#### [Windows XP] Device Information in Registry

Contact: junhyeong.lee@plainbit.co.kr, http://maj3sty.tistory.com

Information	Path	Comments	
Vendor Name Product Name Device Firmware- Version	HKLM\SYSTEM\ControlSet00#\Enum\USBSTOR\Disk&Ven_ <vendor name="">&amp;Prod_<product name=""> &amp;Rev_<device firmware="" version=""></device></product></vendor>		
Vendor ID Product ID	HKLM\SYSTEM\ControlSet00#\Enum\USB\VID_ <vendor id="">&amp;PID_<product id=""></product></vendor>		
ParentIDPrefix	HKLM\SYSTEM\ControlSet00#\Enum\USBSTOR\ <device class="" id="">\ParentIdPrefix</device>	ParentIdPrefix는 Value이다.	
Device Serial-	HKLM\SYSTEM\ControlSet00#\Enum\USB\ <vendor &="" id="" product="">\<device number="" serial=""></device></vendor>		
Number	HKLM\SYSTEM\ControlSet00#\Enum\USBSTOR\ <device class="" id="">\<device number="" serial="">&amp;#&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;HKLM\System\MountedDevices&lt;/td&gt;&lt;td&gt;ParentIdPrefix를 해당 키에서 검색하여&lt;br&gt;매칭&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Drive Letter&lt;/td&gt;&lt;td&gt;HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\&lt;Device Entry&gt;\FriendlyName&lt;/td&gt;&lt;td rowspan=2 colspan=2&gt;─ FriendlyName는 Value이다.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;HKLM\System\ControlSet00#\Enum\WpdBusEnumRoot\UMB\&lt;Device Entry&gt;\FriendlyName&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Volume GUID&lt;/td&gt;&lt;td&gt;HKLM\SYSTEM\MountedDevices\\??\Volume&lt;Volume GUID&gt;&lt;/td&gt;&lt;td&gt;ParentIdPrefix를 해당 키에서 검색하여&lt;br&gt;매칭&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;User Name&lt;/td&gt;&lt;td&gt;HKU\&lt;USER&gt;\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\&lt;Volume GUID&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;First Connection-&lt;br&gt;Time&lt;/td&gt;&lt;td&gt;%SystemRoot%\Setupapi.log&lt;/td&gt;&lt;td&gt;장치를 최초를 연결한 시간이다.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}\&lt;Sub Keys&gt;&lt;/td&gt;&lt;td&gt;해당 시간은 각 키의 Last Written Time이&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td rowspan=2&gt;First Connection-&lt;br&gt;Time After&lt;br&gt;Booting&lt;/td&gt;&lt;td&gt;HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{53F5630D-B6BF-11D0-94F2-00A0C91EFB8B}\&lt;Sub Keys&gt;&lt;/td&gt;&lt;td colspan=2&gt;다.&lt;br&gt;다.&lt;br&gt;해당 시간은 컴퓨터 부팅 후 장치를 연결한 시&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{A5DCBF10-6530-11D2-901F-00C04FB951ED}\&lt;Sub Keys&gt;&lt;/td&gt;&lt;td&gt;각이다.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Last Connection-&lt;br&gt;Time&lt;/td&gt;&lt;td&gt;HKU\&lt;USER&gt;\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\&lt;Volume GUID&gt;&lt;/td&gt;&lt;td&gt;Last Connection Time은 각 키의 Last&lt;br&gt;Written Time이다.&lt;/td&gt;&lt;/tr&gt;&lt;/tbody&gt;&lt;/table&gt;</device></device>		

### [Windows Vista] Device Information in Registry

Information	Path	Comments
Vendor Name Product Name Device Firmware- Version	HKLM\SYSTEM\ControlSet00#\Enum\USBSTOR\Disk&Ven_ <vendor name="">&amp;Prod_<product name=""> &amp;Rev_<device firmware="" version=""></device></product></vendor>	
Vendor ID Product ID	HKLM\SYSTEM\ControlSet00#\Enum\USB\VID_ <vendor id="">&amp;PID_<product id=""></product></vendor>	
Device Serial-	HKLM\SYSTEM\ControlSet00#\Enum\USB\ <vendor &="" id="" product="">\<device number="" serial=""></device></vendor>	
Number	HKLM\SYSTEM\ControlSet00#\Enum\USBSTOR\ <device class="" id="">\<device number="" serial="">&amp;#&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;Volume Serial-&lt;br&gt;Number&lt;br&gt;Volume Label&lt;/th&gt;&lt;td&gt;HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt\_??_USBSTOR#&lt;Device Class ID&gt; #&lt;Unique Instance ID&gt;#&lt;GUID&gt;&lt;Volume Label&gt;_&lt;Volume Serial Number&gt;&lt;/td&gt;&lt;td&gt;- XP 버전 이후 새로 추가 됨&lt;br&gt;- EMDMgmt SubKey는 일반적으로 생성되지 않&lt;br&gt;음&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;Volume Label&lt;/th&gt;&lt;td&gt;HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt\_??_USBSTOR#&lt;Device Class ID&gt; #&lt;Unique Instance ID&gt;#&lt;GUID&gt;&lt;Volume Label&gt;_&lt;Volume Serial Number&gt;&lt;/td&gt;&lt;td&gt;- EMDMgmt SubKey는 일반적으로 생성되지 않음&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;volume Label&lt;/th&gt;&lt;td&gt;HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\&lt;Device Entry&gt;\FriendlyName&lt;/td&gt;&lt;td&gt;- FriendlyName는 Value이다.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;Drive Letter&lt;/th&gt;&lt;td&gt;HKLM\System\MountedDevices&lt;/td&gt;&lt;td&gt;- ParentIdPrefix를 해당 키에서 검색&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;Drive Letter&lt;/th&gt;&lt;td&gt;HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\&lt;Device Entry&gt;\FriendlyName&lt;/td&gt;&lt;td&gt;- FriendlyName는 Value이다.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;Volume GUID&lt;/th&gt;&lt;th&gt;HKLM\SYSTEM\MountedDevices\\??\Volume&lt;Volume GUID&gt;&lt;/th&gt;&lt;th&gt;- Device Serial Number를 해당 키에서&lt;br&gt;검색하여 매칭&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;User Name&lt;/th&gt;&lt;th&gt;HKU\&lt;USER&gt;\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\&lt;Volume GUID&gt;&lt;/th&gt;&lt;th&gt;&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;&lt;/th&gt;&lt;th&gt;%SystemRoot%\Setupapi.log&lt;/th&gt;&lt;th&gt;- 장치를 최초로 연결한 시간이다.&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td rowspan=2&gt;First Connection-&lt;br&gt;Time&lt;/td&gt;&lt;td&gt;HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt\&lt;Device Entry&gt;&lt;/td&gt;&lt;td&gt;- 해당 시간은 각 키의 Last Written Time이다.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\&lt;Device Entry&gt;&lt;/td&gt;&lt;td&gt; HKLM 하이브의 Key는 Windows XP 버전 이&lt;br&gt;후 새로 추가 됨&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;First Connection-&lt;br&gt;Time After&lt;/th&gt;&lt;td&gt;HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}\&lt;Sub Keys&gt;&lt;/td&gt;&lt;td&gt;- 해당 시간은 각 키의 Last Written Time이다.&lt;/td&gt;&lt;/tr&gt;&lt;/tbody&gt;&lt;/table&gt;</device></device>	

Booting	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{53F5630D-B6BF-11D0-94F2-00A0C91EFB8B}\ <sub keys=""></sub>	- 해당 시간은 컴퓨터 부팅 후 장치를 연결한 시각이다.
	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{6AC27878-A6FA-4155-BA85-F98F491D4F33}\ <sub keys=""></sub>	- {6AC27878-A6FA-4155-BA85- F98F491D4F33} Key는 XP 버전 이후 새로 추 가 됨
	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{A5DCBF10-6530-11D2-901F-00C04FB951ED}\ <sub keys=""></sub>	- WpdBusEnumRoot Key는 Windows XP 버전 이후 새로 추가 됨
	HKLM\SYSTEM\ControlSet00#\Enum\WpdBusEnumRoot\UMB\ <device entry=""></device>	>
Last Connection-	HKU\ <user>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\<volume guid=""></volume></user>	- Last Connection Time은 각 키의 Last Written Time이다.
Time	HKLM\SYSTEM\ControlSet00#\Enum\WpdBusEnumRoot\UMB\ <device entry="">\Device Parameters</device>	- Device Parameters Key는 Windows XP 버 전 이후 새로 추가 됨

# [Windows 7 / 8] Device Information in Registry

Information	Path	Comments
Vendor Name Product Name Device Firmware- Version	HKLM\SYSTEM\ControlSet00#\Enum\USBSTOR\Disk&Ven_ <vendor name="">&amp;Prod_<product name=""> &amp;Rev_<device firmware="" version=""></device></product></vendor>	
Vendor ID Product ID	HKLM\SYSTEM\ControlSet00#\Enum\USB\VID_ <vendor id="">&amp;PID_<product id=""></product></vendor>	
Device Serial-	HKLM\SYSTEM\ControlSet00#\Enum\USB\ <vendor &="" id="" product="">\<device number="" serial=""></device></vendor>	
Number	HKLM\SYSTEM\ControlSet00#\Enum\USBSTOR\ <device class="" id="">\<device number="" serial="">&amp;#&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;Volume Serial-&lt;br&gt;Number&lt;br&gt;Volume Label&lt;/th&gt;&lt;th&gt;HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt\_??_USBSTOR#&lt;Device Class ID&gt; #&lt;Unique Instance ID&gt;#&lt;GUID&gt;&lt;Volume Label&gt;_&lt;Volume Serial Number&gt;&lt;/th&gt;&lt;th&gt;- EMDMgmt SubKey는 일반적으로 생성되지 않음&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;&lt;/th&gt;&lt;th&gt;HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt\_??_USBSTOR#&lt;Device Class ID&gt; #&lt;Unique Instance ID&gt;#&lt;GUID&gt;&lt;Volume Label&gt;_&lt;Volume Serial Number&gt;&lt;/th&gt;&lt;th&gt;- EMDMgmt SubKey는 일반적으로 생성되지 않음&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;Volume Label&lt;/th&gt;&lt;td&gt;HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\&lt;Device Entry&gt;\FriendlyName&lt;/td&gt;&lt;td rowspan=2 colspan=2&gt;- FriendlyName는 Value이다.&lt;br&gt;- WpdBusEnumRoot Key는 Vista 버전 이후어&lt;br&gt;Volume Label 추가 정보 획득 가능&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;&lt;/th&gt;&lt;td&gt;HKLM\System\ControlSet00#\Enum\WpdBusEnumRoot\UMB\&lt;Device Entry&gt;\FriendlyName&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;&lt;/th&gt;&lt;td&gt;HKLM\System\MountedDevices&lt;/td&gt;&lt;td&gt;- Device Serial Number를 해당 키에서 검&lt;br&gt;색&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;Drive Letter&lt;/th&gt;&lt;td&gt;HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\&lt;Device Entry&gt;\FriendlyName&lt;/td&gt;&lt;td&gt;- FriendlyName는 Value이다.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;&lt;/th&gt;&lt;td&gt;HKLM\System\ControlSet00#\Enum\WpdBusEnumRoot\UMB\&lt;Device Entry&gt;\FriendlyName&lt;/td&gt;&lt;td&gt;- FriendlyName는 Value이다.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;Volume GUID&lt;/th&gt;&lt;th&gt;HKLM\SYSTEM\MountedDevices\\??\Volume&lt;Volume GUID&gt;&lt;/th&gt;&lt;th&gt;- Device Serial Number를 해당 키에서&lt;br&gt;검색하여 매칭&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;User Name&lt;/th&gt;&lt;th&gt;HKU\&lt;USER&gt;\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\&lt;Volume GUID&gt;&lt;/th&gt;&lt;th&gt;&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;First Connection-&lt;/th&gt;&lt;th&gt;%SystemRoot%\Setupapi.log&lt;/th&gt;&lt;th&gt;- 장치를 최초로 연결한 시간이다.&lt;br&gt;- 해당 시간은 각 키의 Last Written Time이&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;Time&lt;/th&gt;&lt;td&gt;HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt\&lt;Device Entry&gt;&lt;/td&gt;&lt;td&gt;다.&lt;br&gt;- Setupapi.log는 운영체제가 필요에 의해 이&lt;/td&gt;&lt;/tr&gt;&lt;/tbody&gt;&lt;/table&gt;</device></device>	

	·		
	HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\ <device entry=""></device>	전 기록을 압축해 보관하고 새로운 Setupapi.log로 기록을 생성할 때가 있음(파	
	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{10497B1B-BA51-44E5-8318-A65C837B6661}\ <sub keys=""></sub>	일명 ex: Setupapi_ <date>.log) - {10497B1B-BA51-44E5-8318-A65C837B6661} Key는 Vista 이후 버전에서 새로 추가 됨</date>	
	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}\ <sub keys=""></sub>	<b>&gt;</b>	
First Connection- Time After Booting	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{53F5630D-B6BF-11D0-94F2-00A0C91EFB8B}\ <sub keys=""></sub>	- 해당 시간은 각 키의 Last Written Time이다 해당 시간은 컴퓨터 부팅 후 장치를 연결한시각이다.	
	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{6AC27878-A6FA-4155-BA85-F98F491D4F33}\ <sub keys=""></sub>		
	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{A5DCBF10-6530-11D2-901F-00C04FB951ED}\ <sub keys=""></sub>		
	HKLM\SYSTEM\ControlSet00#\Enum\WpdBusEnumRoot\UMB\ <device entry=""></device>		
Last Connection- Time	HKU\ <user>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\<volume guid=""></volume></user>	- Last Connection Time은 각 키의 Last	
	HKLM\SYSTEM\ControlSet00#\Enum\WpdBusEnumRoot\UMB\ <device entry="">\Device Parameters</device>	Written Time이다.	

## [Windows 7 / 8] Device Information in <a href="Event Log">Event Log</a>

Information	Path	Event ID	Comments
Connection Time Verdor Name Device Model Device Serial Number	<pre>%SystemRoot%\System32\winevt\Logs\ Microsoft-Windows-DriverFrameworks-UserMode%40perational.evtx</pre>	2003 2004 2005 2010	LifetimeID 값을 이용하면 동일 저장장치의
Disconnection Time Verdor Name Device Model Device Serial Number	<pre>%SystemRoot%\System32\winevt\Logs\ Microsoft-Windows-DriverFrameworks-UserMode%40perational.evtx</pre>	2102	연결/해제 이벤트를 파악할 수 있다. 하지만 이 값은 절대적이지 않다.
MTP Device Connection - Time MTP Device Name(Type)	<pre>%SystemRoot%\System32\winevt\Logs\ Microsoft-Windows-WPD2)-MTPClassDriver%40perational.evtx</pre>	1005	MTP 장치가 하나만 연결되어 있다면 연결/해저 쌍을 파악할 수 있지만, 여러 개 연결되어 있는 경우 연결/해제 쌍을 파악하기 힘들다.
MTP Device - Disconnection Time	%SystemRoot%\System32\winevt\Logs\ Microsoft-Windows-WPD2)-MTPClassDriver%4Operational.evtx	1002	

### [Windows 10] Device Information in Registry

Information	Path	Comments
Vendor Name Product Name Device Firmware- Version	<pre>HKLM\SYSTEM\ControlSet00#\Enum\USBSTOR\Disk&amp;Ven_<vendor name="">&amp;Prod_<product name=""> &amp;Rev_<device firmware="" version=""></device></product></vendor></pre>	
Vendor ID Product ID	HKLM\SYSTEM\ControlSet00#\Enum\USB\VID_ <vendor id="">&amp;PID_<product id=""></product></vendor>	
Device Serial-	HKLM\SYSTEM\ControlSet00#\Enum\USB\ <vendor &="" id="" product="">\<device number="" serial=""></device></vendor>	
Number	HKLM\SYSTEM\ControlSet00#\Enum\USBSTOR\ <device class="" id="">\<device number="" serial="">&amp;#&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;Volume Serial-&lt;br&gt;Number&lt;br&gt;Volume Label&lt;/th&gt;&lt;td&gt;&lt;pre&gt;HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt\_??_USBSTOR#&lt;Device Class ID&gt; #&lt;Unique Instance ID&gt;#&lt;GUID&gt;&lt;Volume Label&gt;_&lt;Volume Serial Number&gt;&lt;/pre&gt;&lt;/td&gt;&lt;td&gt;- EMDMgmt SubKey는 일반적으로 생성되지 않음&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;&lt;/th&gt;&lt;td&gt;HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt\_??_USBSTOR#&lt;Device Class ID&gt; #&lt;Unique Instance ID&gt;#&lt;GUID&gt;&lt;Volume Label&gt;_&lt;Volume Serial Number&gt;&lt;/td&gt;&lt;td&gt;- EMDMgmt SubKey는 일반적으로 생성되지 않음&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;Volume Label&lt;/th&gt;&lt;td&gt;HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\&lt;Device Entry&gt;\FriendlyName&lt;/td&gt;&lt;td rowspan=2 colspan=2&gt;- FriendlyName는 Value이다.&lt;br&gt;- WpdBusEnumRoot Key는 Vista 버전 이후에&lt;br&gt;Volume Label 추가 정보 획득 가능&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;volume Label&lt;/th&gt;&lt;td&gt;HKLM\System\ControlSet00#\Enum\WpdBusEnumRoot\UMB\&lt;Device Entry&gt;\FriendlyName&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;&lt;/th&gt;&lt;td&gt;HKLM\SOFTWARE\Microsoft\Windows Search\VolumeInfoCache\&lt;Sub Keys&gt;&lt;/td&gt;&lt;td&gt;- Windows 10에서 새로 추가 됨&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;&lt;/th&gt;&lt;td&gt;HKLM\System\MountedDevices&lt;/td&gt;&lt;td&gt;- Device Serial Number를 해당 키에서 검&lt;br&gt;색&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;Pains Letter&lt;/th&gt;&lt;td&gt;HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\&lt;Device Entry&gt;\FriendlyName&lt;/td&gt;&lt;td rowspan=2 colspan=2&gt; FriendlyName는 Value이다.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td rowspan=2&gt;Drive Letter&lt;/td&gt;&lt;td&gt;HKLM\System\ControlSet00#\Enum\WpdBusEnumRoot\UMB\&lt;Device Entry&gt;\FriendlyName&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;HKLM\SOFTWARE\Microsoft\Windows Search\VolumeInfoCache\&lt;Sub Keys&gt;&lt;/td&gt;&lt;td&gt;- Windows 10에서 새로 추가 됨&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;Volume GUID&lt;/th&gt;&lt;td&gt;HKLM\SYSTEM\MountedDevices\\??\Volume&lt;Volume GUID&gt;&lt;/td&gt;&lt;td&gt;- Device Serial Number를 해당 키에서&lt;br&gt;검색하여 매칭&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;User Name&lt;/th&gt;&lt;td&gt;HKU\&lt;USER&gt;\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\&lt;Volume GUID&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;/tbody&gt;&lt;/table&gt;</device></device>	

	%SystemRoot%\Setupapi.log	- 장치를 최초로 연결한 시간이다. - 해당 시간은 각 키의 Last Written Time이	
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt\ <device entry=""></device>	다. - Setupapi.log는 운영체제가 필요에 의해 이	
First Connection- Time	HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\ <device entry=""></device>	전         기록을         압축해         보관하고         새로운           Setupapi.log로         기록을         생성할         때가         있음(파	
	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{10497B1B-BA51-44E5-8318-A65C837B6661}\ <sub keys=""></sub>	일명 ex: Setupapi_ <date>.log) - {10497B1B-BA51-44E5-8318- A65C837B6661} Key는 Vista 이후 버전에서 새로 추가 됨</date>	
	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}\ <sub keys=""></sub>	- 해당 시간은 각 키의 Last Written Time이다. - 해당 시간은 컴퓨터 부팅 후 장치를 연결한	
	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{53F5630D-B6BF-11D0-94F2-00A0C91EFB8B}\ <sub keys=""></sub>		
First Connection- Time After Booting	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{6AC27878-A6FA-4155-BA85-F98F491D4F33}\ <sub keys=""></sub>		
	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{A5DCBF10-6530-11D2-901F-00C04FB951ED}\ <sub keys=""></sub>	시각이다.	
	HKLM\SYSTEM\ControlSet00#\Enum\WpdBusEnumRoot\UMB\ <device entry=""></device>		
Last Connection- Time	HKU\ <user>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\<volume guid=""></volume></user>	- Last Connection Time은 각 키의 Last	
	HKLM\SYSTEM\ControlSet00#\Enum\WpdBusEnumRoot\UMB\ <device entry="">\Device Parameters</device>	Written Time이다.	

### [Windows 10] Device Information in <u>Event Log</u>

Information	Path	Event ID	Comments
Connection Time Vendor Name	<pre>%SystemRoot%\System32\winevt\Logs\ Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx</pre>	2003 2004 2005 2010	- LifetimeID 값을 이용하면 동일 저장장치의 연결/해제 이벤트를 파악할 수 있다. 하지만 이
Device Model Device Serial Number	<pre>%SystemRoot%\System32\winevt\Logs\ Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx</pre>	2102	값은 절대적이지 않다. - 기본 설정이 '비활성화'이다.
Device Model Device Capacity Device Serial Number MBR, VBR Raw Data DeviceGUID	<pre>%SystemRoot%\System32\winevt\Logs\ Microsoft-Windows-Partition%4Diagnostic.evtx</pre>	1006	- 연결/해제 이벤트가 명확하지 않다. 이벤트 로그 연관 분석을 통해 연결/해제 이벤트 가능 성이 높은 것을 추릴 순 있지만 정확하지 않다.
Connection Time Disconnection Time, Vendor Name Product Name Device Serial Number	%SystemRoot%\System32\winevt\Logs\Security.evtx	6416 6419 6420 6421 6422 6423 6424	- 감사 설정 중 "PNP 활동 감사" 항목을 활성 화 해야 로깅된다.
Connection Time DeviceGUID	<pre>%SystemRoot%\System32\winevt\Logs\ Microsoft-Windows-Storage-ClassPnP%4Operational.evtx</pre>	512	- DeviceGUID 값을 Microsoft-Windows- Partition%4Diagnostic.evtx 이벤트와 매 칭시켜 장치 정보를 획득한다.
MTP Device Connection - Time MTP Device Name(Type)	<pre>%SystemRoot%\System32\winevt\Logs\ Microsoft-Windows-WPD2)-MTPClassDriver%4Operational.evtx</pre>	1005	MTP 장치가 하나만 연결되어 있다면 연결/해제 쌍을 파악할 수 있지만, 여러 개 연결되어 있는 경우 연결/해제 쌍을 파악하기 힘들다.

MTP Device - Disconnection Time	<pre>%SystemRoot%\System32\winevt\Logs\ Microsoft-Windows-WPD2)-MTPClassDriver%40perational.evtx</pre>	1002	

