 0, Col 0 Sys 0:KdSrv:S Proc 000:0 Thrd 000:0 ASM OVR CAPS NUM

```

6. 当虚拟机进入系统后，在真机 WINDBG 获得焦点的时候，按下 Ctrl+Break，记得随时调试虚拟机。按下 Ctrl+Break 后，会出现类似的画面：



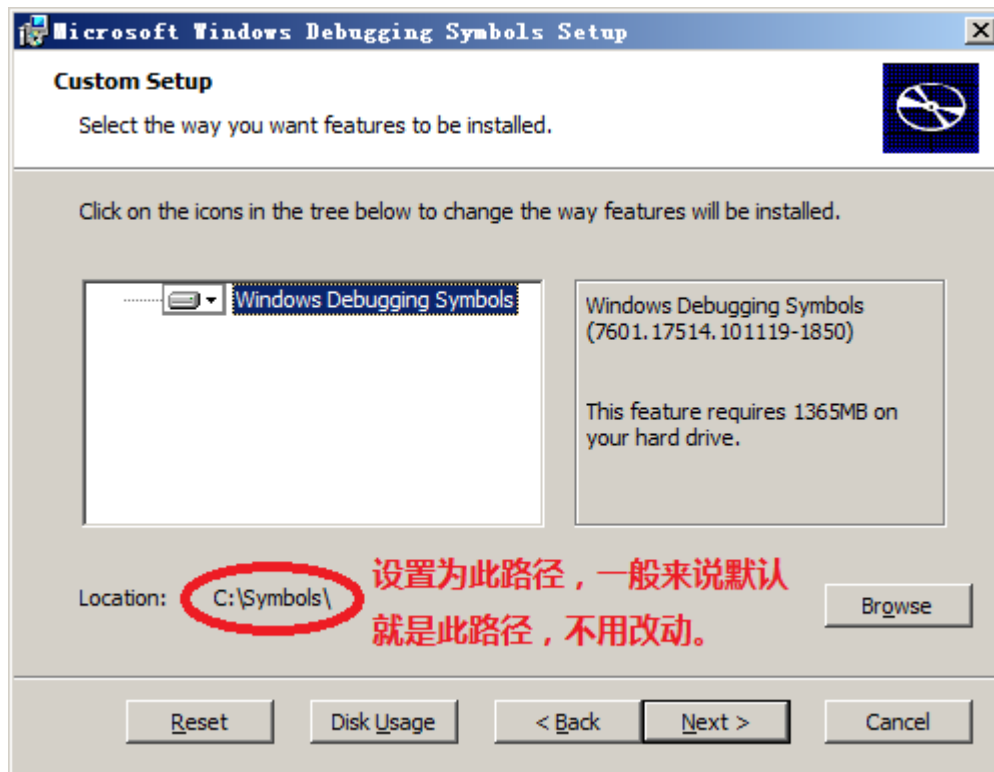
```

Kernel 'com:pipe,reset=0,reconnect,port=\\.\pipe\kd_win7x64vm' - WinDbg:6.2.9200.16384 AMD64
File Edit View Debug Window Help
Command - Kernel 'com:pipe,reset=0,reconnect,port=\\.\pipe\kd_win7x64vm' - WinDbg:6.2.9200.16384 AMD64
KDTARGET: Refreshing KD connection
Fail to read system\currentcontrolset\services\Inhosts\Parameters\EnableUserMode, error=2
Break instruction exception - code 80000003 (first chance)
*****
* You are seeing this message because you pressed either *
* CTRL+C (if you run console kernel debugger) or, *
* CTRL+BREAK (if you run GUI kernel debugger), *
* on your debugger machine's keyboard. *
* *
* THIS IS NOT A BUG OR A SYSTEM CRASH *
* *
* If you did not intend to break into the debugger, press the "g" key, then *
* press the "Enter" key now. This message might immediately reappear. If it *
* does, press "g" and "Enter" again. *
* *
*****
nt!RtlpBreakWithStatusInstruction:
fffff800`03ed7490 cc          int     3

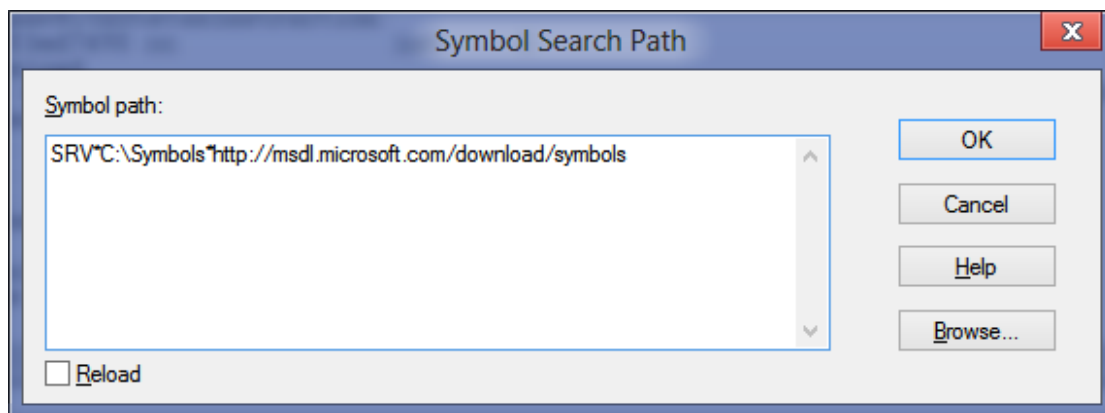
1: kd>
Ln 0, Col 0 Sys 0:KdSrv:S Proc 000:0 Thrd 001:0 ASM OVR CAPS NUM

```

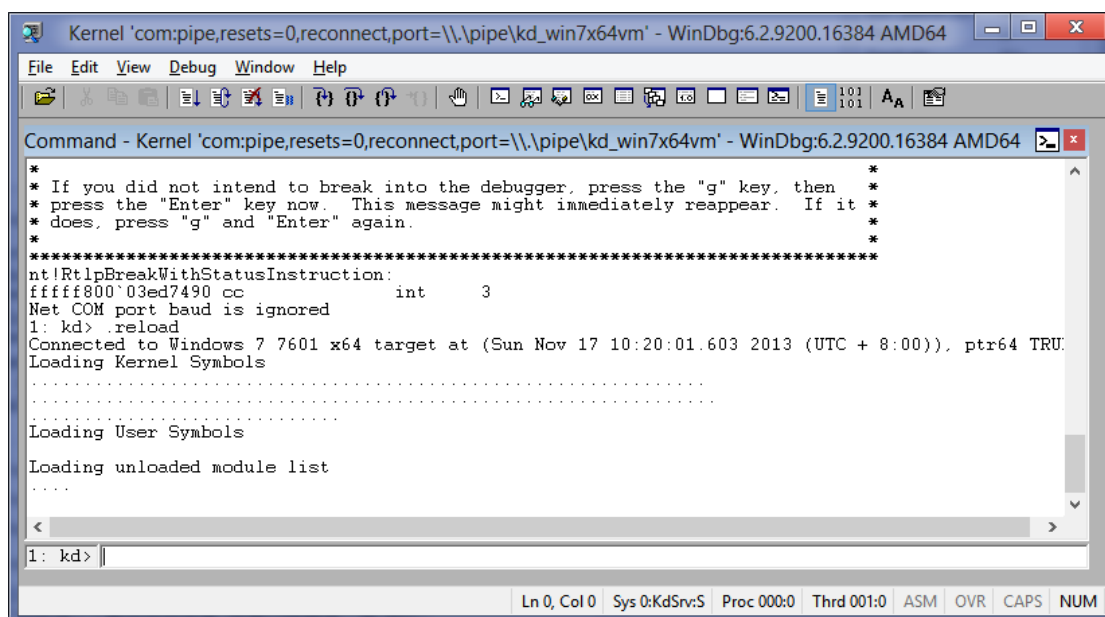
7. 这个时候先不急着调试，先在真机安装符号包。WINDOWS 系统符号的官方下载地址是：<http://msdn.microsoft.com/en-us/windows/hardware/gg463028.aspx>，因为我们要调试的目标系统是 WIN7X64，所以去页面上选择『Windows 7 RTM x64 retail symbols, all languages』或『Windows 7 Service Pack 1 x64 retail symbols, all languages』下载（根据你安装了 WIN7X64SP1 还是 WIN7X64RTM）。下载完毕后安装。安装过程就是一路 NEXT，记得在安装过程中选择把符号安装到 c:\symbols，否则会影响后面的符号加载！



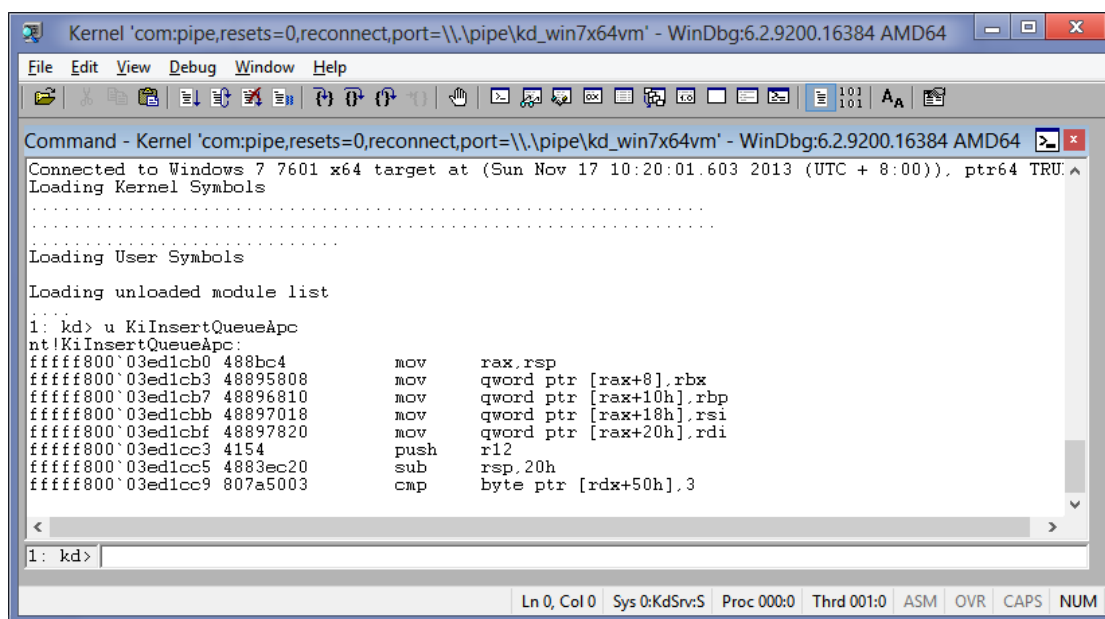
8. 设置 WINDBG 的符号。点击 File->Symbol File Path，输入【SRV*C:\Symbols*http://msdl.microsoft.com/download/symbols】，再按下确定即可。若在按下确定前，勾选一下 Reload 复选框，WINDBG 则会自动重载符号。



9. 让 WINDBG 重载符号。在 WINDBG 的命令行上输入 .reload 即可(注意 reload 前面有个点)。



10. 测试 WINDBG 是否加载符号成功。输入 `u KiInsertQueueApc`，如果出现类似以下的结果，就证明今天的课程学完了！如果没有，请上论坛提问或反馈问题。

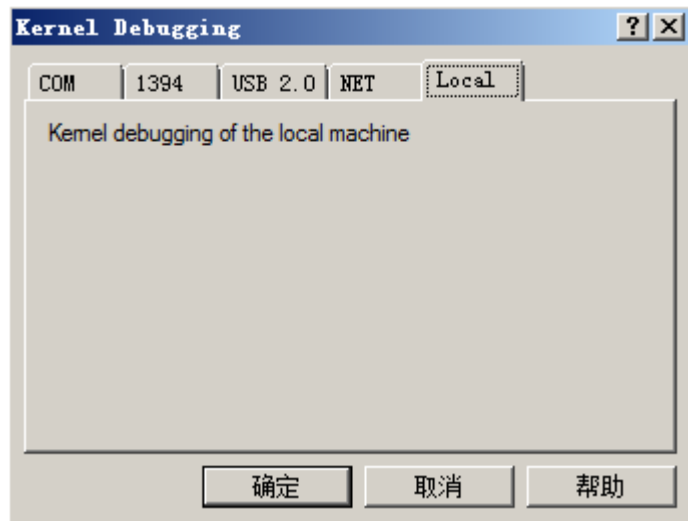


『进行本地内核调试』的步骤：

1. 开启 CMD，输入 `bcdedit -debug on`。



2. 重启计算机。
3. 打开 WINDBG，按下 Ctrl+K，选择 Local，按下确定。



4. 设置调试符号路径（参照前面的方法）。