USB Forensic

Mass Storage Class (MSC): - USB drive

Picture Transfer Protocol (PTP): - pull stuff from your device. but you can't put stuff back on it.

Media Transfer Protocol (MTP): - music, docs, and more.

Windows Portable Devices (WPD): - it's like the universal translator for different device types.

MTP AND MSC

MSC Device:

you open files from MSC Device. you get these little LNK files.

- C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Recent: LNK files for all files and folders you opened.
- C:\Users\Win 7SP1\AppData\Roaming\Microsoft\Office\Recent: Just for Microsoft Office files.

MTP Devices:

it doesn't exist on Windows 10. When you open files from an MTP device, copies get saved in

- C:\Users\<Username>\AppData\Local\Temp\WPDNSE\

WPDNSE folder is temporary. Windows likes to clean it out when you reboot.

You'll see these weird GUIDs like {02601-000-01CD-8801-7I017K017} as folder names.

To Make sense:

1. Dive into the registry and look for the BagMRU entries related to your MTP device.
2. Find the folder GUIDs listed under these entries.
3. Match them up with the GUID-named folders in your WPDNSE directory.

USBSTOR

Registry Key: SYSTEM\CurrentControlSet\Enum\USBSTOR

- Disk&Ven: - Referred as Device class ID:
- 57583..: - Referred as Unique device Serial #

Search Smart: Use the "Find" option in Registry Explorer to search for keys with specific Serial Numbers across all loaded registry hives.

USBSTOR keys could be cleared after 30 days.

USB

Registry Key: SYSTEM\CurrentControlSet\Enum\USB

Stores the Serial Number (VID) and Product ID (PID). VID_046D&PID_C077

This key is like a treasure trove for forensic investigators. Apart from storage devices, you can spot other gadgets like phones, tablets, and printers that were connected to the system—even if Windows didn't recognize them as mass storage devices.

If you stumble upon an unknown VID or PID, there's a handy website to help you out:

linux-usb.org/usb.ids.

Just plug in the numbers, and it'll reveal the manufacturer and product details.

Volume Name and GUID

Registry key: SOFTWARE\Microsoft\Windows Portable Devices\Devices

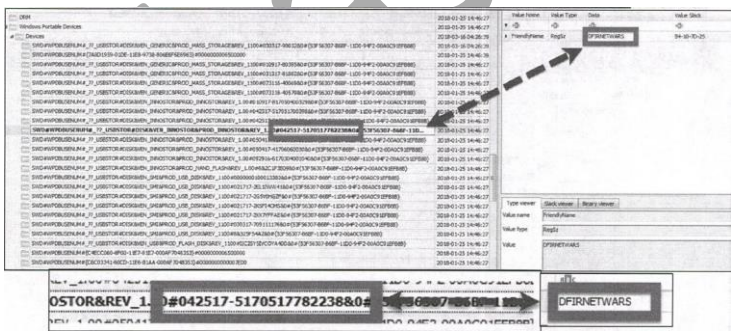
You can also grab the Volume Name (Friendly name) and GUID, which can be handy for future reference.

Windows 10 Example:

Here's how it looks on Windows 10:

- **Windows Portable Devices Key**: You'll find the Volume Name here.
- **Drive Letter**: Unfortunately, not listed directly. But armed with the Volume Name, you can often trace it back using Shell Item historical information.

Another example Taking # ---# value for further analysis: (This is Serial #)



If there is Drive letter way to find drive letter:

Drive Letter and User and Volume GUID:

MSC Only (Windows 7-10)

Steps to Find Last Drive Letter of a USB Device:

1. **Retrieve Device Serial Number**:
    - Retrieve the device Serial Number from the **USBSTOR** registry key, which was stored earlier.
2. **Examine SYSTEM Hive and MountedDevices Key**:
    - Open the **SYSTEM** hive from the Windows registry.
    - Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices**.
3. **Find Drive Letter Using Serial Number**:
    - Search for the device Serial Number within the **MountedDevices** key.
    - The last device associated with a drive letter will have its Serial Number listed. This indicates the drive letter assigned to that specific device.

Steps to Locate Volume GUID:

1. **Search MountedDevices for Serial Number**:
    - Look for the device's Serial Number within the data values of the various GUIDs in **SYSTEM\MountedDevices**.
2. **Identify the Relevant GUID**:
    - Once the Serial Number is located, determine the corresponding GUID and note it down.

Mapping GUID to User:

- **NTUSER.DAT Hive**:
    - Use the noted GUID to search through the **MountPoints2** key in the user's **NTUSER.DAT** hive.
    - This key is located at **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Mountpoints2**.
- **Mapping to User**:
    - Each Volume GUID listed under **MountPoints2** corresponds to a different local or removable drive connected to the system.

- The Volume Serial Number from **SYSTEM\MountedDevices** should match one of the entries in **MountPoints2**, helping to identify the user associated with the device.

First time and last time and USB Removal

MSC USB device times to track.

USB Times:

- First time device is connected
- Last time device is connected
- Removal time

Registry Key : **HKLM\SYSTEM*CurrentControlSet*\Enum\USBSTOR*Ven_Prod_Version**USB iSerial#*\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\####**

- ***0064 = First Install (Win7 / 8)***
  Also found in setupapi.log / setupapi.dev.log (Alternate)
- ***0066 = Last Connected (Win8+ only)***
  Also \Enum\USB\VID_XXXX&PID_YYYY last write time of USB Serial # key (Alternate)

o 0067 = Last Removal (Win8+ only)
NTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{GUID}
last write time of key ***(****Alternate)*

USB First Time Device Connected Logs:

XP: C:\Windows**setupapi.log**

Vista+: C:\Windows\inf**setupapi.dev.log**

Search for the device's Serial # within these logs and you can discover the first time a device was plugged in to a computer.

Event Logging:

1. **Event ID 20001**

When you plug in a USB or any device, Windows often tries to install its drivers automatically. This action creates an "Event ID 20001" in the system logs.

2. This log, known as **DriverFrameworks UserMode**

Device connection and disconnection times.

3. **Event ID 4663**

Record of BYOD (Bring Your Own Device) usage after auditing is configured. It links user accounts with device actions, like copying a file.

4. **Event ID 4656**
   Failed access to removable devices.
5. **Event ID 6416**
   Within the Advanced Audit Policy Configuration, a new option can be added under "Detailed Tracking". lf"Audit PNP Activity" is enabled (it is not on by default), the Security log will record an event every time a Plug and Play device is added to the system.
   Detailed hardware info and it's all in one place.
6. **MBAM/Operational log**
   If your computer uses BitLocker for encryption, MBAM/Operational log can tell you when removable media gets mounted or dismounted.

Tip:- "Audit Removable Storage" (EID 4663) and "Audit Plug and Play Activity" (EID 6416) enabled. Both Event ID complement each other very well (And using both easily identified which user using timestamp)

EMDMgmt Key

Optional: Finding Your USB's Volume Serial Number

Steps to Find Volume Serial Number:

1. Check the Volume Info:
   - Use a tool like vol.exe to find the Volume Label and Serial Number of your USB.
2. Look in the Registry:
   - Open Regedit and navigate to SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt.
   - Search for your USB's Unique Serial Number or Volume Name.
   - The last number you see there is your Volume Serial Number in decimal form.
3. Convert to Hex:
   - Take that decimal number and plug it into a calculator.
   - Switch your calculator to Hex mode to see the Volume Serial Number in hex.

Why Bother?

- Check the USB's usage history.
- Analyze recent documents or shortcuts linked to the USB.

Quick Guide for Windows

1. Vendor, Product, Version

- **Path**: **SYSTEM\CurrentControlSet\Enum\USBSTOR**
- Vendor:
- Product:
- Version:

2. USB Unique Serial Number ID

- **Path: SYSTEM\CurrentControlSet\Enum\USB**
- USB Unique Serial Number ID**:**

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

- **Path**: **SYSTEM\CurrentControlSet\Enum\USB -->** Perform search for UB S/N
- **VID**:
- **PID**:

4. Volume GUIDs

- **Path: SYSTEM\MountedDevices** -->Search Serial Number in drive letter
- VolumeGUID**:**

5. Drive Letter

- **Path**: **SYSTEM\MountedDevices -->** Search for Volume GUID in drive letter
- **Drive Letter**:

Or

NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\Explorer\RecentDocs -> Perform Search for Volume Name

Or

Perform Shortcut (LNK) file analysis-> Perform Search for Volume Name

Drive Letter=

6. Volume Name

- **Path**: **SOFTWARE\Microsoft\Windows Portable Devices\Devices -->** Search USB serial number and match with volume name
- **Volume Name**:
- **Drive Letter (VISTA ONLY)**:

7. Volume Serial Number (Key will ONLY be present if system drive is NOT SSD)

- **Path**: **SOFTWARE\Microsoft\WindowsNT\CurrentVersion\EMDMgmt -->** Search volume name/Serial Number. Convert Serial number to hex value for link analysis.
- **Volume Serial Number (HEX)**:

8. User of USB Device

- **Path**: **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 -->**Search for GUID
- **User**:

9. First Time Device Connected

- **Path**: **C:\Windows\inf\setupapi.dev.log -->**Search unique serial number
- **Time/Timezone**:

SYSTEM\CurrentControlSet\Enum\USBSTOR\ Ven Prod_ Version\USB iSerial #\Properties\ {83da6326-97a6-4088-9453-a1923f573b29} \0064 ->Value= Windows 64-Bit Hex Value timestamp - Use DCodeDate

10. Last Time Device Connected

- **Path**: **SYSTEM\CurrentControlSet\Enum\USB\VID_XXXX&PID_YYYY -->**Search serial number
- **Time/Timezone**:

or

NTUSER//Software/Microsoft/Windows/CurrentVersion/Explorer/MountPoints2/{GUID} -> Perform search for Device { GUID}

Time/Timezone =

SYSTEM\CurrentControlSet\Enum\USBSTOR\ Ven_Prod_ Version\USB iSerial #\Properties\ {83da6326-97a6-4088-9453-a1923f573b29}\0066 ->Value= Windows 64-Bit Hex Value timestamp - Use DCodeDate

11. Time Device Removed

SYSTEM\CurrentControlSet\Enum\USBSTOR\ Ven Prod_ Version\USB iSerial #\Properties\ {83da6326-97a6-4088-9453-a1923f573b29}\0067 ->Value= Windows 64-Bit Hex Value timestamp - Use DCodeDate

Tips for Timestamps

- For Windows 64-bit Hex Value timestamps, use **DCodeDate** to decode them.