Project 12: Kernel Debugging with WinDbg (PC version) (20 pts.)

What You Need

- A Windows 7 machine with VMware Player installed.
- A Windows XPSP3 virtual machine to examine.

Purpose

Introduction to WinDbg and kernel debugging

The Two Machines

You need two Windows machines to do this project: One is the TARGET machine, which is a virtual machine running Win XP SP3.

The other is the WINDBG machine, which is the Windows 7 host.

Adding a Boot Menu Item to the TARGET machine

Start the Windows XPSP3 virtual machine.

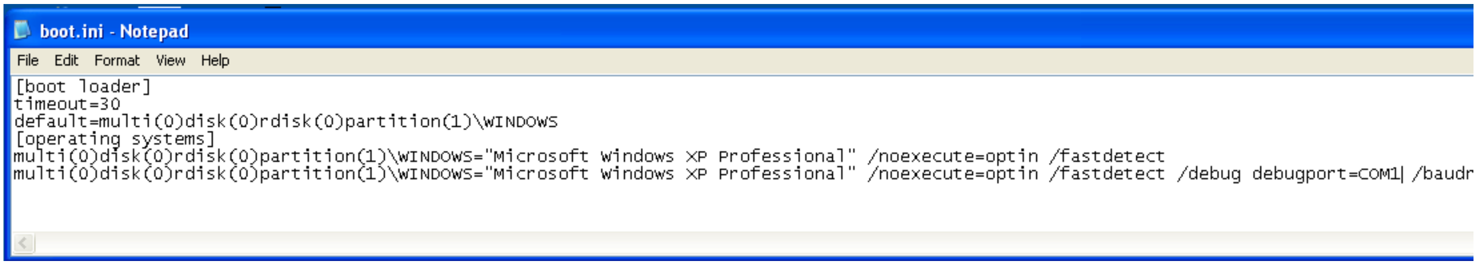
Click **Start**, **Run**.

In the Run box, execute this command:

```
notepad c:\boot.ini
```

In Notepad, copy the existing boot line, paste it at the end of the file, and add these switches to the end of the line, as shown below:

```
/debug /debugport=com1 /baudrate=115200
```



```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional" /noexecute=optin /fastdetect
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional" /noexecute=optin /fastdetect /debug debugport=COM1 /baudr
```

Save the file.

If you cannot save the file, open a Command Prompt and execute this command, to remove the Read-only, System, and Hidden flags from the file:

```
attrib -R -S -H c:\boot.ini
```

Adding a Virtual Serial Adapter

Power off the TARGET virtual machine. You cannot make this change while the virtual machine is running or suspended.

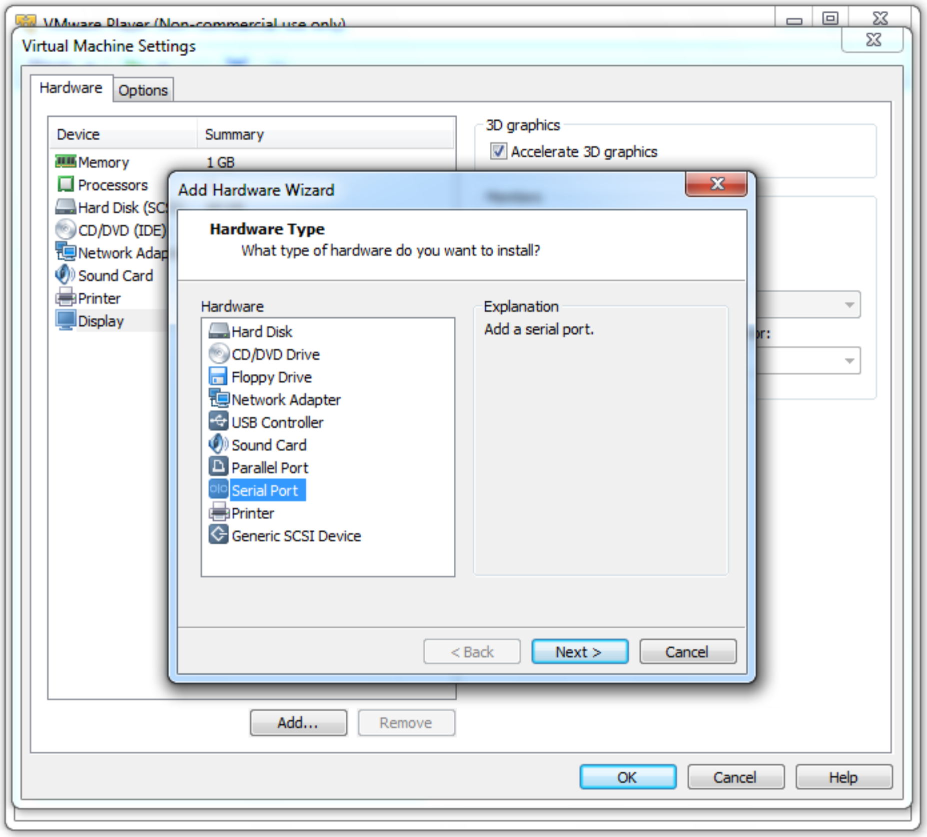
On the WINDBG machine, start VMware Player.

In the left pane of VMware Player, click your TARGET machine.

At the lower right of VMware Player, click "**Edit virtual machine settings**".

In the left side of the "Virtual Machine Settings" box, click the **Add...** button.

In the "Hardware Type" box, select "**Serial Port**", as shown below.



Add Hardware Wizard

Hardware Type

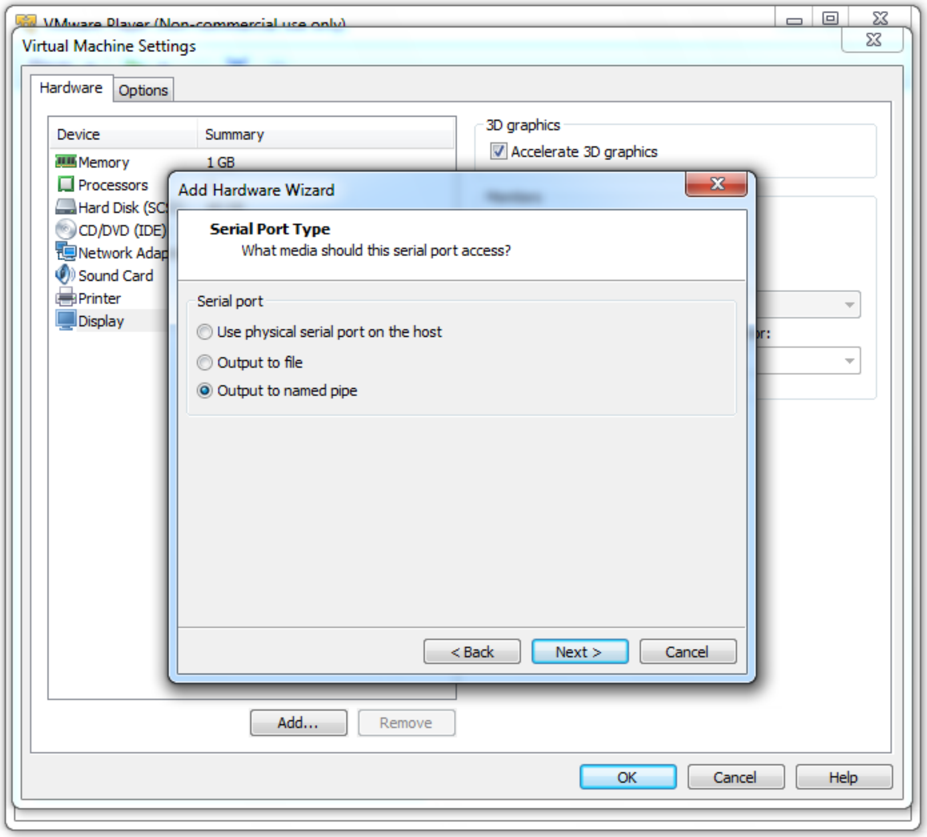
What type of hardware do you want to install?

Explanation

Add a serial port.

Click **Next**.

In the "Serial Port Type" box, click "**Output to named pipe**", as shown below.



Add Hardware Wizard

Serial Port Type

What media should this serial port access?

Serial port

○ Use physical serial port on the host

○ Output to file

● Output to named pipe

Click **Next**.

In the "Specify Socket" box, enter a Named Pipe of

```
\\.\pipe\com_1
```

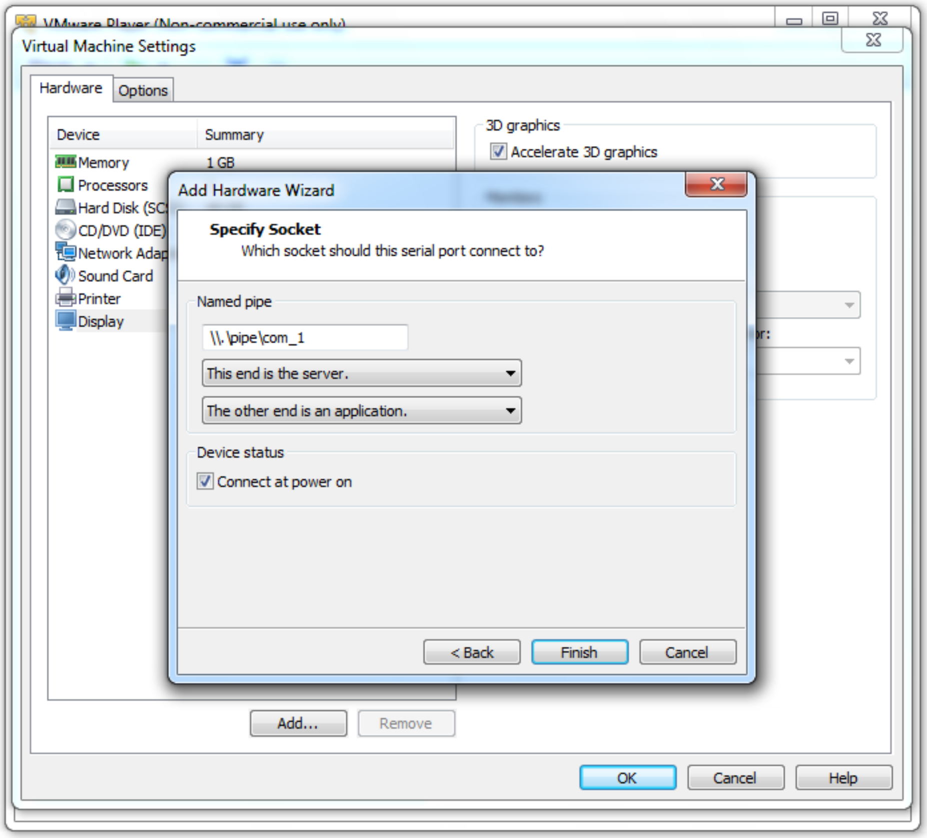
In the two drop-down list boxes, select

This end is the server.

and

The other end is an application.

as shown below.



Add Hardware Wizard

Specify Socket

Which socket should this serial port connect to?

Named pipe

\\.\pipe\com_1

This end is the server.

The other end is an application.

Device status

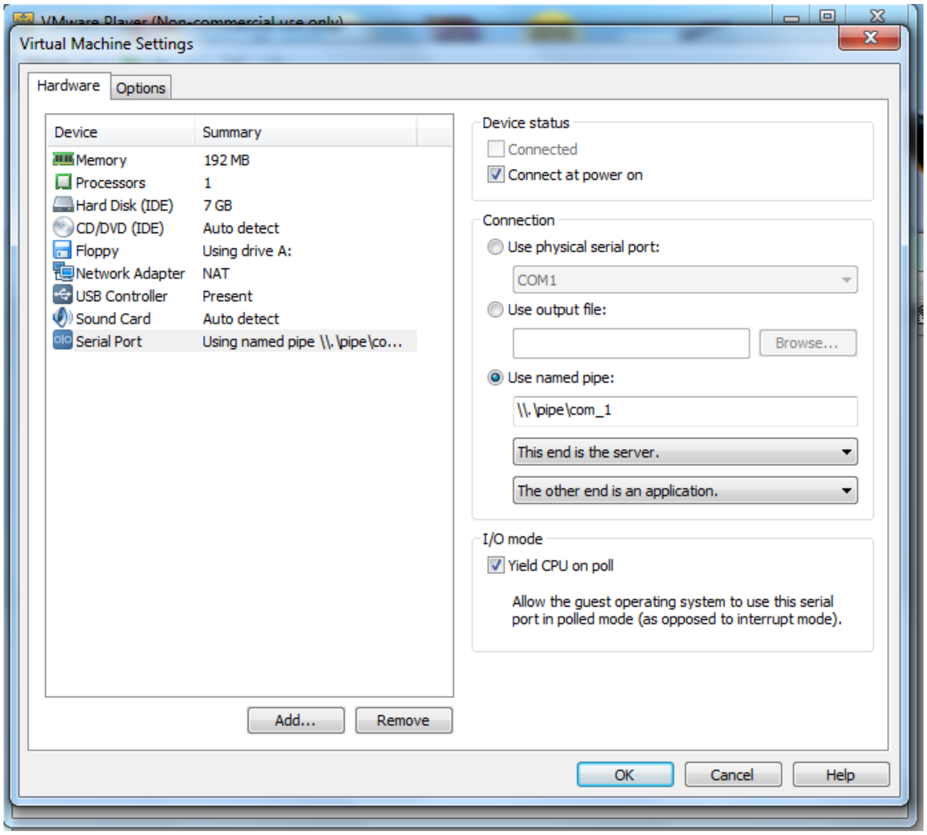
☑ Connect at power on

☑ Accelerate 3D graphics

Click **Finish**.

In the "Virtual Machine Settings" box, on the lower right, click the "**Yield CPU on poll**" box, as shown below.

Then click the **OK** button.



Virtual Machine Settings

Device	Summary
Memory	192 MB
Processors	1
Hard Disk (IDE)	7 GB
CD/DVD (IDE)	Auto detect
Floppy	Using drive A:
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Serial Port	Using named pipe \\.\pipe\co...

Device status

□ Connected

☑ Connect at power on

Connection

○ Use physical serial port:

COM1

○ Use output file:

● Use named pipe:

\\.\pipe\com_1

This end is the server.

The other end is an application.

I/O mode

☑ Yield CPU on poll

Allow the guest operating system to use this serial port in polled mode (as opposed to interrupt mode).

Downloading Microsoft Symbols

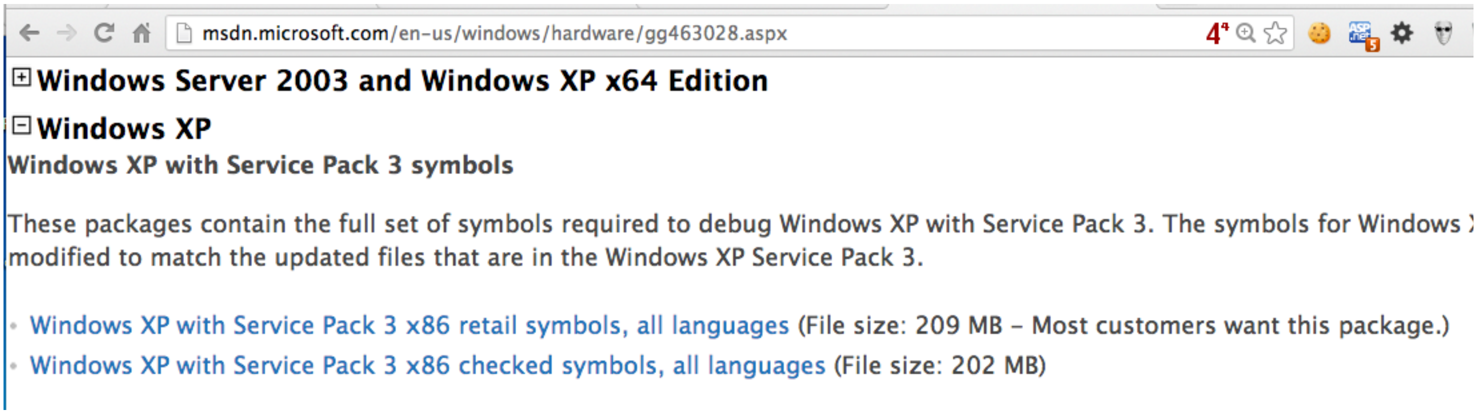
Kernel debugging is much easier with symbols.

WinDbg can download them automatically as needed, but downloading them separately is the best procedure if you plan to work without always being connected to a reliable, high-speed Internet connection.

Start the WINDBG machine. in a Web browser, go to

http://msdn.microsoft.com/en-us/windows/hardware/gg463028.aspx

Download the symbol file for "Windows XP with Service Pack 3 x86 retail symbols, all languages", as shown below.



msdn.microsoft.com/en-us/windows/hardware/gg463028.aspx

⊞ Windows Server 2003 and Windows XP x64 Edition

⊟ Windows XP

Windows XP with Service Pack 3 symbols

These packages contain the full set of symbols required to debug Windows XP with Service Pack 3. The symbols for Windows X modified to match the updated files that are in the Windows XP Service Pack 3.

- Windows XP with Service Pack 3 x86 retail symbols, all languages (File size: 209 MB – Most customers want this package.)
- Windows XP with Service Pack 3 x86 checked symbols, all languages (File size: 202 MB)

You end up with an EXE file. Run it in the WINDBG machine. Accept all the default options.

First it will extract into a temporary directory with a long name, then it will automatically extract into C:\Windows\Symbols. Accept that selection.

Installing WinDbg on the WINDBG Machine

On the WINDBG machine, open a browser and go to

http://msdn.microsoft.com/en-US/windows/desktop/bg162891

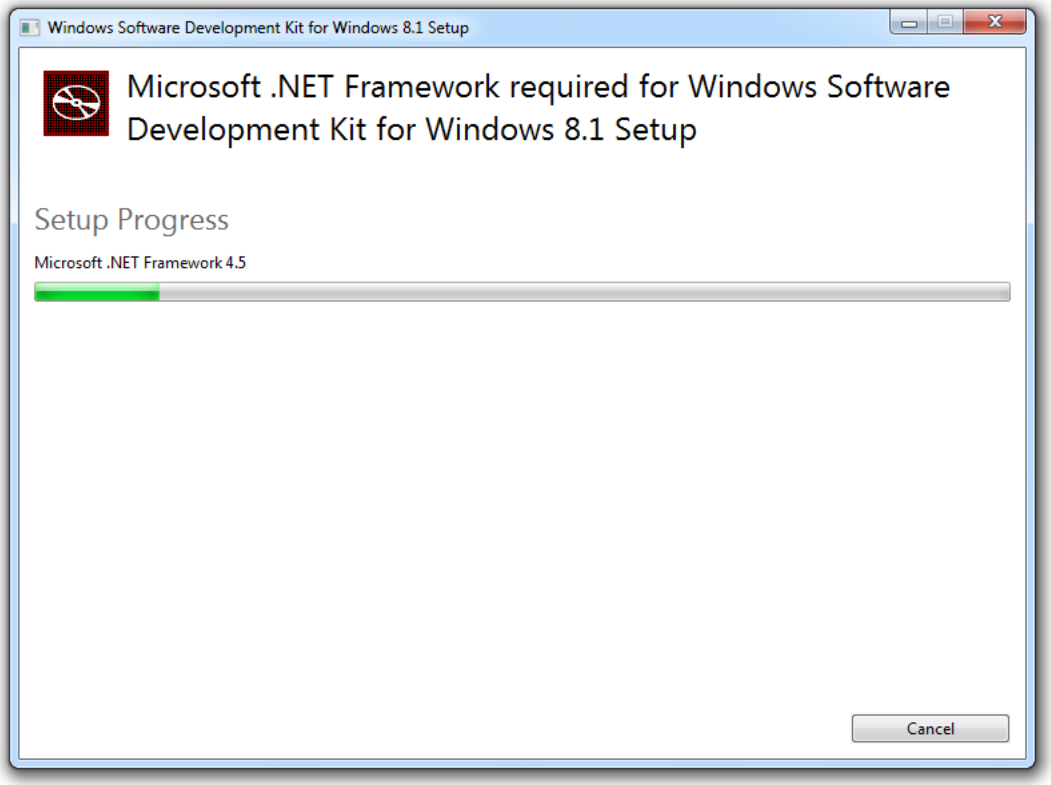
Click the blue **Download** button.

Save the sdksetup.exe file on your desktop.

Double-click the **sdksetup.exe** file.

Accept the agreement and click the "**Accept & Install**" button.

Wait while .NET installs, as shown below.



Windows Software Development Kit for Windows 8.1 Setup

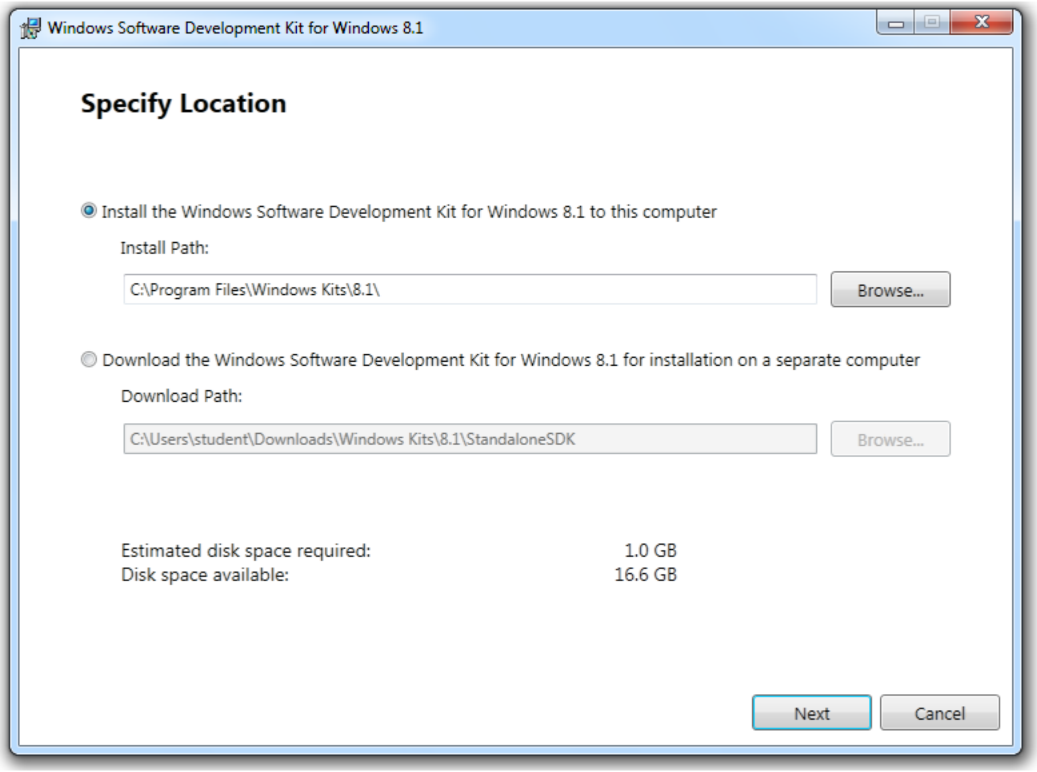
Microsoft .NET Framework required for Windows Software Development Kit for Windows 8.1 Setup

Setup Progress

Microsoft .NET Framework 4.5

In the "Specify Location" box, accept the default options, as shown below.

Click **Next**.



Windows Software Development Kit for Windows 8.1

Specify Location

● Install the Windows Software Development Kit for Windows 8.1 to this computer

Install Path:

C:\Program Files\Windows Kits\8.1\

○ Download the Windows Software Development Kit for Windows 8.1 for installation on a separate computer

Download Path:

C:\Users\student\Downloads\Windows Kits\8.1\StandaloneSDK

Estimated disk space required: 1.0 GB

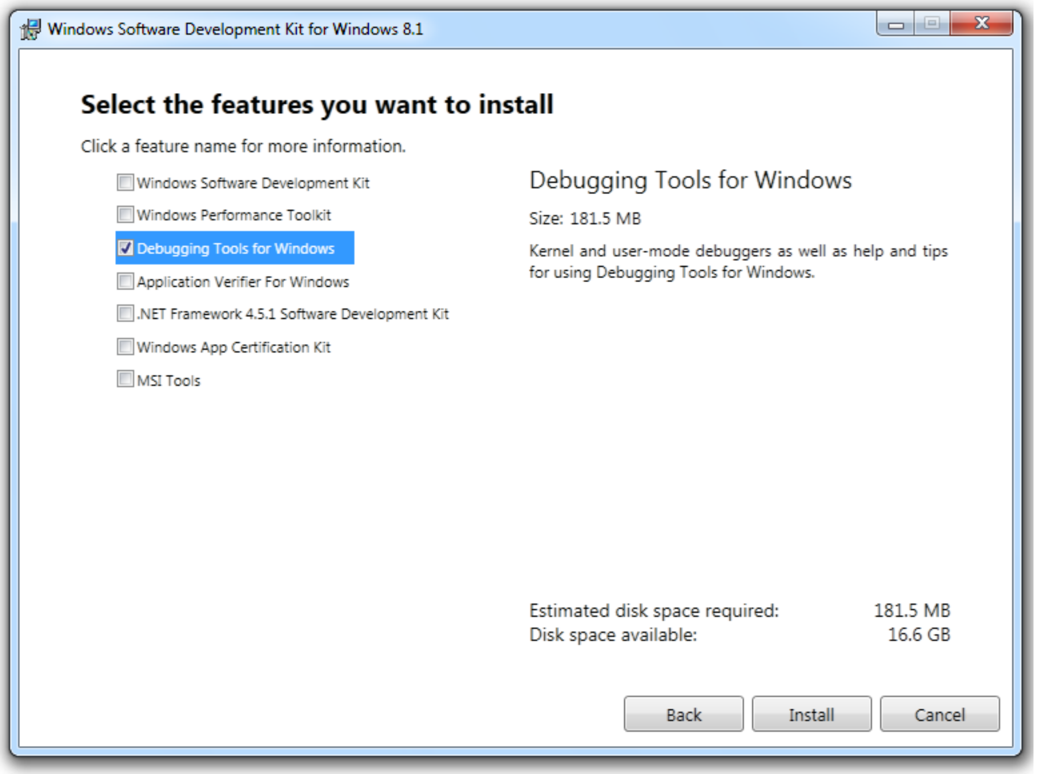
Disk space available: 16.6 GB

In the "Join the Customer Experience Improvement Program (CEIP)" box, accept the default selection of No and click **Next**.

In the "License Agreement" box, click **Accept**.

In the "Select the features you want to install" box, clear all the check boxes except "**Debugging Tools for Windows**", as shown below.

Click **Install**.



Windows Software Development Kit for Windows 8.1

Select the features you want to install

Click a feature name for more information.

- □ Windows Software Development Kit
- □ Windows Performance Toolkit
- ☑ Debugging Tools for Windows
- □ Application Verifier For Windows
- □ .NET Framework 4.5.1 Software Development Kit
- □ Windows App Certification Kit
- □ MSI Tools

Debugging Tools for Windows

Size: 181.5 MB

Kernel and user-mode debuggers as well as help and tips for using Debugging Tools for Windows.

Estimated disk space required:	181.5 MB
Disk space available:	16.6 GB

When the process is complete, you see a message saying "Welcome to the Windows Software Deveopment Kit for Windows 8.1!".

Click **Close**.

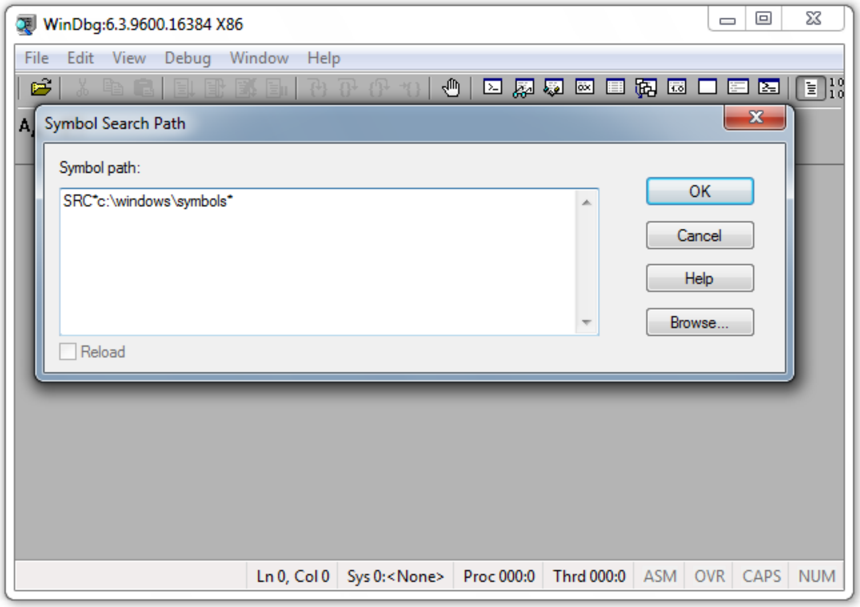
Configuring Symbols in WinDbg

Click **Start**. Type in **WINDBG**.

Launch WinDbg. If you are using Windows 7, run it as Administrator.

In WinDbg, click **File**, "**Symbol File Path**". Enter this line, as shown below:

```
SRC*c:\windows\symbols*
```



WinDbg:6.3.9600.16384 X86

Symbol Search Path

Symbol path:

```
SRC*c:\windows\symbols*
```

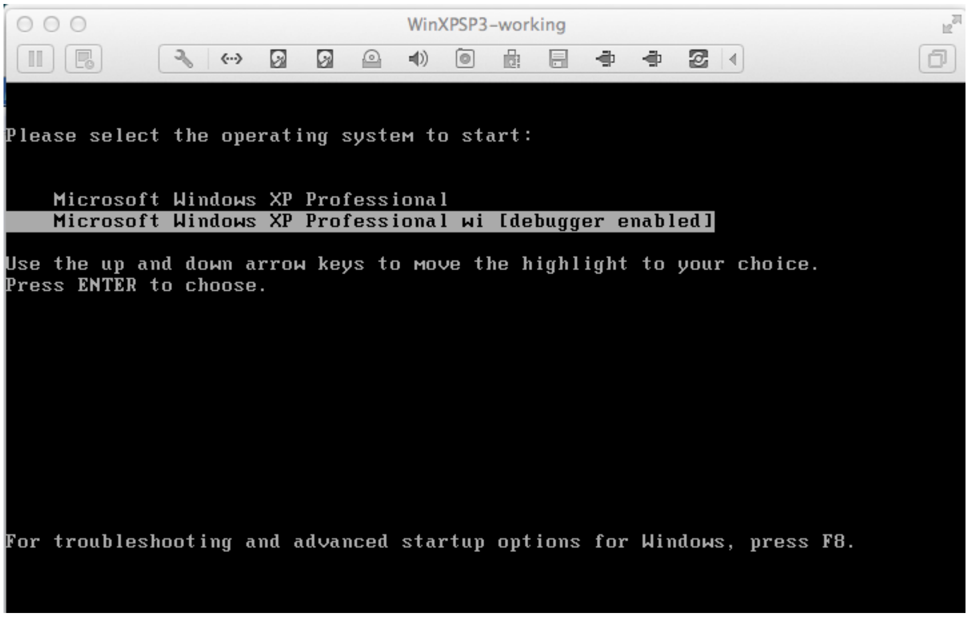
□ Reload

Click the **OK** button.

Starting the TARGET machine

Start the TARGET virtual machine.

When you should see two boot-menu options, choose the second one, "Microsoft Windows XP Professional with debugger enabled", as shown below.



```
Please select the operating system to start:


    Microsoft Windows XP Professional
    Microsoft Windows XP Professional wi [debugger enabled]

Use the up and down arrow keys to move the highlight to your choice.
Press ENTER to choose.



For troubleshooting and advanced startup options for Windows, press F8.
```

Starting Kernel Debugging

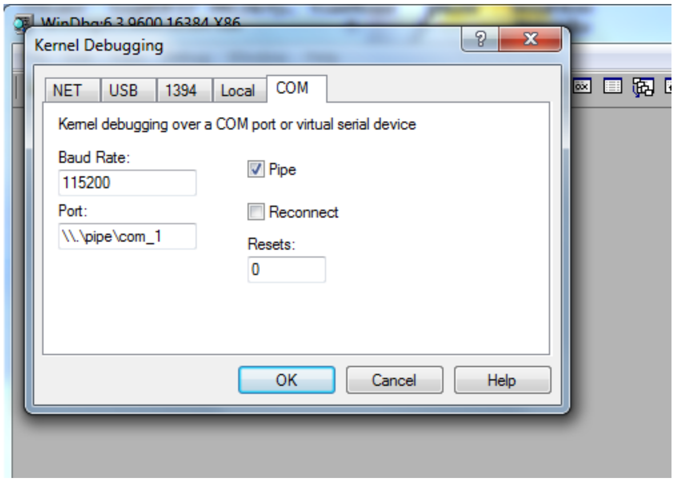
In WinDbg, click **File**, "**Kernel Debug**".

In the "Kernel Debugging" box, click the **COM** tab.

Change the Port to

```
\\.\pipe\com_1
```

and check the **Pipe** box, as shown below. Then click **OK**.



Kernel debugging over a COM port or virtual serial device

Baud Rate: 115200

Port: \\.\pipe\com_1

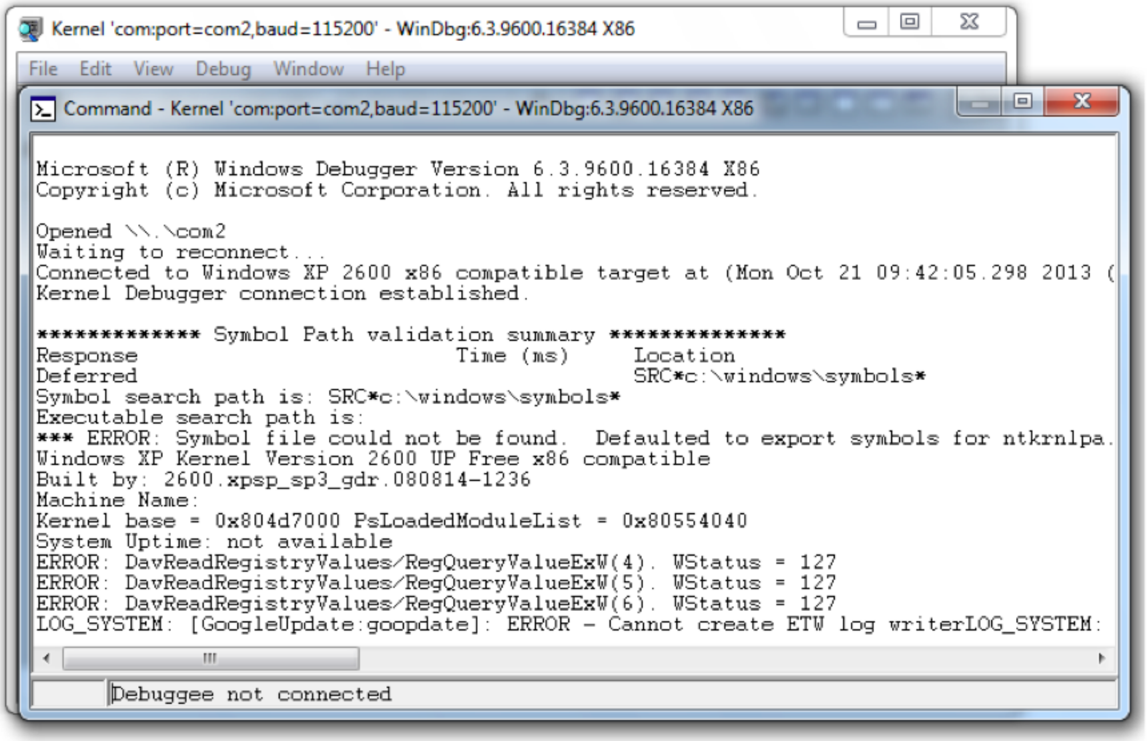
☑ Pipe

□ Reconnect

Resets: 0

Your WINDBG machine should now show the message "**Connected to Windows XP**", as shown below. (The figure below shows "com_2" instead of "com_1", just ignore that.)

If it doesn't connect, try restarting the virtual machine.


Kernel 'com:port=com2,baud=115200' - WinDbg:6.3.9600.16384 X86
File Edit View Debug Window Help
Command - Kernel 'com:port=com2,baud=115200' - WinDbg:6.3.9600.16384 X86

```
Microsoft (R) Windows Debugger Version 6.3.9600.16384 X86
Copyright (c) Microsoft Corporation. All rights reserved.

Opened \\.\com2
Waiting to reconnect...
Connected to Windows XP 2600 x86 compatible target at (Mon Oct 21 09:42:05.298 2013 (
Kernel Debugger connection established.

************* Symbol Path validation summary **************
Response                         Time (ms)     Location
Deferred                                       SRC*c:\windows\symbols*
Symbol search path is: SRC*c:\windows\symbols*
Executable search path is:
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for ntkrnlpa.
Windows XP Kernel Version 2600 UP Free x86 compatible
Built by: 2600.xpsp_sp3_gdr.080814-1236
Machine Name:
Kernel base = 0x804d7000 PsLoadedModuleList = 0x80554040
System Uptime: not available
ERROR: DavReadRegistryValues/RegQueryValueExW(4). WStatus = 127
ERROR: DavReadRegistryValues/RegQueryValueExW(5). WStatus = 127
ERROR: DavReadRegistryValues/RegQueryValueExW(6). WStatus = 127
LOG_SYSTEM: [GoogleUpdate:goopdate]: ERROR - Cannot create ETW log writerLOG_SYSTEM:

Debuggee not connected
```

Saving a Screen Image

Make sure you can see the message "**Connected to Windows XP**", as shown above.

On your keyboard, press the PrntScrn key.

Click **Start**, type in **PAINT**, and open Paint.

Press **Ctrl+V** to paste in the image of your desktop.

YOU MUST SUBMIT WHOLE-DESKTOP IMAGES TO GET FULL CREDIT.

Save the image with a filename of "**Proj 12 from YOUR NAME**".

Turning in Your Project

Email the images to: **cnit.126sam@gmail.com** with a subject line of **Proj 12 From Your Name**, replacing Your Name with your own first and last name. Send a Cc to yourself.

Last Modified: 10-21-13 10:23 pm