Windows Internals 7ed part1

9780735684188

|  |  |
| --- | --- |
| PAGE # | Errata |
| 1 | Location on page: Under "Windows operating system versions" titleReads:This book covers the most recent version of the Microsoft Windows client and server operating systems: Windows 10 (32-bit on x86 and ARM, and 64-bit version on x64) and Windows Server 2012 R2 (which exists as 64-bit version only).Should read:This book covers the most recent version of the Microsoft Windows client and server operating systems: Windows 10 (32-bit on x86 and ARM, and 64-bit version on x64) and Windows Server 2016 (which exists as 64-bit version only). |
| 2 | From Pavel, authorLocation: Note – last sentenceReads:(See Chapter 8, “System mechanisms,” in Windows Internals Part 2 for details.)Should read:(See the section “Image Loader,” in Chapter 3 for details.) |
| 11 | Location on page: Last paragraph on page 10Currently Reads:Each process also points to its parent or creator process (which may be, but is not always, its creator process). Should read:Each process also points to its parent (which may be, but is not always, its creator process). |
| 18 | Location on page: Second to last paragraph on page 18 and first note on page 19Reads:The volatile registers, stacks, and private storage area are called the thread’s context. Because thisinformation is different for each machine architecture that Windows runs on, this structure, by necessity,is architecture-specific. The Windows GetThreadContext function provides access to this architecturespecificinformation (called the CONTEXT block).Should read: (Replace entire paragraph with the following)The volatile and non-volatile registers as well as a private storage area are called the thread’s context. Because this information is different for each machine architecture that Windows runs on, this structure, by necessity, is architecture-specific. The Windows GetThreadContext function provides access to this architecture specific information (called the CONTEXT block). Additionally, each thread has its own stack as well (pointed to by a stack register part of the thread’s context)." |
| 19 | Location on page: first NoteReads: "Wow64 (Windows on Windows)" Should Read:"Wow64 (Windows on Windows 64-bit)". |
| 26 | Location on page: top, step 3Reads:press the **Suppr** key on the keyboard.Should Read: press the **Delete** key on the keyboard. |
| 31 | Location on page: top ½ of pageReads:"Objects and handles (references to instances of an object) are discussed in more detail in Chapter 8 in Part 2."Should read:"Objects and handles (references to objects) are discussed in more detail in Chapter 8 in Part 2." |
| 54 | Location on page: topReads: There are six different versions of Windows Server 2016: Windows Server 2016 Datacenter, WindowsServer 2016 Standard, Windows Server 2016 Essentials, Windows Server 2006 MultiPoint PremiumServer, Windows Storage Server 2016, and Microsoft Hyper-V Server 2016.Should read:There are six different versions of Windows Server 2016: Windows Server 2016 Datacenter, WindowsServer 2016 Standard, Windows Server 2016 Essentials, Windows Server 2016 MultiPoint PremiumServer, Windows Storage Server 2016, and Microsoft Hyper-V Server 2016. |
| 73 | Location on page: top 4th bullet pointDescription of error: "These include internal support functions called within Ntoskrnl.dll"It should say: "These include internal support functions called within Ntoskrnl.exe". |
| 81 | Location on page: Ksigningpolicy contractDescription of error: "processes on certain SKUs or FUTHER configure Device Guard"Should read:"processes on certain SKUs or FURTHER configure Device Guard" |
| 115 | Location on page: middle, the word Process is missing the CReads: PROESS\_QUERY Should Read:PROCESS\_QUERY |
| 116 | Location on page: middleReads:two special enhanced key usage (EKU) OIDs that can be encoded in a digital code signing certificate: 1.3.6.1.4.1.311.10.3.22 and 1.3.6.4.1.311.10.3.20.Should read:two special enhanced key usage (EKU) OIDs that can be encoded in a digital code signing certificate: 1.3.6.1.4.1.311.10.3.22 and 1.3.6.1.4.1.311.10.3.20." |
| 123 | Location on page: bottomReads "Isolated User Mode EKU (1.3.6.1.4.311.10.3.37)." Should Read:"Isolated User Mode EKU (1.3.6.1.4.1.311.10.3.37)." |
| 167 | Location on page: bottomDescription of error: – replace all instances of PsActiveModuleList with PsLoadedModuleList and replace the entire code line in the last sentence of the paragraph.Reads:Likewise, the kernel-mode loader has its own database of such entries, which is directly accessible through the PsActiveModuleList global data variable. To dump the kernel’s loaded module database, you can use a similar !list command as shown in the preceding experiment by replacing the pointer at the end of the command with nt!PsActiveModuleList and using the new structure/module name: !list nt!\_KLDR\_DATA\_TABLE\_ENTRY nt!PsActiveModuleList. Should read Likewise, the kernel-mode loader has its own database of such entries, which is directly accessible through the PsLoadedModuleList global data variable. To dump the kernel’s loaded module database, you can use a similar !list command as shown in the preceding experiment by replacing the pointer at the end of the command with nt! PsLoadedModuleList and using the new structure/module name: !list -x " dt nt!\_kldr\_data\_table\_entry" nt!PsLoadedModuleList  |
| 167 | Location on page: Middle bullet 3.Description of error: Command is Syntactically Incorrect and does not work. In the book the dash ended up as a long ‘em’ dash vs the regular dash.!list –x "dt ntdll!\_LDR\_DATA\_TABLE\_ENTRY" @@C++(&@$peb->Ldr->InLoadOrderModuleList)The correct Command should be regular dash in front of the x!list -x "dt ntdll!\_LDR\_DATA\_TABLE\_ENTRY" @@C++(&@$peb->Ldr->InLoadOrderModuleList) |
| 216 | Location on page: bottomReads:earlier, which sets priorities of 4, 8, 13, 14, 6, and 10, respectively.Should read:earlier, which sets priorities of 4, 8, 13, 24, 6, and 10, respectively. |
| 221 | Location on page: bottom of 221, step 13Reads:Note that you can also make this change in Process Manager.)Should Read:Note that you can also make this change in Process Explorer.) |
| 424 | Description of error: In the "Memory Notification Events" section, just after table 5-18 there is a note and the registry key is wrong.Reads:You can override the high and low memory values by adding the LowMemoryThreshold or HighMemoryThreshold DWORD registry value under HKLM\SYSTEM\CurrentControlSet\Session Manager\Memory Management.Should Read:You can override the high and low memory values by adding the LowMemoryThreshold or HighMemoryThreshold DWORD registry value under HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management |
| 509 | Location on page: first paragraphReads:The following command reports information on the highlighted handle (handle value 0xD4) in the preceding screenshot, which is in the Dwm.exe process that has a process ID of 452 decimal:Should read:The following command reports information on the highlighted handle (handle value 0x348) in the preceding screenshot, which is in the Dwm.exe process that has a process ID of 452 decimal: |
| 551 | Location on page:  bottomBullet #4Reads:■ IoPagingReadLowPriorityBumpedCount and IoPagingWriteHighPriorityBumpedCountShould read:■ IoPagingReadLowPriorityBumpedCount and IoPagingWriteLowPriorityBumpedCount |
| 600 | Location on page: bottumReads:When a driver decides that a component should change performance state, it calls PoFxIssuePerfStateChange or PoFxIssuePerfStateChangeMultiple. Should read:When a driver decides that a component should change performance state, it calls PoFxIssueComponentPerfStateChange or PoFxIssueComponentPerfStateChangeMultiple. |
| 734 | Location on page: Table 7-18 and first paragraphDescription of error: Beginning in Windows 8, the UAC slider doesn't turn off UAC completely anymore. Turning off UAC is no longer supportable with the new AppContainer model, so the slider won't do that.Reads:The lowest position is strongly discouraged because it turns UAC off completely as far as administrativeaccounts are concerned. All processes run by a user with an administrative account will be run withthe user’s full administrative rights in effect; there is no filtered admin token. Registry and file systemvirtualization are disabled as well for these accounts, and the Protected mode of Internet Explorer isdisabled. However, virtualization is still in effect for non-administrative accounts, and non-administrativeaccounts will still see an OTS elevation prompt when they attempt to change Windows settings, run aprogram that requires elevation, or use the Run as Administrator context menu option in Explorer.Should read: (replace entire paragraph)The lowest position is strongly discouraged because it turns UAC off completely as far as administrativeaccounts are concerned. Prior to Windows 8, all processes run by a user with an administrative account are run withthe user’s full administrative rights in effect; there is no filtered admin token. Starting with Windows 8, UAC cannot be turned off completely, because of the AppContainer model. Admin users won’t be prompted for elevation, but processes will not elevate unless required to do so by the manifest or launched from an elevated process. |