



# Profile Windows XP USB Drive Enclosures

<b>XP USB Drive Enclosures</b>	
<b>1. Write Down Vendor, Product, Version</b>	
SYSTEM\CurrentControlSet\Enum\USBSTOR	
<b>2. Write Down Serial Numbers</b>	
SYSTEM\CurrentControlSet\Enum\USBSTOR	Serial Number =
<b>3. Determine Vendor-ID (VID) and Product-(PID)</b>	
SYSTEM\CurrentControlSet\Enum\USB -> Perform search for S/N	VID_XXXX = PID_YYYY =
<b>4. Determine Disk Identity</b>	
Examine MBR of hard drive (Sector 0)-> 4 byte hex value starting at offset 440	Disk ID =
<b>5. Determine Drive Letter Device Mapped To</b>	
SYSTEM\MountedDevices-> Perform search for Disk ID in Drive Letters	Drive =
<b>6. Write Down Volume GUIDs</b>	
SYSTEM\MountedDevices-> Perform Search for Disk ID in the GUIDs	{GUID} =
<b>7. Find User That Used The Specific USB Device</b>	
NTUSER.DAT\Software\Microsoft\Windows\ CurrentVersion\Explorer\MountPoints2-> Search for Device GUID	User =
<b>8. Discover First Time Device Connected</b>	
C:\Windows\setupapi.log -> Perform search for Serial Number	Time/Timezone =
<b>9. Determine First Time Device Connected After Last Reboot</b>	
SYSTEM\CurrentControlSet\Control\Devic eClasses\{53f56307-b6bf-11d0-94f2- 00a0c91efb8b}-> Perform search for S/N or SYSTEM\CurrentControlSet\Enum\USB\ VID_XXXX&PID_YYYY -> Perform search for Serial Number (Last Written Time of Serial Number Key)	Time/Timezone =
<b>10. Determine Last Time Device Connected</b>	
NTUSER//Software/Microsoft/Windows/Cur rentVersion/Explorer/MountPoints2/{GUI D} -> Perform search for Device {GUID}	Time/Timezone =



# Profile VISTA USB Drive Enclosures

<b><u>VISTA USB Drive Enclosures</u></b>	
<b>1. Write Down Vendor, Product, Version</b>	
SYSTEM\CurrentControlSet\Enum\USBSTOR	
<b>2. Write Down Serial Numbers</b>	
SYSTEM\CurrentControlSet\Enum\USBSTOR	Serial Number =
<b>3. Determine Vendor-ID (VID) and Product-(PID)</b>	
SYSTEM\CurrentControlSet\Enum\USB -> Perform search for S/N	VID_XXXX = PID_YYYY =
<b>4. Determine Disk Identity</b>	
Examine MBR of hard drive (Sector 0)-> 4 byte hex value starting at offset 440	Disk ID =
<b>5. Write Down Volume GUIDs</b>	
SYSTEM\MountedDevices-> Perform Search for Disk ID	GUID =
<b>6. Determine Drive Letter Device Mapped To</b>	
SYSTEM\MountedDevices-> Perform search for Disk ID in the Drive Letters	Drive =
<b>7. Find User That Used The Specific USB Device</b>	
NTUSER.DAT\Software\Microsoft\Windows\C urrentVersion\Explorer\MountPoints2-> Search for Device GUID	User =
<b>8. Discover First Time Device Connected</b>	
C:\Windows\inf\setupapi.dev.log -> Perform search for Serial Number	Time/Timezone =
<b>9. Determine First Time Device Connected After Last Reboot</b>	
SYSTEM\CurrentControlSet\Enum\USBSTOR\ Vendor_Product_Version -> Perform search for Serial Number (Last Written Time of Serial Number Key)	Time/Timezone =
<b>10. Determine Last Time Device Connected</b>	
SYSTEM\CurrentControlSet\Enum\USB\ VID_XXXX&PID_YYYY -> Perform search for Serial Number (Last Written Time of Serial Number Key)	Time/Timezone =



# Profile Windows 7 USB Drive Enclosures

<b>Win7 USB Drive Enclosures</b>	
<b>1. Write Down Vendor, Product, Version</b>	
SYSTEM\CurrentControlSet\Enum\USBSTOR	
<b>2. Write Down Serial Numbers</b>	
SYSTEM\CurrentControlSet\Enum\USBSTOR	Serial Number =
<b>3. Determine Vendor-ID (VID) and Product-(PID)</b>	
SYSTEM\CurrentControlSet\Enum\USB -> Perform search for S/N	VID_XXXX = PID_YYYY =
<b>4. Determine Disk Identity</b>	
Examine MBR of hard drive (Sector 0)-> 4 byte value starting at offset 440	Disk ID =
<b>5. Determine Drive Letter Device Mapped To</b>	
SYSTEM\MountedDevices-> Perform search for Disk ID in the Drive Letters	Drive =
<b>6. Write Down Volume GUIDs</b>	
SYSTEM\MountedDevices-> Perform Search for Disk ID in the GUIDs	GUID =
<b>7. Find User That Used The Specific USB Device</b>	
NTUSER.DAT\Software\Microsoft\Windows\C urrentVersion\Explorer\MountPoints2-> Search for Device GUID	User =
<b>8. Discover First Time Device Connected</b>	
C:\Windows\inf\setupapi.dev.log -> Perform search for Serial Number	Time/Timezone =
<b>9. Determine First Time Device Connected After Last Reboot</b>	
SYSTEM\CurrentControlSet\Enum\USBSTOR\ Vendor_Product_Version -> Perform search for Serial Number (Last Written Time of Serial Number Key)	Time/Timezone =
<b>10. Determine Last Time Device Connected</b>	
SYSTEM\CurrentControlSet\Enum\USB\ VID_XXXX&PID_YYYY -> Perform search for Serial Number (Last Written Time of Serial Number Key)	Time/Timezone =