Windows Registry Cheat Sheet

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer

- \ComDlg32
    - \LastVisitedPidlMRU ← Tracks apps used to open/save files
    - \OpenSavePidlMRU ← Tracks files accessed via open/save dialog
- \Mountpoints2 ← Tracks data about removable devices (USB, etc.)
- \RecentDocs ← Recent file interaction
- \RunMRU ← Start → Run history
- \TypedPaths ← Paths manually entered into Explorer address bar
- \UserAssist ← Per-user evidence of execution (GUI programs)
- \WordWheelQuery* ← Explorer search history

*Windows 11 22H2 / Windows Server 2022 and earlier

HKCU\SOFTWARE\Classes

- **%USERPROFILE%\AppData\Local\Microsoft\Windows\UsrClass.dat "plugs in" here**

HKCU\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache

- MuiCache: shows per-user evidence of execution (GUI programs); time of execution NOT tracked

HKCU\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell

- ShellBags: tracks per-user Explorer folder browsing
- \BagMRU
- \Bags

Additional ShellBags subkeys in this location track the Desktop and Network Locations:

HKCU\SOFTWARE\Microsoft\Windows\Shell

- \BagMRU
- \Bags

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

- Starts programs on user logon (affects **CURRENT USER** only)

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

- Starts programs on user logon (affects **ALL USERS**)

HKLM\SYSTEM\*CurrentControlSet*\Enum\USB ← USB VID / PID
HKLM\SYSTEM\*CurrentControlSet*\Enum\USBSTOR ← USB Class ID / Serial #

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
- **0066** = Last Connected (Win8+ only)
    - Also \Enum\USB\VID_XXXX&PID_YYYY last write time of USB Serial # key
    - Also \MountPoints2\{GUID} last write time of key
- **0067** = Last Removal (Win8+ only)

HKLM\SYSTEM\MountedDevices

- Find Serial # to obtain the **Drive Letter** of the USB device
- Find Serial # to obtain the **Volume GUID** of the USB device

HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices

- Find Serial # and then look for *FriendlyName* to obtain the **Volume Name** of the USB device

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt

- Key will ONLY be present if system drive is NOT an SSD
- Traditionally used for ReadyBoost
- Find Serial # to obtain the **Volume Serial Number** of the USB device
    - The Volume Serial Number will be in decimal – convert to hex
    - You can find complete history of Volume Serial Numbers here, even if the device has been formatted multiple times. The USB device's Serial # will appear multiple times, each with a different Volume Serial Number generated on each format.

Using the **Volume GUID** found in **SYSTEM\MountedDevices**, you can find the **user** that actually mounted the USB device:

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Mountpoints2

USB Times:

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

While not a Registry artifact, note that USB First Time Device Connected Logs are also available:

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

Search for the device's **Serial #** within these logs to determine the first time the device was connected.

HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation

HKLM\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName

HKLM\SYSTEM\CurrentControlSet\services\LanmanServer\Shares

- Stores all Network Shares

HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces

- Stores network interface configuration information (record the interface GUID!)

Network Location Awareness (NLA) was included in Vista+, and aggregates the network information for a PC and generates a GUID to identify each network (a “network profile”, if you will). The Windows Firewall uses that information to apply firewall rules to the appropriate profile. You can find evidence of every network a machine has connected to using NLA registry keys.

Check the last write time of a key to determine the last time a PC connected to a particular network.

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList

- \Signatures
  - \Unmanaged (record **DefaultGatewayMac**, **DnsSuffix**, **FirstNetwork** (SSID), **ProfileGuid**)
  - \Managed
- \Nla
  - \Cache
- Profiles

Most info regarding NLA will be stored under the **NetworkList** key above, and also:
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\HomeGroup

Network Type, and First / Last Connected Times (find using the **ProfileGuid** key harvested from Signatures\Unmanaged):

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{GUID}

HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\{GUID} → (XP only, use last write time of the key to determine the last time the network was connected)

0x06	=	Wired
0x17	=	Broadband
0x47	=	Wireless

You will also find **DateCreated** and **DateLastConnected** under this key.

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

- Also known as "**Shimcache**", this can *sometimes* be an evidence of execution artifact
  - Prior to Windows 10, an InsertFlag (sometimes incorrectly referred to as an "Execution Flag") could be used to indicate likely execution. In Windows 10 and later, it may still be possible to determine if execution took place if the last four (4) bytes of a Shimcache record are equal to `00 00 00 01`.
- Stores the full file path and name and last modified (M) timestamp

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters

EnablePrefetcher Key:

0 = Disabled
1 = Application prefetching enabled
2 = Boot prefetching enabled (default on Windows 2003 only)
3 = Application and Boot prefetching enabled (default)

- Task Scheduler calls Windows Disk Defragmenter every three (3) days
- When idle, lists of files and directories referenced during boot process and application startups is processed
- The processed result is stored in **Layout.ini** in the Prefetch directory, and is subsequently passed to the Disk Defragmenter, instructing it to re-order those files into sequential positions on the physical hard drive