[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>&Prod_<Product Name>&Rev_<Device Firmware Version>	
Vendor ID **Product ID**	HKLM\SYSTEM\ControlSet00#\Enum\USB\VID_<Vendor ID>&PID_<Product ID>	
ParentIDPrefix	HKLM\SYSTEM\ControlSet00#\Enum\USBSTOR\<Device Class ID>\ParentIdPrefix	ParentIdPrefix는 Value이다.
Device Serial-Number	HKLM\SYSTEM\ControlSet00#\Enum\USB\<Vendor ID & Product ID>\<Device Serial Number>	
	HKLM\SYSTEM\ControlSet00#\Enum\USBSTOR\<Device Class ID>\<Device Serial Number>&#	
Drive Letter	HKLM\System\MountedDevices	ParentIdPrefix를 해당 키에서 검색하여 매칭
	HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\<Device Entry>\FriendlyName	FriendlyName는 Value이다.
	HKLM\System\ControlSet00#\Enum\WpdBusEnumRoot\UMB\<Device Entry>\FriendlyName	
Volume GUID	HKLM\SYSTEM\MountedDevices\\??\Volume<Volume GUID>	ParentIdPrefix를 해당 키에서 검색하여 매칭
User Name	HKU\<USER>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\<Volume GUID>	
First Connection-Time	*%SystemRoot%*\Setupapi.log	장치를 최초를 연결한 시간이다.
First Connection-Time After Booting	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}\<Sub Keys>	해당 시간은 각 키의 Last Written Time이다. 해당 시간은 컴퓨터 부팅 후 장치를 연결한 시각이다.
	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{53F5630D-B6BF-11D0-94F2-00A0C91EFB8B}\<Sub Keys>	
	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{A5DCBF10-6530-11D2-901F-00C04FB951ED}\<Sub Keys>	
Last Connection-Time	HKU\<USER>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\<Volume GUID>	Last Connection Time은 각 키의 Last Written Time이다.

[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>&Prod_<Product Name> &Rev_<Device Firmware Version>	
Vendor ID Product ID	HKLM\SYSTEM\ControlSet00#\Enum\USB\VID_<Vendor ID>&PID_<Product ID>	
Device Serial-Number	HKLM\SYSTEM\ControlSet00#\Enum\USB\<Vendor ID & Product ID>\<Device Serial Number>	
	HKLM\SYSTEM\ControlSet00#\Enum\USBSTOR\<Device Class ID>\<Device Serial Number>&#	
Volume Serial-Number Volume Label	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt_??_USBSTOR#<Device Class ID> #<Unique Instance ID>#<GUID><Volume Label>_<Volume Serial Number>	- XP 버전 이후 새로 추가 됨 - EMDMgmt SubKey는 일반적으로 생성되지 않음
Volume Label	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt_??_USBSTOR#<Device Class ID> #<Unique Instance ID>#<GUID><Volume Label>_<Volume Serial Number>	- EMDMgmt SubKey는 일반적으로 생성되지 않음
	HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\<Device Entry>\FriendlyName	- FriendlyName는 Value이다.
Drive Letter	HKLM\System\MountedDevices	- ParentIdPrefix를 해당 키에서 검색
	HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\<Device Entry>\FriendlyName	- FriendlyName는 Value이다.
Volume GUID	HKLM\SYSTEM\MountedDevices\\??\Volume<Volume GUID>	- Device Serial Number를 해당 키에서 검색하여 매칭
User Name	HKU\<USER>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\<Volume GUID>	
First Connection-Time	*%SystemRoot%*\Setupapi.log	- 장치를 최초로 연결한 시간이다. - 해당 시간은 각 키의 Last Written Time이다. - HKLM 하이브의 Key는 Windows XP 버전 이후 새로 추가 됨
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt\<Device Entry>	
	HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\<Device Entry>	
First Connection-Time After	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}\<Sub Keys>	- 해당 시간은 각 키의 Last Written Time이다.

Booting	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{53F5630D-B6BF-11D0-94F2-00A0C91EFB8B}\<Sub Keys>	- 해당 시간은 컴퓨터 부팅 후 장치를 연결한 시각이다. - {6AC27878-A6FA-4155-BA85-F98F491D4F33} Key는 XP 버전 이후 새로 추가 됨 - WpdBusEnumRoot Key는 Windows XP 버전 이후 새로 추가 됨
	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{6AC27878-A6FA-4155-BA85-F98F491D4F33}\<Sub Keys>	
	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{A5DCBF10-6530-11D2-901F-00C04FB951ED}\<Sub Keys>	
	HKLM\SYSTEM\ControlSet00#\Enum\WpdBusEnumRoot\UMB\<Device Entry>	
Last Connection-Time	HKU\<USER>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\<Volume GUID>	- Last Connection Time은 각 키의 Last Written Time이다. - Device Parameters Key는 Windows XP 버전 이후 새로 추가 됨
	HKLM\SYSTEM\ControlSet00#\Enum\WpdBusEnumRoot\UMB\<Device Entry>\Device Parameters	

[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>&Prod_<Product Name>&Rev_<Device Firmware Version>	
Vendor ID Product ID	HKLM\SYSTEM\ControlSet00#\Enum\USB\VID_<Vendor ID>&PID_<Product ID>	
Device Serial-Number	HKLM\SYSTEM\ControlSet00#\Enum\USB\<Vendor ID & Product ID>\<Device Serial Number>	
	HKLM\SYSTEM\ControlSet00#\Enum\USBSTOR\<Device Class ID>\<Device Serial Number>&#	
Volume Serial-Number Volume Label	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt_??_USBSTOR#<Device Class ID>#<Unique Instance ID>#<GUID><Volume Label>_<Volume Serial Number>	- EMDMgmt SubKey는 일반적으로 생성되지 않음
Volume Label	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt_??_USBSTOR#<Device Class ID>#<Unique Instance ID>#<GUID><Volume Label>_<Volume Serial Number>	- EMDMgmt SubKey는 일반적으로 생성되지 않음
	HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\<Device Entry>\FriendlyName	- FriendlyName는 Value이다. - WpdBusEnumRoot Key는 Vista 버전 이후에 Volume Label 추가 정보 획득 가능
	HKLM\System\ControlSet00#\Enum\WpdBusEnumRoot\UMB\<Device Entry>\FriendlyName	
Drive Letter	HKLM\System\MountedDevices	- Device Serial Number를 해당 키에서 검색
	HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\<Device Entry>\FriendlyName	- FriendlyName는 Value이다.
	HKLM\System\ControlSet00#\Enum\WpdBusEnumRoot\UMB\<Device Entry>\FriendlyName	
Volume GUID	HKLM\SYSTEM\MountedDevices\\??\Volume<Volume GUID>	- Device Serial Number를 해당 키에서 검색하여 매칭
User Name	HKU\<USER>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\<Volume GUID>	
First Connection-Time	*%SystemRoot%*\Setupapi.log	- 장치를 최초로 연결한 시간이다. - 해당 시간은 각 키의 Last Written Time이다. - Setupapi.log는 운영체제가 필요에 의해 이
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt\<Device Entry>	

	HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\<Device Entry>	전 기록을 압축해 보관하고 새로운 Setupapi.log로 기록을 생성할 때가 있음(파일명 ex: Setupapi_<date>.log) - {10497B1B-BA51-44E5-8318-A65C837B6661} Key는 Vista 이후 버전에서 새로 추가 됨
	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{10497B1B-BA51-44E5-8318-A65C837B6661}\<Sub Keys>	
First Connection-Time After Booting	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}\<Sub Keys>	- 해당 시간은 각 키의 Last Written Time이다. - 해당 시간은 컴퓨터 부팅 후 장치를 연결한 시각이다.
	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{53F5630D-B6BF-11D0-94F2-00A0C91EFB8B}\<Sub Keys>	
	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{6AC27878-A6FA-4155-BA85-F98F491D4F33}\<Sub Keys>	
	HKLM\SYSTEM\ControlSet00#\Control\DeviceClasses\{A5DCBF10-6530-11D2-901F-00C04FB951ED}\<Sub Keys>	
	HKLM\SYSTEM\ControlSet00#\Enum\WpdBusEnumRoot\UMB\<Device Entry>	
Last Connection-Time	HKU\<USER>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\<Volume GUID>	- Last Connection Time은 각 키의 Last Written Time이다.
	HKLM\SYSTEM\ControlSet00#\Enum\WpdBusEnumRoot\UMB\<Device Entry>\Device Parameters	

[Windows 7 / 8] Device Information in Event Log

Information	Path	Event ID	Comments
Connection Time **Verdor Name** **Device Model** **Device Serial Number**	*%SystemRoot%*\System32\winevt\Logs\ Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx	2003 2004 2005 2010	LifetimeID 값을 이용하면 동일 저장장치의 연결/해제 이벤트를 파악할 수 있다. 하지만 이 값은 절대적이지 않다.
Disconnection Time **Verdor Name** **Device Model** **Device Serial Number**	*%SystemRoot%*\System32\winevt\Logs\ Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx	2102	
MTP Device Connection - Time **MTP Device Name(Type)**	*%SystemRoot%*\System32\winevt\Logs\ Microsoft-Windows-WPD2)-MTPClassDriver%4Operational.evtx	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	*%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	HKLM\SYSTEM\ControlSet00#\Enum\USBSTOR\Disk&Ven_<Vendor Name>&Prod_<Product Name>&Rev_<Device Firmware Version>	
Vendor ID Product ID	HKLM\SYSTEM\ControlSet00#\Enum\USB\VID_<Vendor ID>&PID_<Product ID>	
Device Serial-Number	HKLM\SYSTEM\ControlSet00#\Enum\USB\<Vendor ID & Product ID>\<Device Serial Number>	
	HKLM\SYSTEM\ControlSet00#\Enum\USBSTOR\<Device Class ID>\<Device Serial Number>&#	
Volume Serial-Number Volume Label	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt_??_USBSTOR#<Device Class ID>#<Unique Instance ID>#<GUID><Volume Label>_<Volume Serial Number>	- EMDMgmt SubKey는 일반적으로 생성되지 않음
Volume Label	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt_??_USBSTOR#<Device Class ID>#<Unique Instance ID>#<GUID><Volume Label>_<Volume Serial Number>	- EMDMgmt SubKey는 일반적으로 생성되지 않음
	HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\<Device Entry>\FriendlyName	- FriendlyName는 Value이다. - WpdBusEnumRoot Key는 Vista 버전 이후에 Volume Label 추가 정보 획득 가능
	HKLM\System\ControlSet00#\Enum\WpdBusEnumRoot\UMB\<Device Entry>\FriendlyName	
	HKLM\SOFTWARE\Microsoft\Windows Search\VolumeInfoCache\<Sub Keys>	- Windows 10에서 새로 추가 됨
Drive Letter	HKLM\System\MountedDevices	- Device Serial Number를 해당 키에서 검색
	HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices\<Device Entry>\FriendlyName	- FriendlyName는 Value이다.
	HKLM\System\ControlSet00#\Enum\WpdBusEnumRoot\UMB\<Device Entry>\FriendlyName	
	HKLM\SOFTWARE\Microsoft\Windows Search\VolumeInfoCache\<Sub Keys>	- Windows 10에서 새로 추가 됨
Volume GUID	HKLM\SYSTEM\MountedDevices\\??\Volume<Volume GUID>	- Device Serial Number를 해당 키에서 검색하여 매칭
User Name	HKU\<USER>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\<Volume GUID>	

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

[Windows 10] Device Information in Event Log

Information	Path	Event ID	Comments
Connection Time **Vendor Name** **Device Model** **Device Serial Number**	*%SystemRoot%*\System32\winevt\Logs\ Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx	2003 2004 2005 2010	- LifetimeID 값을 이용하면 동일 저장장치의 연결/해제 이벤트를 파악할 수 있다. 하지만 이 값은 절대적이지 않다. - 기본 설정이 '비활성화' 이다.
	%SystemRoot%\System32\winevt\Logs\ Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx	2102	
Device Model **Device Capacity** **Device Serial Number** **MBR, VBR Raw Data** **DeviceGUID**	*%SystemRoot%*\System32\winevt\Logs\ Microsoft-Windows-Partition%4Diagnostic.evtx	1006	- 연결/해제 이벤트가 명확하지 않다. 이벤트 로그 연관 분석을 통해 연결/해제 이벤트 가능성이 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 활성화 해야 로깅된다.
Connection Time **DeviceGUID**	*%SystemRoot%*\System32\winevt\Logs\ Microsoft-Windows-Storage-ClassPnP%4Operational.evtx	512	- DeviceGUID 값을 Microsoft-Windows-Partition%4Diagnostic.evtx 이벤트와 매칭시켜 장치 정보를 획득한다.
MTP Device Connection - Time **MTP Device Name(Type)**	*%SystemRoot%*\System32\winevt\Logs\ Microsoft-Windows-WPD2)-MTPClassDriver%4Operational.evtx	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	*%SystemRoot%*\System32\winevt\Logs\ Microsoft-Windows-WPD2)-MTPClassDriver%4Operational.evtx	1002	