Project 11x: Kernel Debugging with WinDbg over Ethernet with Windows 8 (20 pts.)

What You Need

- Two real (not virtual) Windows 8 machines

Purpose

To debug crashes in a kernel, without using a real or virtual serial cable.

Identifying your Computers

Choose one computer to be the **Host** and one to be the **Target**. The computer that runs the debugger is called the host computer, and the computer being debugged is called the target computer. The host computer must be running Windows XP or later, and the target computer must be running Windows 8 or later.

Turn off Firewalls

On both computers, click **Start**, type in **FIREWALL**, click "**Windows Firewall**", and turn off Windows Firewall.

Choosing a NIC

Start the Windows 8 Target computer. Log in as **student** with no password.

I checked the Microsoft list of supported adapters, and that said we should use the Intel NIC, not the Realtek NIC:

Supported Ethernet NICs for Network Kernel Debugging in Windows 8.1

However, in practice, the Realtek NIC seems to work better, so I recommend ignoring the Microsoft list and just trying the card(s) you have.

Plug in a NIC of your choice.

In Network Connections, disable all NICs you aren't using.

Install WinDbg on your Host Computer

On the Windows 8 Host machine, open Internet Explorer and go to

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

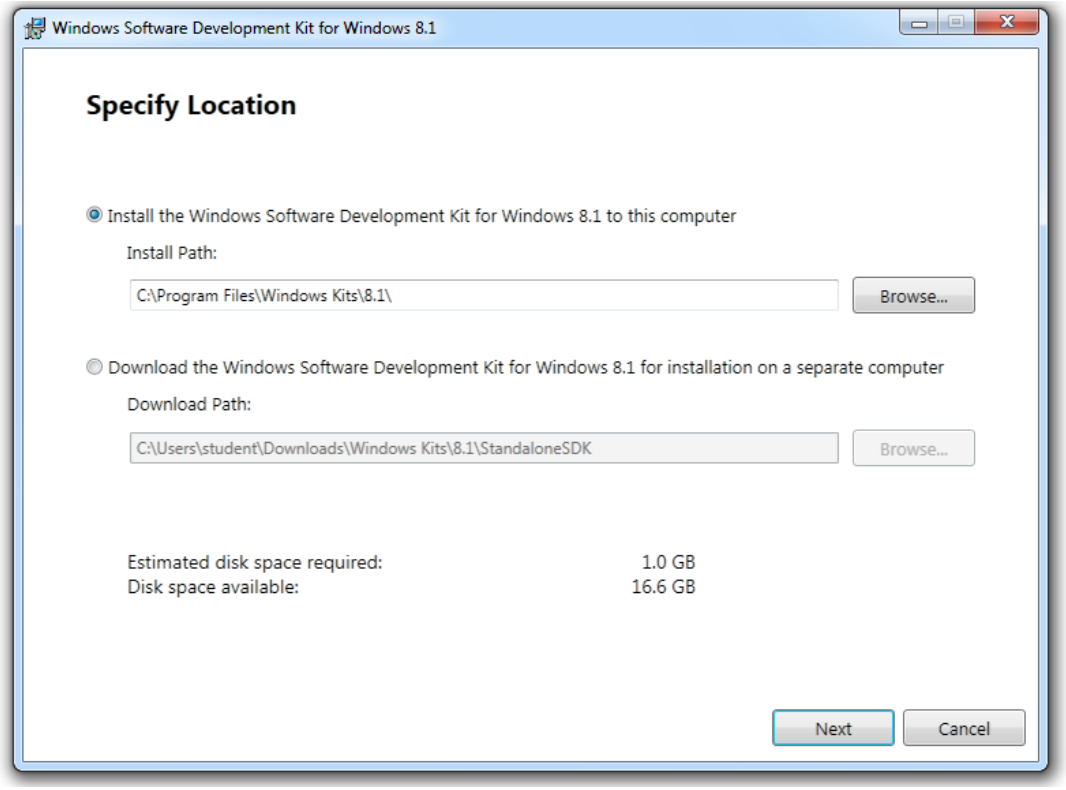
Click the blue **Download** button.

Run the setup file.

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

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

Click **Next**.

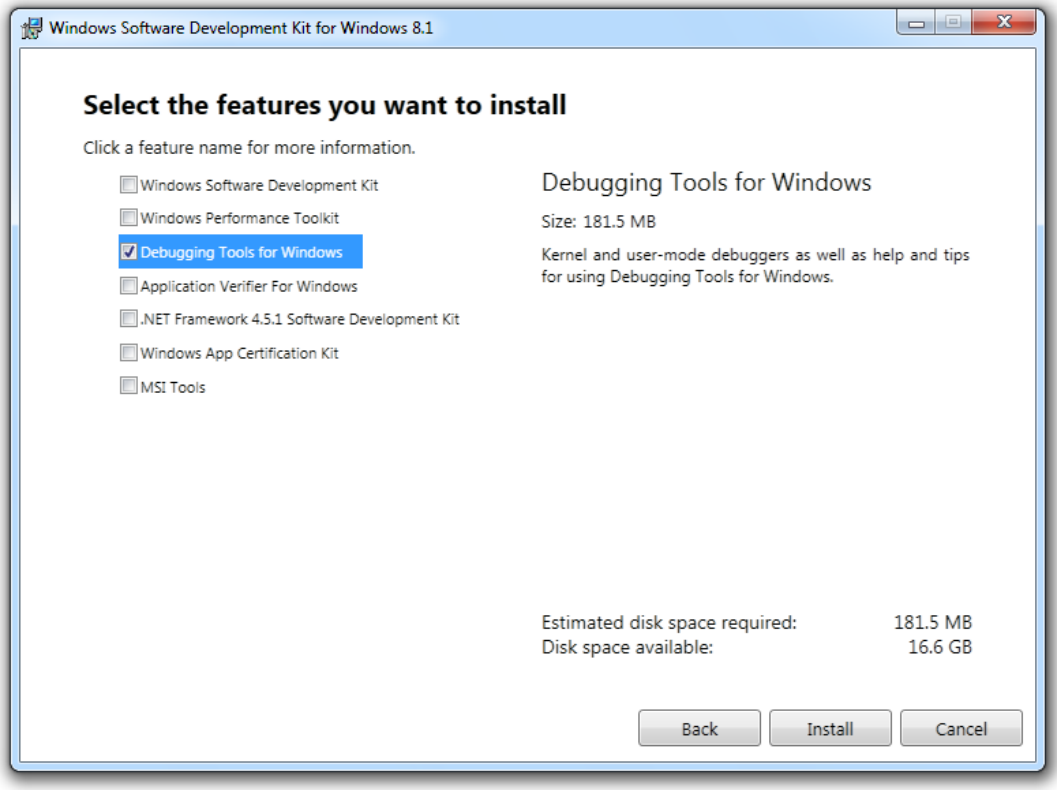


In the "Join the Customer Experience Improvement Program (CEIP)" box, accept the default selection of No and click **Next**.

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**.



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

Click **Close**.

Find the IP Address of your Host Computer

On your Windows 8 Host computer, click **Start**. Type in **CMD** and press **Enter**.

Execute this command:

```
IPCONFIG
```

Find your computer's IP address and record it.

Configuring Debugging on your Target Computer

On your Windows 8 Target machine, click **Start**. Type in **CMD**

Right-click "**Command Prompt**" and cick "**Run as Administrator**".

In the User Account Control box, click **Yes**.

In the Administrator Command Prompt window, execute these commands, replacing the IP address with the IP address of your Host Windows 8 machine:

```
bcdedit /debug on

bcdedit /dbgsettings net hostip:192.168.1.170 port:50000 key:1.2.3.4
```

Note: the key used here is easy to use but not secure--using a longer, more random, key is safer.

Then restart the Target computer. The boot menu will show "Windows 8 [debugger enabled]", if it is a multiboot system like the ones in S214.

Setting Up the Host Computer

On the Host computer, in the Start screen, type **WINDBG**

Right-click "**WinDbg (X64)**" and click "**Run as Administrator**".

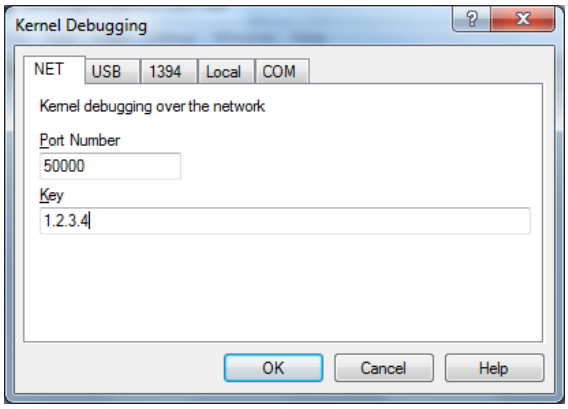
In the User Account Control box, click **Yes**.

Click **File**, "**Kernel Debug**".

On the NET tab, enter a key of

1.2.3.4

as shown below. Then click **OK**.



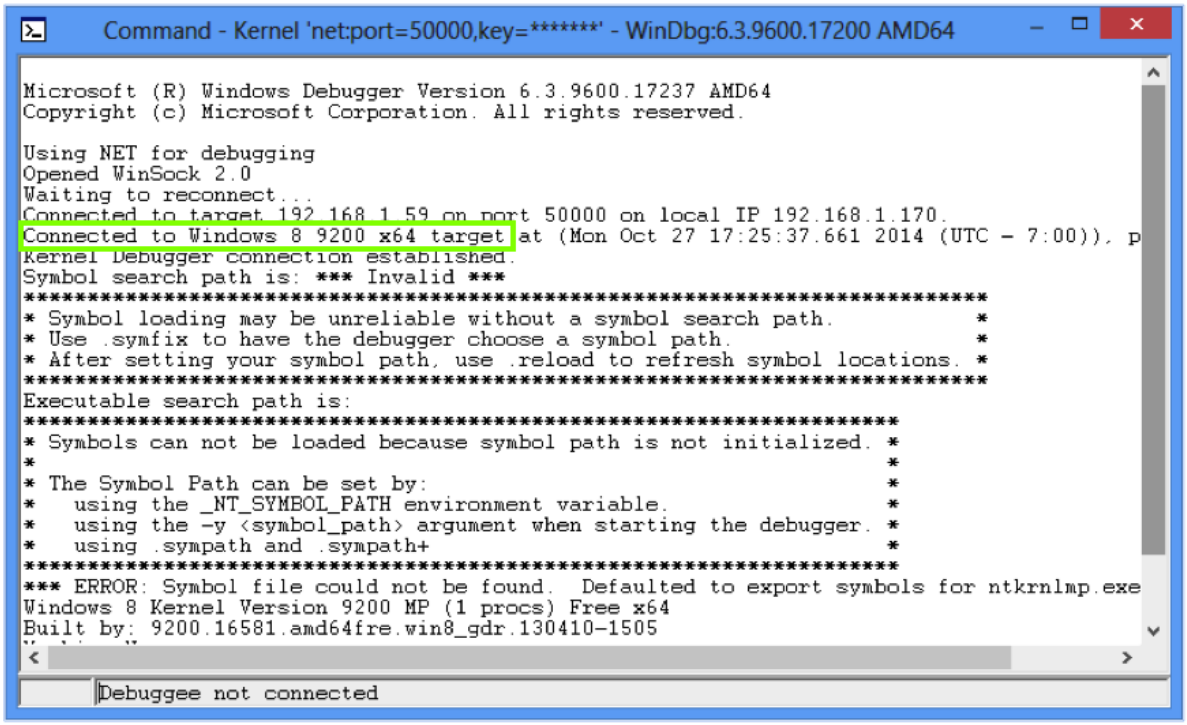
If a box pops up saying "Windows Firewall has blocked some features of this app", click "**Allow access**".

WinDbg shows a message: "Waiting to reconnect...".

If the message doesn't change in a few seconds, restart the Target computer again.

Establishing a Connection

When the connection is extablished, you'll see the message "Connected to Windows 8", as shown below.



Saving the Screen Image

Make sure you can see the "**Connected to Windows**" message.

Save a FULL DESKTOP image with the filename **Proj 11x from Your Name**.

Turning in Your Project

Send the image as an email attachment to **cnit.126sam@gmail.com** with a Subject line of **Proj 11x from Your Name**.

Source

[Setting Up Kernel-Mode Debugging over a Network Cable Manually]

Posted 10-27-14 5:43 PM by Sam Bowne