使用WinDbg和虚拟机调试Windows驱动程序

作者：hustwing　　hustwing@126.com　MSN：hustwing@hotmail.com

本文范围和说明：

本文只讲解具体的操作过程，不涉及详细的原理，若要深入了解，请参阅Debugging Help(Debugging Tools For Windows)；

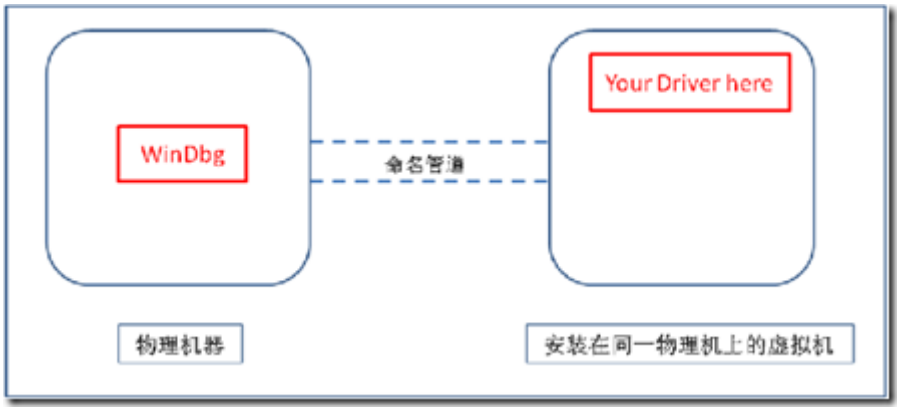
文中使用Virtual PC 2007作为虚拟机，但对于Virtual PC的其他版本或者VMWare都适用(VMWare设置命名管道的方式有点小不同)。

WinDbg更新很快，几乎月月有更新，下面是微软网站的下载链接：

http://www.microsoft.com/whdc/DevTools/Debugging/default.mspx

正文：

在开发驱动程序时，调试是一件很头痛的事情，如果你在自己机器的操作系统上安装你要调试的驱动程序的话，可能一不小心就是一个Bug Check（蓝屏），这个时候，你可能要进安全模式，卸载你的驱动程序，甚至有可能你需要重新安装操作系统。解决驱动程序的调试，一个比较好的方案就是在你的物理机器上装上一个虚拟机，在虚拟机上安装你要调试的驱动程序，然后使用WinDbg在你的物理机器上调试你虚拟机上的驱动程序。大致的示意图如下：



基本的步骤分为三步：

1. 安装过程：在你的机器上安装安装虚拟机和WinDbg软件；

2. 配置过程：对你的WinDbg和虚拟机软件做一些必要的配置；

3. 调试过程：给出一个最简单的调试启动过程，不涉及复杂的内核调试技术；

一、 安装过程

首先，你需要在你自己的机器上安装虚拟机，我安装的是Virtual PC 2007，然后需要在你的虚拟机上安装好操作系统，操作系统的版本取决于你要在哪一个操作系统上调试你的驱动程序。虚拟机以及虚拟机操作系统的安装过程网络上针对VirtualPC或者VMWare都有很详细的资料。

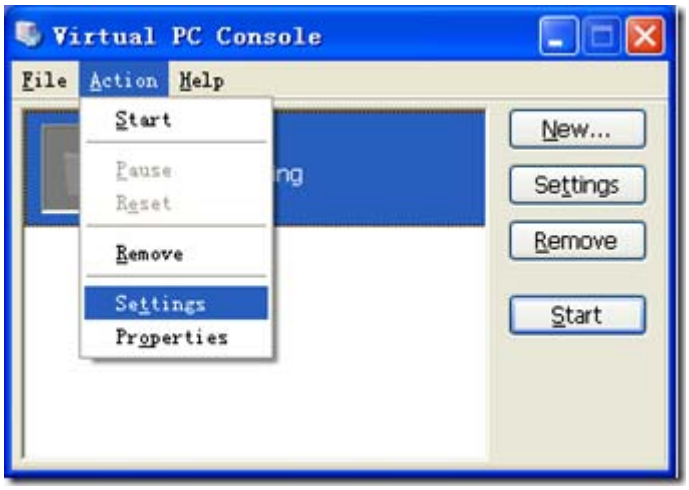
然后在你的物理机器上装上WinDbg，我用的是写本文时的最新版：6.8.0004.0，可以按我给出的链接在微软的网站上去下最新版，好像安装过程也不是很复杂，没有什么特别的配置，在此不再赘述。

二、 配置过程

安装好软件以后，剩下的就是配置了。首先你要对你的虚拟机作如下的配置：

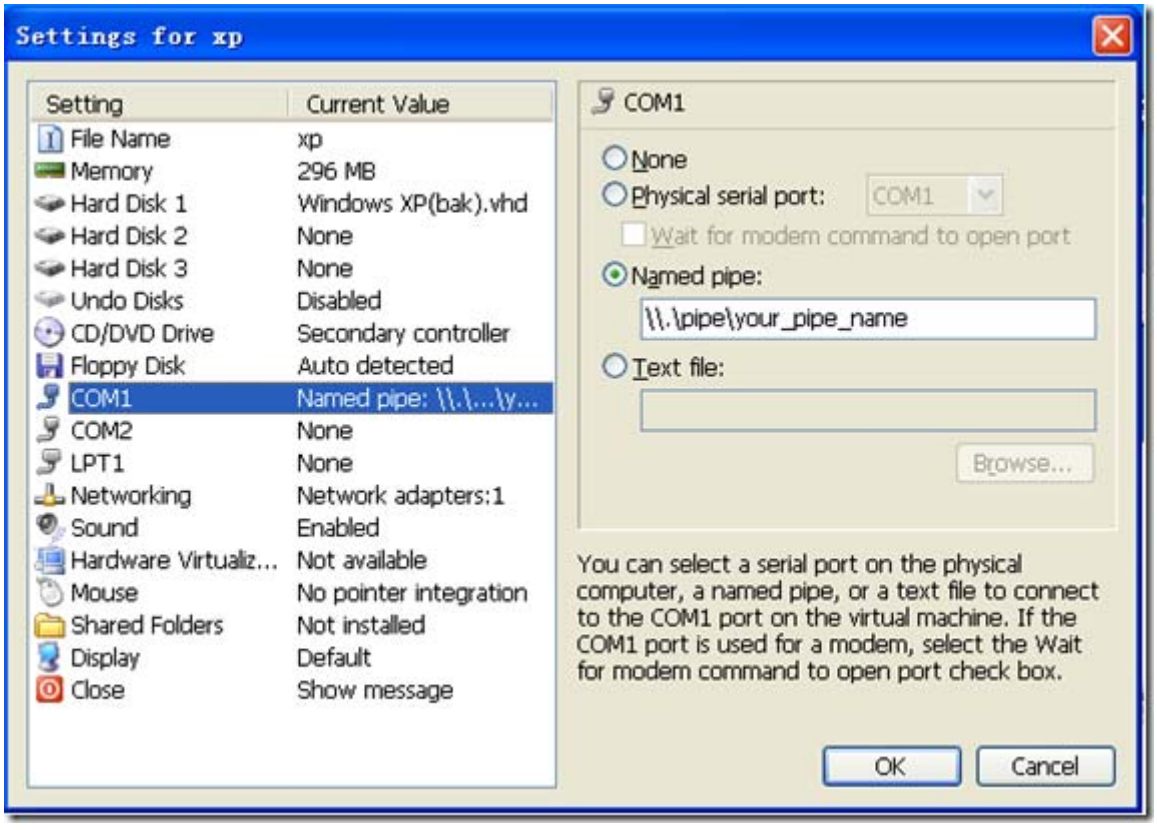
配置命名管道：你需要在你的虚拟机上建立命名管道，WinDbg通过此管道与你的虚拟机建立连接。给虚拟机配置命名管道的方法在虚拟机的帮助文档或网上很容易找到。以下给出Virtual PC 2007上建立命名管道的方法（so easy:)）

打开Virtual PC 2007，点击”Action”->”Settings”，进入虚拟机的设置页面：



在虚拟机的设置页面中，选择”COM1”或者”COM2”，在右边的属性项中点选”Named Pipe”，然后指定一个管道名称，注意命名管道的名称格式，当虚拟机的物理机和你的调试机器是同一台机器时，管道名称格式如下：

\\.\pipe\your_pipename_whatever

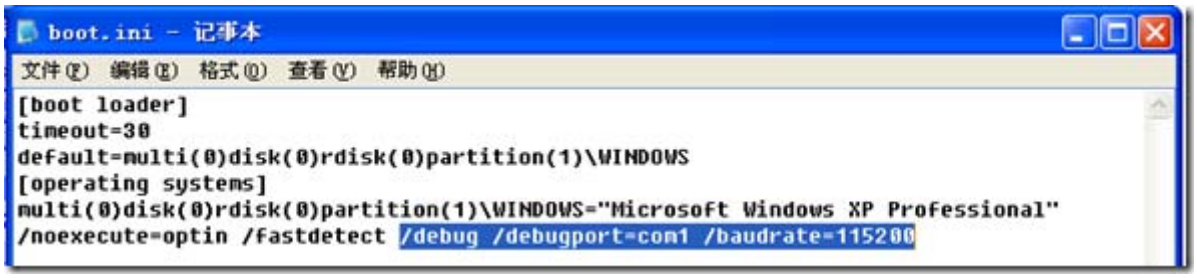


给虚拟机配置好命名管道以后，还需要给虚拟机配置启动模式，以调试模式启动：

找到"C:\boot.ini"（%SystemRoot%）文件（别告诉我你找不到啊，嘿嘿），将此文件的只读属性去掉（右击文件，选择” 属性”，去掉”只读”的选项）,用记事本和其他文本工具打开，加上如下启动选项：

/debug /debugport=com1 /baudrate=115200

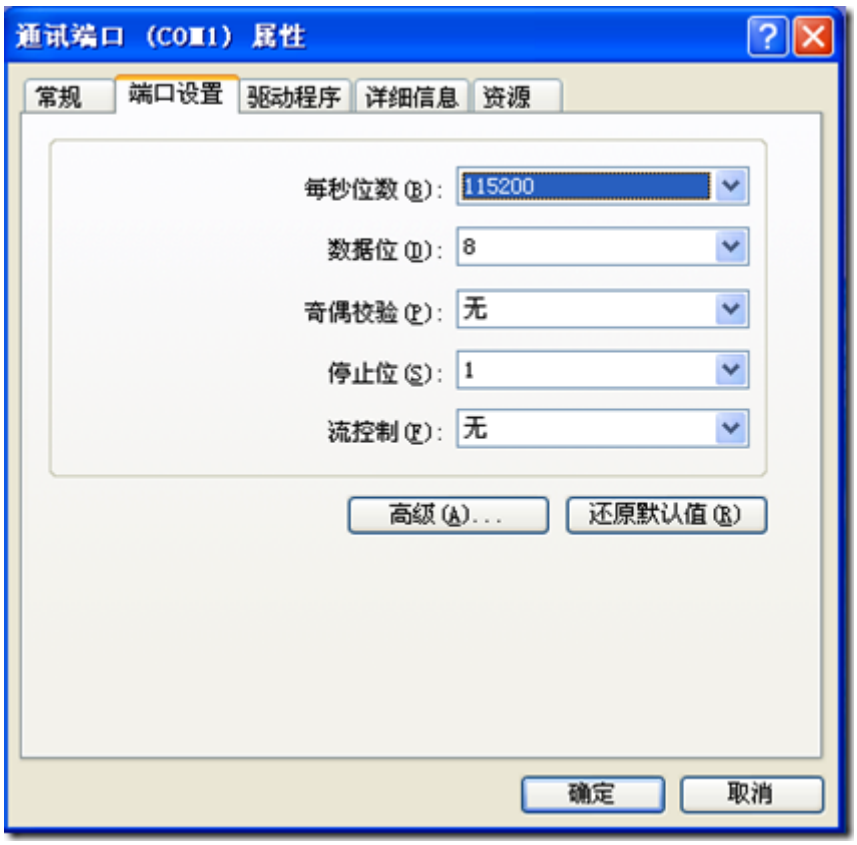
注意这里的debugport指定的端口必须与你在上一步配置的命名管道的端口相同，至于baudrate，你可以指定为57600或115200，需要注意的是，物理机上该端口的baudrate值必须和你在这里指定的baudrate相同。配置如下图：



至此，虚拟机的配置已完毕。

剩下的是物理机的配置，这个工作就比较简单了。

首先，安装WinDbg；然后，配置物理机COM端口的baudrate：“我的电脑”->（右键）”属性”->”硬件”->”设备管理器”，选择你在虚拟机上配置的相同的COM口，右击”属性”，配置COM的每秒位数值与你在虚拟机的/baudrate值相同。其他的值可以就用缺省值，如下图：



然后，配置WinDbg的启动选项，我喜欢做成一个批处理文件，bat（或cmd）文件内容如下：

windbg -k com:pipe,port=\\.\pipe\your_pipe_name

这里的your_pipe_name名称就是你配置的虚拟机的命名管道名称。把这个批处理文件放在你的WinDbg.exe所在的目录。然后就一切OK了。

三、 调试过程

首先，启动你的虚拟机，然后单击物理机上你做的那个bat文件，注意，如果这时候你的虚拟机还没有启动，单击bat文件会出现"系统找不到指定文件"的错误。这是因为你的虚拟机没有启动，或者你的虚拟机的COM口还没有准备好。不要紧，在虚拟机操作系统启动的过程中等个一两秒，再执行批处理文件，如果一切OK的话，WinDbg中会出现如下图所示的信息：

Microsoft (R) Windows Debugger Version 6.8.0004.0 X86

Copyright (c) Microsoft Corporation. All rights reserved.

```
Opened \\.\pipe\my_pipe
Waiting to reconnect...
Connected to Windows XP 2600 x86 compatible target, ptr64 FALSE
Kernel Debugger connection established.
Symbol search path is: *** Invalid ***
************************************************************************
* Symbol loading may be unreliable without a symbol search path.       *
* Use .symfix to have the debugger choose a symbol path.               *
* After setting your symbol path, use .reload to refresh symbol locations. *
************************************************************************
```

此时，按住ctrl+break，你就可以挂起虚拟机操作系统，open你的source file，F9加入断点，你就开始你的驱动程序调试之旅了:)。如果你还想加入操作系统的调试符号，你需要将如下的值加入到你的WinDbg配置中：

在WinDbg中，"File"->"Symbol file path"中加入如下的值：

```
SRV*d:\winsymbols*http://msdl.microsoft.com/download/symbols
```

其中，d:\winsymbols就是你期望下载下来的符号的保存路径，因为是动态下载，所以要保证机器联网才行。

Lastly，enjoy your kernel debug journey！