Proj 12: Kernel Debugging with Livekd and Windows Server 2008 (20 pts.)

What You Need

A Windows Server 2008 machine, real or virtual.

Purpose

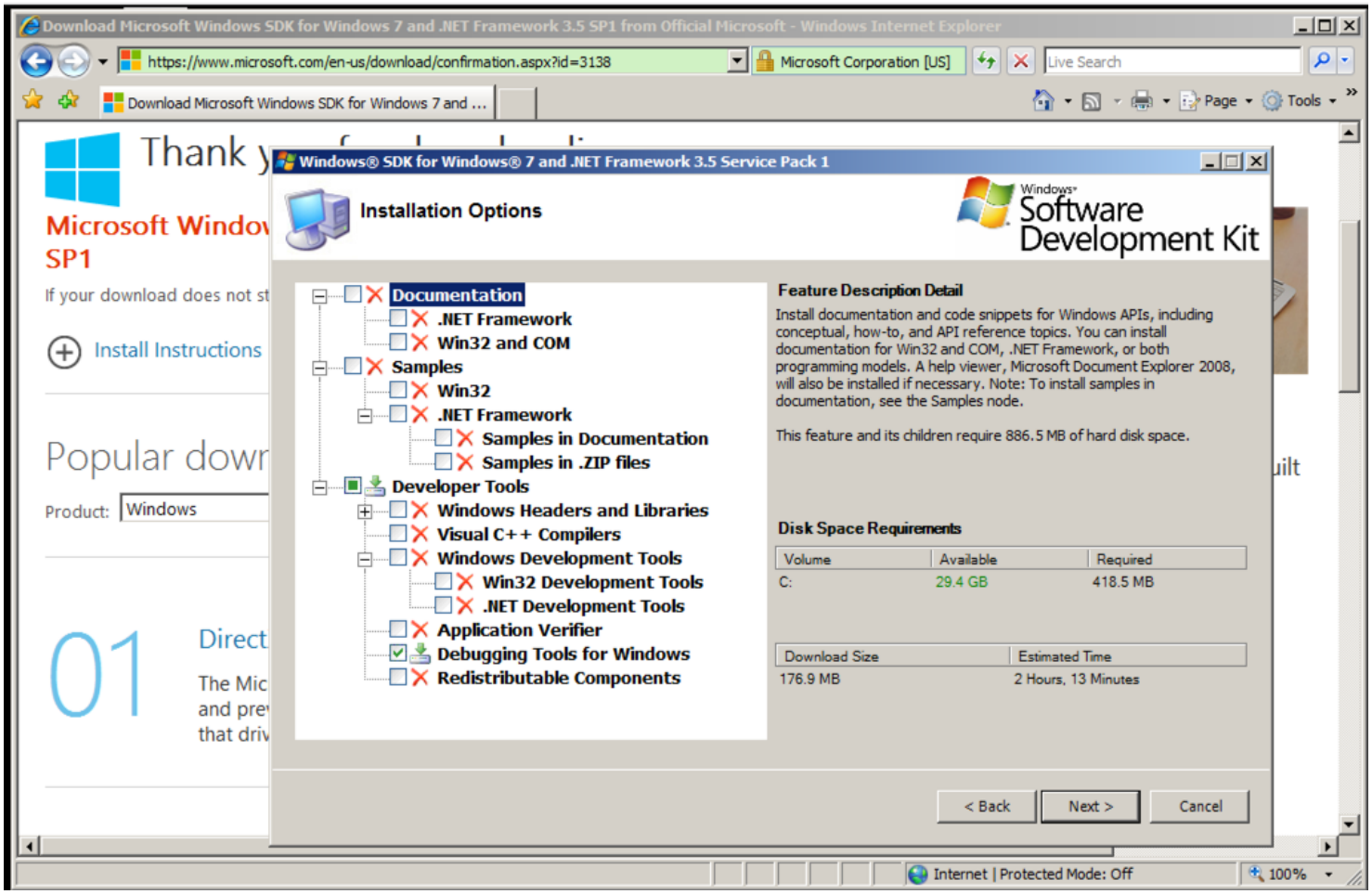
To debug the Windows kernel. To get full functionality, you need to use two machines and a network connection, but the Sysinternals Livekd utility makes it possible to get a lot of kernel debugging functionality with a single PC, which is very convenient!

Installing Debugging Tools for Windows

Open a Web browser and go to :

https://www.microsoft.com/en-us/download/details.aspx?id=3138

Install the Software Development Kit, with the Installation Options shown below:



Editing the Path

Open a Command Prompt and execute this command:

```
windbg
```

If Windbg opens, everything is working and you can close it.

If it fails to open, which is very common, that means the SDK did not adjust the Path. To fix it, click **Start**. Right-click **Computer** and click **Properties**.

Click "**Advanced System Settings**".

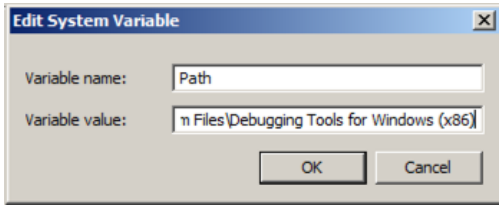
In System Properties, on the **Advanced** tab, click the "**Environment Variables**" button.

In the Environment Variables box, in the "System variables" section, scroll down and click **Path**. Click the **Edit...** button.

At the end of the Path, append a semicolon followed by the path to Windbg, which will be similar to this:

```
C:\Program Files\Debugging Tools for Windows (x86)\
```

Your window should look like the image below.



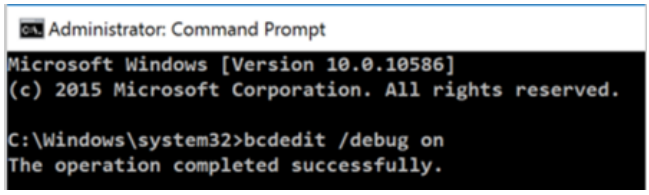
Click **OK** three times.

Setting Up Local Kernel-Mode Debugging

Open an Administrator Command Prompt window.

In the Administrator Command Prompt window, execute this command:

```
bcdedit /debug on
```



Click **Start**, **Power**, **Restart**.

Getting LiveKD

In a Web browser, go to

https://technet.microsoft.com/en-us/sysinternals/bb897415.aspx

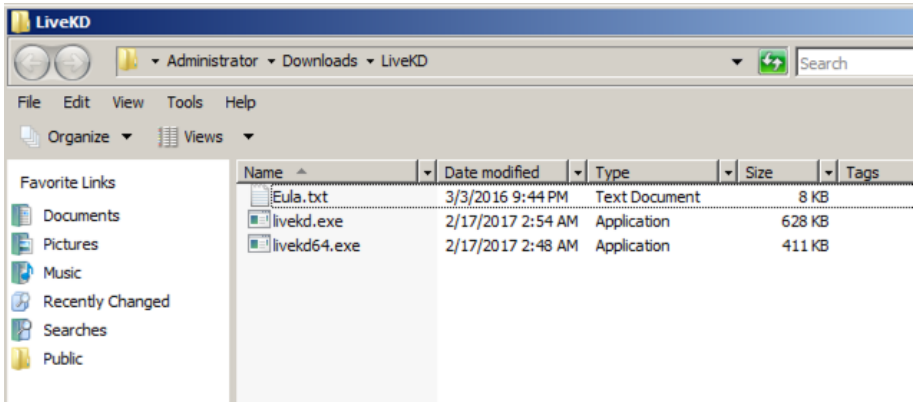
Click the "**Download LiveKd**" link.

Click "**Open Folder**".

Right-click **LiveKD.zip** and click "**Extract All...**", **Extract**.

A LiveKd window opens, showing three files, as shown below. Notice the path to this folder. When I did it, it was

Administrator · Downloads · LiveKD



Open an Administrator Command Prompt window.

In the Administrator Command Prompt window, execute this command. If your extracted files are in a different folder, you will have to modify this command.

```
copy C:\Users\Administrator\Downloads\LiveKD\livekd.exe c:\Windows\System32
```

```
C:\>copy C:\Users\Administrator\Downloads\LiveKD\livekd.exe C:\Windows\System32
        1 file(s) copied.

C:\>_
```

Using LiveKd

In the Administrator Command Prompt window, execute this command:

```
livekd -w
```

A "SYSINTERNALS SOFTWARE LICENSE TERMS" box pops up. Click the **Agree** button.

If you see "Error finding windbg.exe", as shown below, fix that with the Troublehooting advice in the box below.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>livekd -w

LiveKd v5.40 - Execute kd/windbg on a live system
Sysinternals - www.sysinternals.com
Copyright (C) 2000-2015 Mark Russinovich and Ken Johnson

Error finding windbg.exe:
The system cannot find the file specified.


Exiting LiveKd.


C:\Windows\system32>
```

Using Livekd

When Livekd starts, it asks you whether to set the _NT_SYMBOL_PATH automatically, as shown below.

Type **y** and press **Enter**.

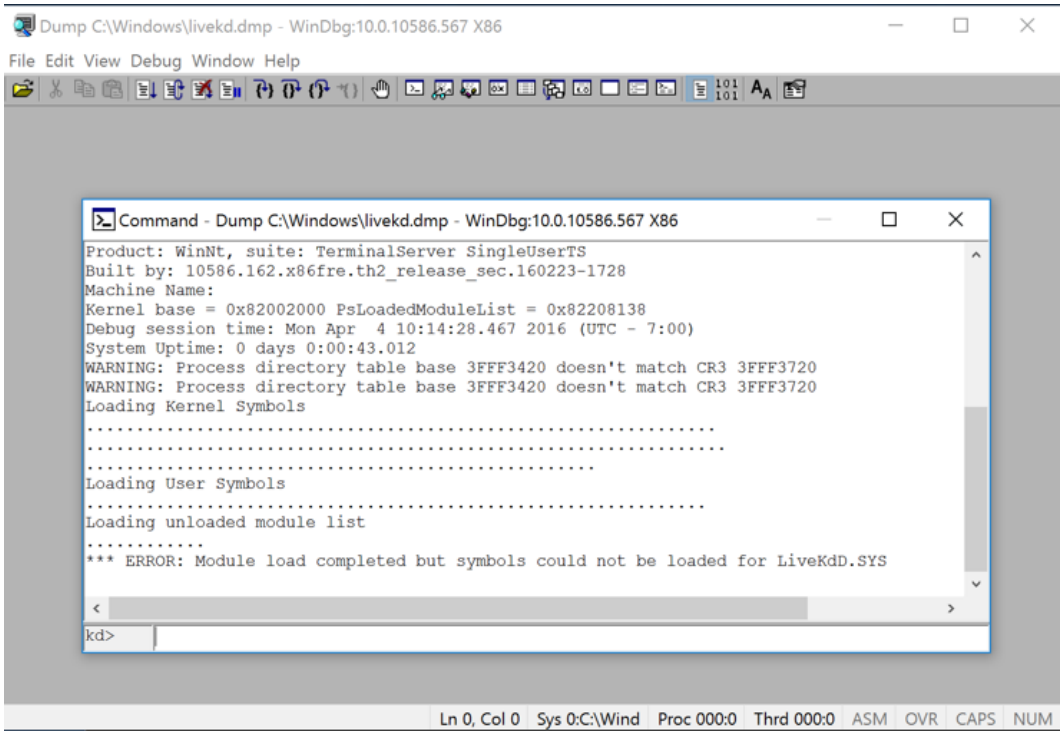
```
C:\Windows\system32>livekd -w

LiveKd v5.40 - Execute kd/windbg on a live system
Sysinternals - www.sysinternals.com
Copyright (C) 2000-2015 Mark Russinovich and Ken Johnson


Symbols are not configured. Would you like LiveKd to set the _NT_SYMBOL_PATH
directory to reference the Microsoft symbol server so that symbols can be
obtained automatically? (y/n) _
```

Livekd asks "Enter the folder to which symbols download". Press **Enter** to accept the default option.

Windbg launches, as shown below.



If you wish to change the font, click **View**, **Font**.

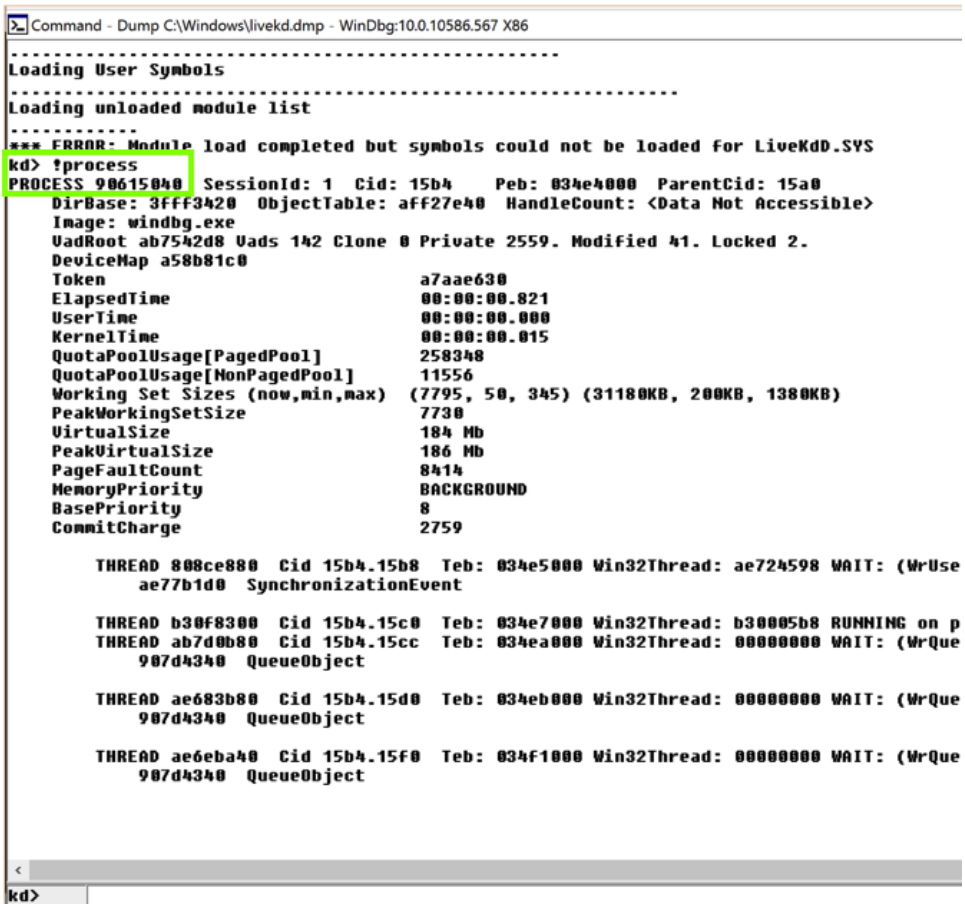
Make the "Command" window larger, as shown below.

This is a strange combination of a GUI and command-line, like the other debuggers we've used. Commands are typed into the box at the bottom and the results appear in the large top pane.

At the bottom of the Command window, in the command bar, execute this command:

```
!process
```

You should see the "**kd> !process**" command, and its output, showing a **PROCESS** number, as shown below.



```
Command - Dump C:\Windows\livekd.dmp - WinDbg:10.0.10586.567 X86
------------------------------------------------
Loading User Symbols
------------------------------------------------------------
Loading unloaded module list
-----------
*** ERROR: Module load completed but symbols could not be loaded for LiveKdD.SYS
kd> !process
PROCESS 90615040  SessionId: 1  Cid: 15b4    Peb: 034e4000  ParentCid: 15a0
    DirBase: 3fff3420  ObjectTable: aff27e40  HandleCount: <Data Not Accessible>
    Image: windbg.exe
    VadRoot ab7542d8 Vads 142 Clone 0 Private 2559. Modified 41. Locked 2.
    DeviceMap a58b81c0
    Token                             a7aae630
    ElapsedTime                       00:00:00.821
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.015
    QuotaPoolUsage[PagedPool]         258348
    QuotaPoolUsage[NonPagedPool]      11556
    Working Set Sizes (now,min,max)  (7795, 50, 345) (31180KB, 200KB, 1380KB)
    PeakWorkingSetSize                7730
    VirtualSize                       184 Mb
    PeakVirtualSize                   186 Mb
    PageFaultCount                    8414
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      2759

        THREAD 808ce880  Cid 15b4.15b8  Teb: 034e5000 Win32Thread: ae724598 WAIT: (WrUse
            ae77b1d0  SynchronizationEvent

        THREAD b30f8300  Cid 15b4.15c0  Teb: 034e7000 Win32Thread: b30005b8 RUNNING on p
        THREAD ab7d0b80  Cid 15b4.15cc  Teb: 034ea000 Win32Thread: 00000000 WAIT: (WrQue
            907d4340  QueueObject

        THREAD ae683b80  Cid 15b4.15d0  Teb: 034eb000 Win32Thread: 00000000 WAIT: (WrQue
            907d4340  QueueObject

        THREAD ae6eba40  Cid 15b4.15f0  Teb: 034f1000 Win32Thread: 00000000 WAIT: (WrQue
            907d4340  QueueObject

kd>
```

Saving the Screen Image

Make sure you can see the "**kd> !process**" command and a **PROCESS** number.

On your keyboard, press the PrntScrn key.

Open Paint and paste in the image.

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.

Sources

Setting Up Local Kernel Debugging of a Single Computer Manually

Getting Started with WinDbg (Kernel-Mode)

Windows 7 x64 Local and Live Kernel Debugging

Updated 3-11-17