CS490 Windows Internals Lab

Sep 17, 2012

1. Check System Information

(1) Which version of NTOSKRNL.EXE?

Go to Programs/Administrative Tools/Event Viewer. Select System Log. Double-click an Event Log entry with an Event ID of 6009.

(2) Check if it's booted with PAE version (Windows2000 or WinXp):

Registry entry:

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

Check the PhysicalAddressExtenstion item.

(3) Which kernel image and HAL at installation?

Run Windbg, using the following commands:

Check kernel information: lm vm nt

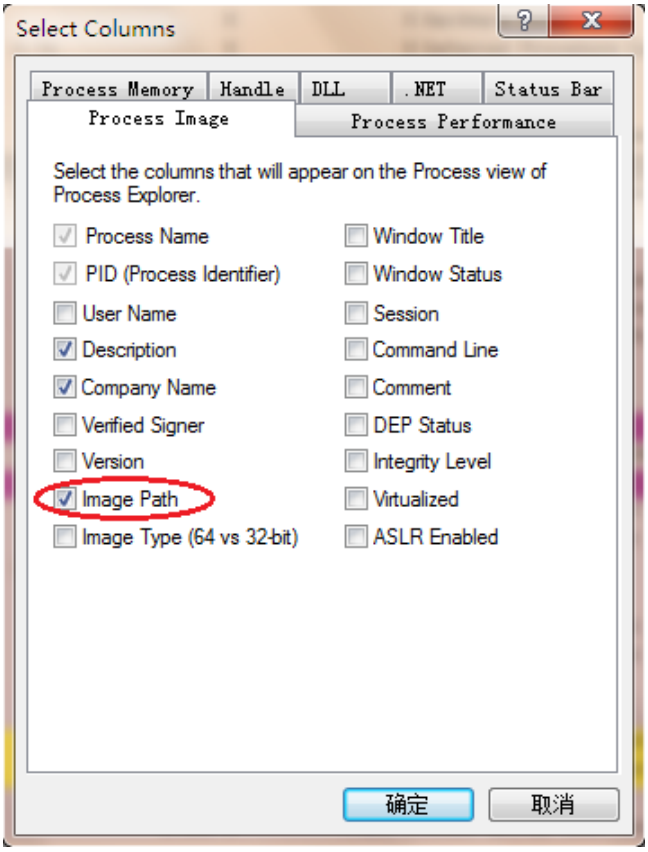
Check HAL information: lm vm hal

2. Process Details with Process Explorer

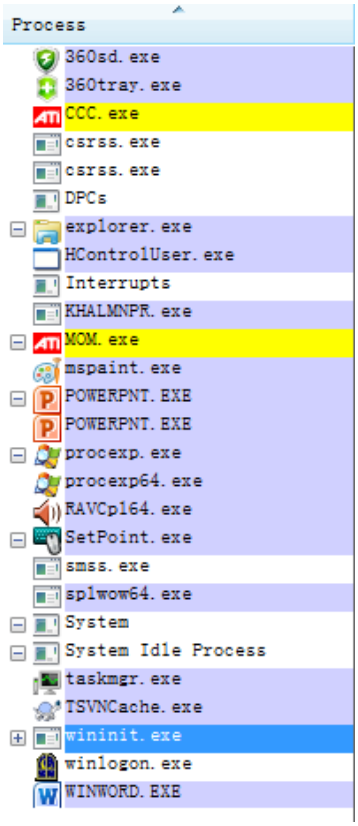
When Process Explorer starts, it shows by default the process list on the top half and opened handles for the currently selected process on the bottom half. It also shows image descriptions, company names, and full paths if the mouse pointer hovers over the process name. Notice that, the first time you run Process Explorer, you will receive a message that symbols are not currently configured. If you didn't set the symbol path in Lab 1, please configure it as described in Lab 1.

In this lab, we follow these steps:

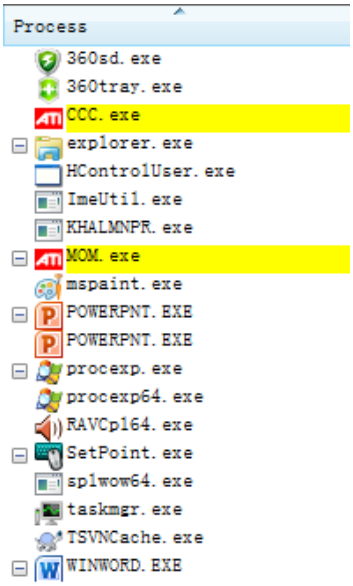
1. Turn off the lower pane by deselecting View, Show Lower Pane.
2. Notice that processes hosting services are highlighted by default in pink. Your own processes are highlighted in blue.
3. Hover your mouse pointer over the image name for processes, and notice the full path displayed by the ToolTip.
4. Click on View, Select Columns, and add the image path.



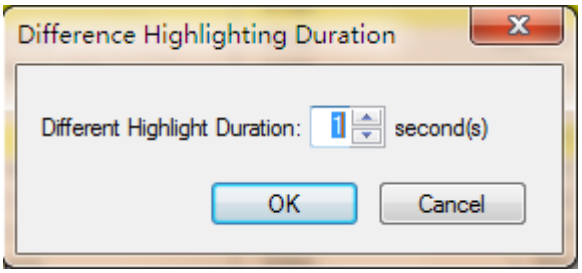
5. Sort on the process column, and notice the tree view disappears. (You can either display tree view or sort by any of the columns shown.) Click again to sort from Z to A. Then click again (or CTRL+T) and the display returns to tree view.



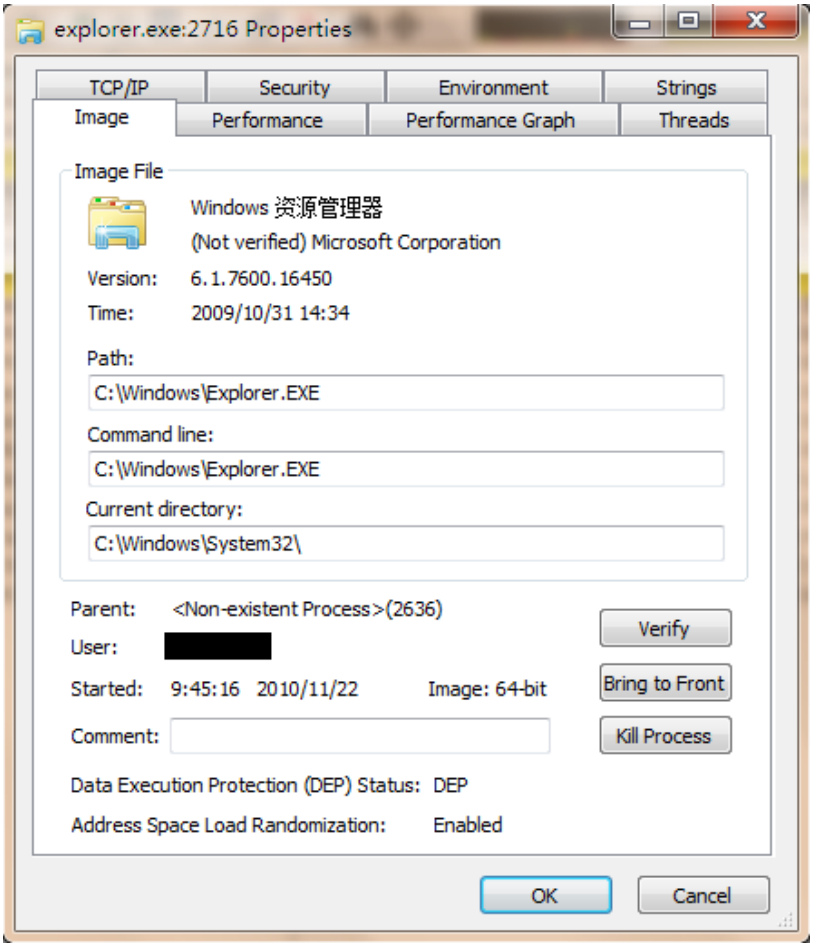
6. Deselect “View”, “Show Processes from All Users” to show only your processes.



7. Go to Options, Difference Highlight Duration, and change the value to 5 seconds. Then launch a new process (anything), and notice the new process highlighted in green for 5 seconds. Exit this new process, and notice the process is highlighted in red for 5 seconds before disappearing from the display. This can be useful to see processes being created and exiting on your system.

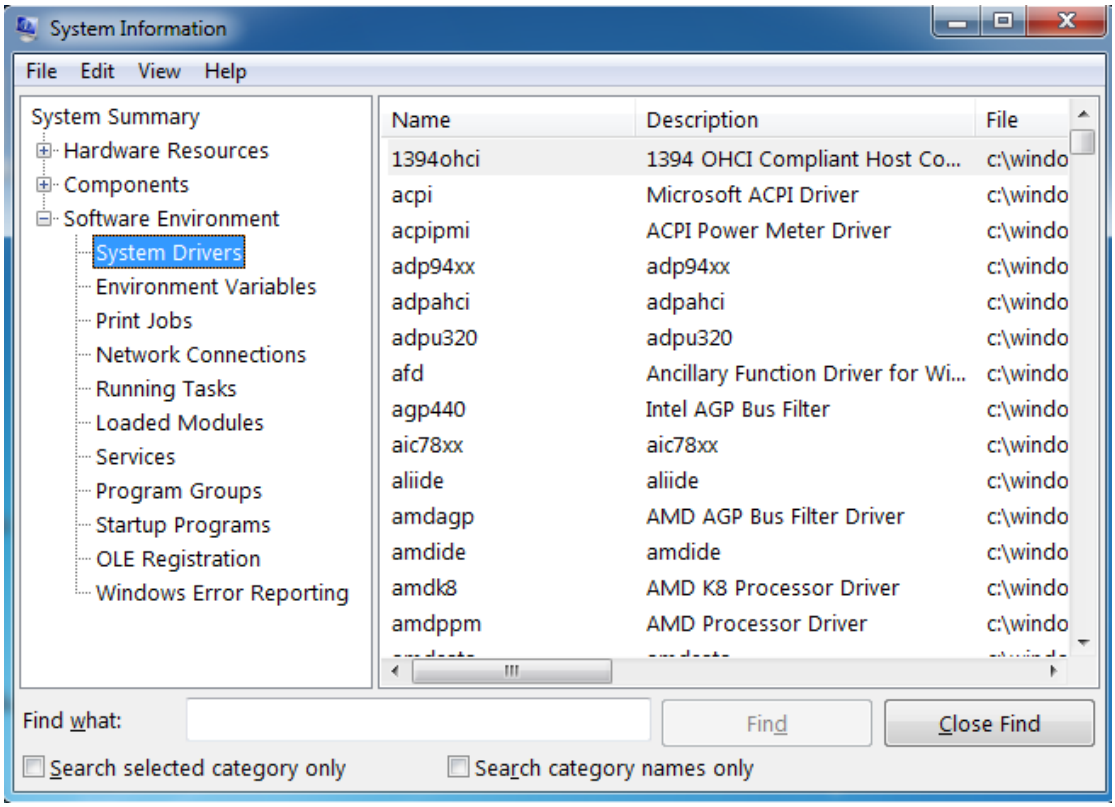


8. Finally, double-click on a process and explore the various tabs available from the process properties display. Check the information in all of the tabs.



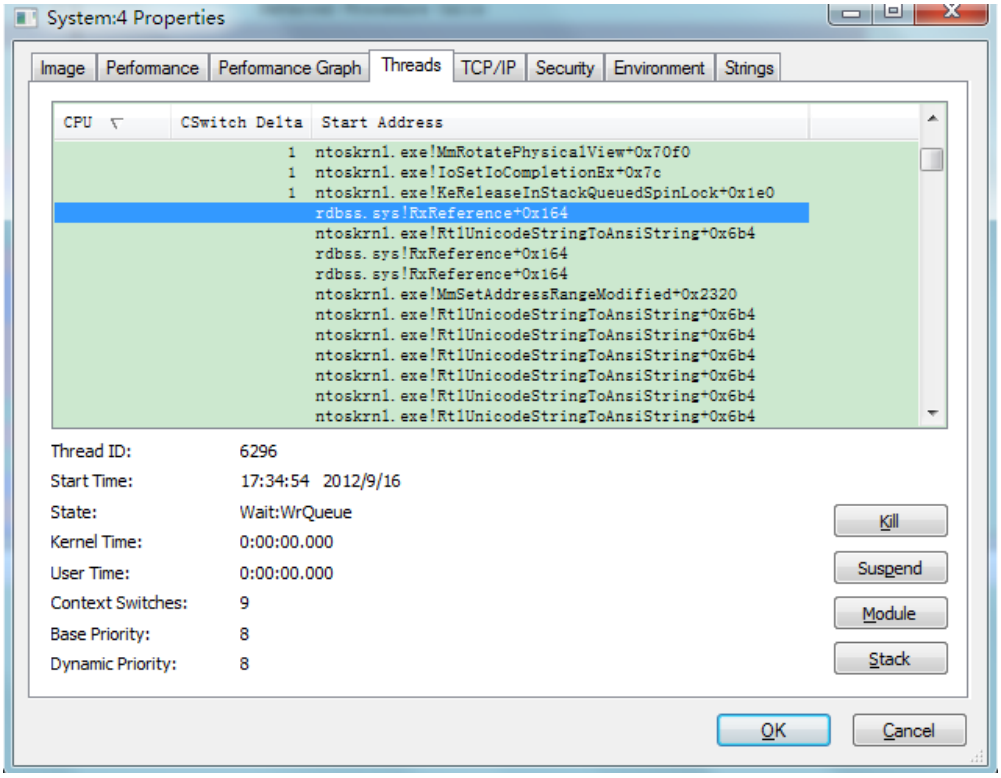
3. Viewing Installed drivers

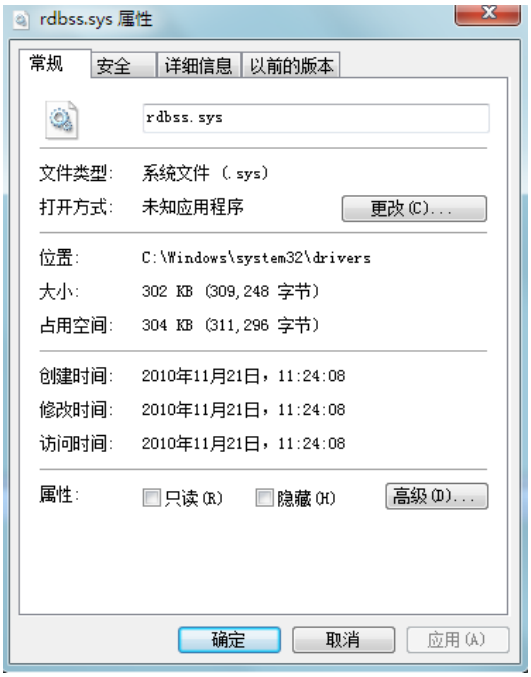
You can list the installed drivers by running Msinfo32.exe (click Start->Run and then enter Msinfo32). Then expand Software Environment and open System Drivers. In Msinfo32, you can view types, file path, status and many other information of an installed driver in your system.



4. Identifying System Threads in the System Process

In the Process Explorer, double click System process, and then click the Threads tab. You can find all the system threads in that tab. To see which driver creates a system thread, click that thread and then click Module button. Here is an example:


System:4 Properties
Image
Performance
Performance Graph
Threads
TCP/IP
Security
Environment
Strings
CPU
CSwitch Delta
Start Address
1 ntoskrnl.exe!MmRotatePhysicalView+0x70f0
1 ntoskrnl.exe!IoSetIoCompletionEx+0x7c
1 ntoskrnl.exe!KeReleaseInStackQueuedSpinLock+0x1e0
rdbss.sys!RxReference+0x164
ntoskrnl.exe!RtlUnicodeStringToAnsiString+0x6b4
rdbss.sys!RxReference+0x164
rdbss.sys!RxReference+0x164
ntoskrnl.exe!MmSetAddressRangeModified+0x2320
ntoskrnl.exe!RtlUnicodeStringToAnsiString+0x6b4
ntoskrnl.exe!RtlUnicodeStringToAnsiString+0x6b4
ntoskrnl.exe!RtlUnicodeStringToAnsiString+0x6b4
ntoskrnl.exe!RtlUnicodeStringToAnsiString+0x6b4
ntoskrnl.exe!RtlUnicodeStringToAnsiString+0x6b4
ntoskrnl.exe!RtlUnicodeStringToAnsiString+0x6b4
Thread ID: 6296
Start Time: 17:34:54 2012/9/16
State: Wait:WrQueue
Kernel Time: 0:00:00.000
User Time: 0:00:00.000
Context Switches: 9
Base Priority: 8
Dynamic Priority: 8
Kill
Suspend
Module
Stack
OK
Cancel


rdbss.sys 属性
常规
安全
详细信息
以前的版本
rdbss.sys
文件类型: 系统文件 (.sys)
打开方式: 未知应用程序
更改(C)...
位置: C:\Windows\system32\drivers
大小: 302 KB (309,248 字节)
占用空间: 304 KB (311,296 字节)
创建时间: 2010年11月21日，11:24:08
修改时间: 2010年11月21日，11:24:08
访问时间: 2010年11月21日，11:24:08
属性: 只读(R) 隐藏(H) 高级(D)...
确定
取消
应用(A)