### XP USB KEY/Thumbdrive

1. **Write Down Vendor, Product, Version**

   ```
   SYSTEM\CurrentControlSet\Enum\USBSTOR
   Vendor = 
   Product = 
   Version = 
   ```

2. **Write Down Serial Numbers**

   ```
   SYSTEM\CurrentControlSet\Enum\USBSTOR
   Serial Number = 
   ```

3. **Determine Parent Prefix ID**

   ```
   SYSTEM\CurrentControlSet\Enum\USBSTOR
   Parent Prefix ID = 
   ```

4. **Determine Vendor-ID (VID) and Product-PID**

   ```
   SYSTEM\CurrentControlSet\Enum\USB
   Perform search for S/N
   VID_XXXX = 
   PID_YYYY = 
   ```

5. **Determine Drive Letter Device Mapped To**

   ```
   SYSTEM\MountedDevices->
   Perform search for Parent Prefix ID in the Drive Letter
   Drive = 
   ```

6. **Write Down Volume GUIDs**

   ```
   SYSTEM\MountedDevices->
   Perform search for Parent Prefix ID in the GUIDs
   {GUID} = 
   ```

7. **Find User That Used The Specific USB Device**

   ```
   NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2->
   Search for Device GUID
   User = 
   ```

8. **Discover First Time Device Connected**

   ```
   C:\Windows\setupapi.log -> Perform search for Serial Number
   Time/Timezone = 
   ```

9. **Determine First Time Device Connected After Last Reboot**

   ```
   SYSTEM\CurrentControlSet\Control\DeviceClasses\{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 = 
   ```

10. **Determine Last Time Device Connected**

    ```
    NTUSER//Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2/{GUID} -> Perform search for Device {GUID}
    Time/Timezone = 
    ```

---

http://forensics.sans.org  
http://twitter.com/sansforensics
# VISTA USB Key/Thumbdrives

<table>
<thead>
<tr>
<th>VISTA USB KEY/Thumbdrive</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Write Down Vendor, Product, Version</strong></td>
</tr>
<tr>
<td>SYSTEM\CurrentControlSet\Enum\USBSTOR</td>
</tr>
<tr>
<td>Vendor = Product = Version =</td>
</tr>
<tr>
<td><strong>2. Write Down Serial Numbers</strong></td>
</tr>
<tr>
<td>SYSTEM\CurrentControlSet\Enum\USBSTOR</td>
</tr>
<tr>
<td>Serial Number =</td>
</tr>
<tr>
<td><strong>3. Determine Vendor-ID (VID) and Product-(PID)</strong></td>
</tr>
<tr>
<td>SYSTEM\CurrentControlSet\Enum\USB -&gt; SYSTEM\CurrentControlSet\Enum\USBSTOR</td>
</tr>
<tr>
<td>Perform search for S/N</td>
</tr>
<tr>
<td>VID_XXXX = PID_YYYY =</td>
</tr>
<tr>
<td><strong>4. Write Down Volume GUIDs</strong></td>
</tr>
<tr>
<td>SYSTEM\MountedDevices-&gt; Perform Search for Serial Number or SYSTEM\MountedDevices-&gt; Perform Search for Serial Number and Match with Volume Name</td>
</tr>
<tr>
<td>GUID = Drive Letter = Volume Name=</td>
</tr>
<tr>
<td><strong>5. Determine Drive Letter and Volume Name Device Mapped To</strong></td>
</tr>
<tr>
<td>SOFTWARE\Microsoft\Windows Portable Devices\Devices-&gt; Perform Search for Serial Number or SOFTWARE\Microsoft\Windows Portable Devices\Devices-&gt; Perform Search for Serial Number and Match with Volume Name</td>
</tr>
<tr>
<td>Drive Letter = Volume Name=</td>
</tr>
<tr>
<td><strong>6. Find User That Used The Specific USB Device</strong></td>
</tr>
<tr>
<td>NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2-&gt; SYSTEM\MountedDevices</td>
</tr>
<tr>
<td>Search for Device GUID User =</td>
</tr>
<tr>
<td><strong>7. Discover First Time Device Connected</strong></td>
</tr>
<tr>
<td>C:\Windows\inf\setupapi.dev.log -&gt; Perform search for Serial Number or C:\Windows\inf\setupapi.dev.log -&gt; Perform search for Serial Number and Match with Volume Name</td>
</tr>
<tr>
<td>Time/Timezone =</td>
</tr>
<tr>
<td><strong>8. Determine First Time Device Connected After Last Reboot</strong></td>
</tr>
<tr>
<td>SYSTEM\CurrentControlSet\Enum\USBSTOR\Vendor_Product_Version -&gt; SYSTEM\CurrentControlSet\Enum\USBSTOR or</td>
</tr>
<tr>
<td>SYSTEM\CurrentControlSet\Enum\USBSTOR\Vendor_Product_Version -&gt; SYSTEM\CurrentControlSet\Enum\USBSTOR or</td>
</tr>
<tr>
<td>SYSTEM\CurrentControlSet\Control\Device Classes{53f56307-b6bf-11d0-94f2-00a0c91efb8b} -&gt; Perform search for S/N (Last Written Time of Key that has Serial Number and Vendor/Product/Revision)</td>
</tr>
<tr>
<td>SYSTEM\CurrentControlSet\Enum\USB\VID_XXXX&amp;PID_YYYY -&gt; Perform search for Serial Number (Last Written Time of Serial Number Key) or</td>
</tr>
<tr>
<td>SYSTEM\CurrentControlSet\Enum\USB\VID_XXXX&amp;PID_YYYY -&gt; Perform search for Serial Number (Last Written Time of Serial Number Key) or</td>
</tr>
<tr>
<td>NTUSER//Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2/{GUID} -&gt; Perform search for Device {GUID}</td>
</tr>
<tr>
<td>Time/Timezone =</td>
</tr>
</tbody>
</table>

[http://forensics.sans.org](http://forensics.sans.org)  
[http://twitter.com/sansforensics](http://twitter.com/sansforensics)
# Profile Windows 7 USB Keys/Thumbdrives

## Win7 USB Key/Thumbdrive

1. **Write Down Vendor, Product, Version**

   ```
   SYSTEM\CurrentControlSet\Enum\USBSTOR
   Vendor = 
   Product = 
   Version = 
   ```

2. **Write Down Serial Numbers**

   ```
   SYSTEM\CurrentControlSet\Enum\USBSTOR
   Serial Number = 
   ```

3. **Determine Vendor-ID (VID) and Product-(PID)**

   ```
   SYSTEM\CurrentControlSet\Enum\USB
   Perform search for S/N
   VID_XXXX = 
   PID_YYYY = 
   ```

4. **Determine Drive Letter Device Mapped To**

   ```
   SYSTEM\MountedDevices->
   Perform search for Serial Number in the Drive Letters
   Drive = 
   ```

5. **Write Down Volume GUIDs**

   ```
   SYSTEM\MountedDevices->
   Perform Search for Serial Number in the GUIDs
   GUID = 
   ```

6. **Find User That Used The Specific USB Device**

   ```
   NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2->
   Search for Device GUID
   ```

7. **Discover First Time Device Connected**

   ```
   C:\Windows\inf\setupapi.dev.log -> Perform search for Serial Number
   ```

8. **Determine First Time Device Connected After Last Reboot**

   ```
   SYSTEM\CurrentControlSet\Enum\USBSTOR\Vendor_Product_Version -> Perform search for Serial Number (Last Written Time of Serial Number Key)
   ```
   ```
   or
   ```
   SYSTEM\CurrentControlSet\Control\Device Classes\{53f56307-b6bf-11d0-94f2-00a0c91efb8b} -> Perform search for S/N (Last Written Time of Key that has Serial Number and Vendor/Product/Revision)
   ```

9. **Determine Last Time Device Connected**

   ```
   SYSTEM\CurrentControlSet\Enum\USB\VID_XXXX&PID_YYYY -> Perform search for Serial Number (Last Written Time of Serial Number Key)
   ```
   ```
   or
   ```
   NTUSER//Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2/{GUID} -> Perform search for Device {GUID}
   ```

---

http://forensics.sans.org
http://twitter.com/sansforensics