## **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: Im vm nt

Check HAL information: Im 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.

Select Columns		-	? X
Process Memory Handle	DLL	. NET	Status Bar
Process Image	Proc	ess Perf	ormance
Select the columns that will appear on the Process view of Process Explorer.			
Process Name	- W	indow Title	
PID (Process Identifier)	- W	'indow Stat	tus
User Name	E Se	ession	
Description	Co	ommand Li	ne
Company Name	📃 Co	omment	
Verified Signer	D	EP Status	
Version	🔳 Int	tegrity Lev	el
Image Path	🔲 Vi	rtualized	
🔲 Image Type (64 vs 32-bit)	A.	SLR Enabl	ed
	Ē	确定	取消

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.

Difference Highlighting Duration		
Different Highlight Duration: 🚺 💌 second(s)		
OK Cancel		

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.

🗃 explorer.exe	e:2716 Properties			
TCP/IP	Security	Environment	Strings	
Image	Performance	Performance Graph	Threads	
- Image File -				
	Windows 资源管理器	2		
6-6	(Not verified) Micros	oft Corporation		
Version:	6.1.7600.16450			
Time:	2009/10/31 14:34			
Path:				
C:\Windo	ws\Explorer.EXE			
Command	Command line:			
C:\Windo	C:\Windows\Explorer.EXE			
Current di	rectory:			
C:\Windo	ows\System32\			
Parent:	<non-existent process<="" td=""><td>&gt;(2636)</td><td></td></non-existent>	>(2636)		
User:			Verify	
Started:	9:45:16 2010/11/22	Image: 64-bit	Bring to Front	
Comment:			Kill Process	
Data Execut	tion Protection (DEP) S	tatus: DEP		
Address Spa	ace Load Randomizatio	n: Enabled		
		ОК	Cancel	

# 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.

🦉 System Information				
File Edit View Help				
System Summary	Name	Description	File 🔺	
<ul> <li>Hardware Resources</li> <li>Components</li> <li>Software Environment</li> <li>System Drivers</li> <li>Environment Variables</li> <li>Print Jobs</li> <li>Network Connections</li> <li>Running Tasks</li> <li>Loaded Modules</li> </ul>	1394ohci acpi acpipmi adp94xx adpahci adpu320 afd agp440 aic78xx	1394 OHCI Compliant Host Co Microsoft ACPI Driver ACPI Power Meter Driver adp94xx adpahci adpu320 Ancillary Function Driver for Wi Intel AGP Bus Filter aic78xx	c:\windo c:\windo c:\windo c:\windo c:\windo c:\windo c:\windo c:\windo c:\windo	
Program Groups Startup Programs OLE Registration Windows Error Reporting	aliide amdagp amdide amdk8 amdppm	aliide AMD AGP Bus Filter Driver amdide AMD K8 Processor Driver AMD Processor Driver	c:\windo c:\windo c:\windo c:\windo c:\windo	
Find what:     Find     Close Find       Search selected category only     Search category names only				

## 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 Propertie	es	a house and	
Image Performance	Performance	Graph Threads TCP/IP Security Environment Strings	
CPU ∇ CSw:	itch Delta	Start Address	
	1 1 1	<pre>ntoskrn1. exe!MmRotatePhysicalView+0x70f0 ntoskrn1. exe!IoSetIoCompletionEx+0x7c ntoskrn1. exe!KeReleaseInStackQueuedSpinLock+0x1e0 rdbss.sys!RxReference+0x164 ntoskrn1. exe!RtlUnicodeStringToAnsiString+0x6b4 ntoskrn1. exe!RtEtAddressRangeModified+0x2320 ntoskrn1. exe!RtLUnicodeStringToAnsiString+0x6b4 ntoskrn1. exe!RtlUnicodeStringToAnsiString+0x6b4</pre>	
Thread ID:	6296		
Start Time:	17:34:54	2012/9/16	
State:	Wait:WrQ	lueue	Kill
Kernel Time:	0:00:00.0		Suggard
User Time:	0:00:00.0	00	Suspenu
Context Switches:	9		Module
Base Priority:	8		Stade
Dynamic Priority:	8	<u> </u>	<u>C</u> ancel

i rdbss.sys 届	
常规安全	: 详细信息 以前的版本
2	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)
	<b>确定 取消</b> 应用 (A)