



Sourabh Giri



Windows Forensics

The **Windows Registry** is like the brain of a Windows system. It is a collection of databases that store all the important configuration details for the system. These details include information about the computer's hardware, installed software, user settings, and even recently used files or devices. From a **forensics perspective**, the registry is valuable because it provides critical insights into a computer's activity, such as which programs were run, what devices were connected, and much more.

You can view and edit the registry using a built-in tool called **regedit.exe**. This tool allows users to explore and modify the data in the registry.

Key Components of the Windows Registry:

1. Keys and Values:

- **Registry Keys:** These are like folders in a file system. When you open the registry in regedit.exe, the "folders" you see are the keys.
 - **Registry Values:** These are the actual data stored inside the keys. Think of them as files stored inside folders.
 - **Registry Hive:** A collection of keys, subkeys, and values grouped together in one file.
-

Structure of the Registry:

The registry is organized into **five root keys**, each serving a specific purpose:

1. HKEY_CURRENT_USER (HKCU):

- Stores settings and configurations for the currently logged-in user.
- Examples: Desktop background, Control Panel settings, screen colors, etc.
- This key reflects the user's profile and is specific to them.

2. HKEY_USERS (HKU):

- Contains data for all user profiles on the system.
- The **HKEY_CURRENT_USER** is a subkey of this root key.
- Think of it as a master key containing settings for every user account.



3. HKEY_LOCAL_MACHINE (HKLM):

- Stores system-wide settings for the computer, regardless of which user is logged in.
- Examples: Hardware configuration, software installed for all users, etc.
- It is vital for system stability and contains information that applies to every user.

4. HKEY_CLASSES_ROOT (HKCR):

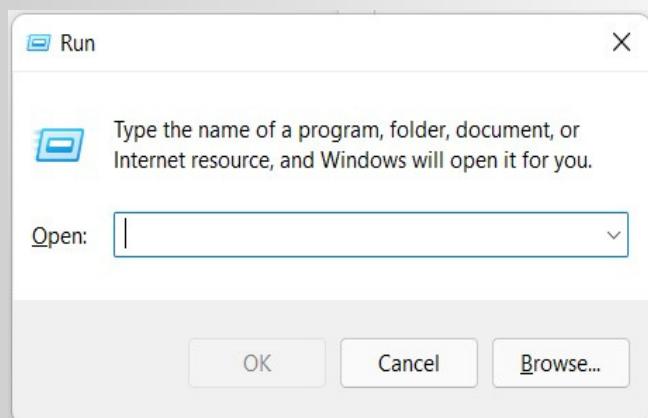
- Contains settings that determine how files and programs interact.
- Example: When you double-click a .txt file, this key ensures it opens with Notepad (or another default program).
- **Details on its behavior:**
 - It is a merged view of two keys:
 - **HKEY_LOCAL_MACHINE\Software\Classes:** Default settings for all users.
 - **HKEY_CURRENT_USER\Software\Classes:** Overrides default settings for the current user.
 - If you change something in HKCR:
 - If a corresponding key exists in **HKEY_CURRENT_USER\Software\Classes**, the change is saved there.
 - Otherwise, the change is saved in **HKEY_LOCAL_MACHINE\Software\Classes**.

5. HKEY_CURRENT_CONFIG (HKCC):

- Contains information about the computer's **hardware configuration** during startup.
- Example: Details about the current hardware profile being used (like which monitor or printer is connected).

Accessing the Registry:

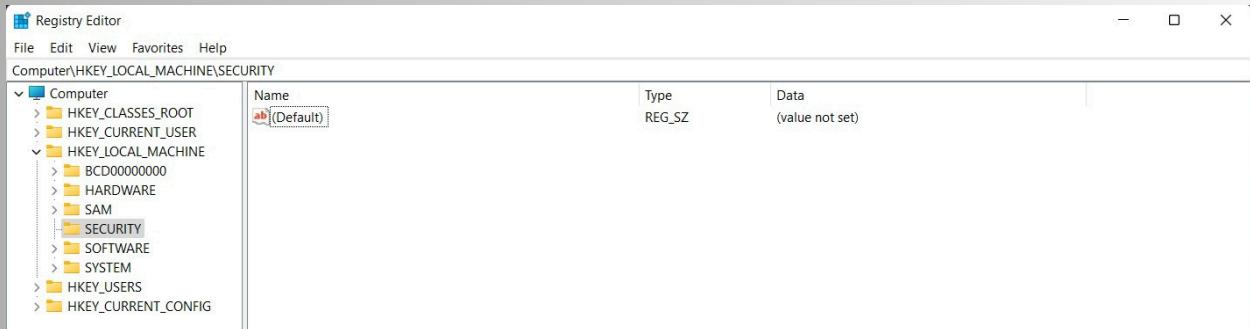
1. Press the **Windows Key + R** to open the Run prompt.
2. Type **regedit.exe** and hit **Enter**.
3. This will open the **Registry Editor** window.



Exploring the Registry:

On the left side, you'll see a **tree view** with the root keys (like HKCU, HKLM, etc.).

- When you click on a key, its **values** (data) will appear on the right pane.
- You can view or edit these values by right-clicking on them and selecting **Properties**.
-



Why is the Registry Important?

System Configuration: Stores critical information that makes your system run

- smoothly.
- Forensics Use:** Helps investigators trace user activity, identify recently connected devices, or check recently used programs.
- Customizations:** Advanced users can modify the registry to tweak system behavior.
-

Summary of Root Keys:

Root Key	Purpose
HKEY_CURRENT_USER	Current user's settings (desktop, Control Panel, etc.).
HKEY_USER	Settings for all user profile on the system
HKEY_LOCAL_MACHINE	System-wide settings (hardware, software, etc)
HKEY_CLASSES_ROOT	Determines which program opens files and how programs interact with files. Current hardware profile used during system startup.
HKEY_CURRENT_CONFIG	



Accessing the Registry on a Live System

When working on a **live Windows system**, you can access the registry using the built-in tool called **regedit.exe**. This tool allows you to view all the standard **root keys** (like HKEY_LOCAL_MACHINE, HKEY_CURRENT_USER, etc.) that were explained earlier.

Accessing the Registry on a Disk Image

If you're analyzing a **disk image** (instead of a live system), you cannot use regedit.exe directly. Instead, you need to know where the **registry hives** (the actual registry files) are located on the disk. These hives are stored in specific locations, typically in the directory: **C:\Windows\System32\Config**

The key hives in this directory are:

1. **DEFAULT**
○ This hive is mounted under: **HKEY_USERS\DEFAULT**
2. **SAM**
○ This hive is mounted under: **HKEY_LOCAL_MACHINE\SAM**
3. **SECURITY**
○ This hive is mounted under: **HKEY_LOCAL_MACHINE\SECURITY**
4. **SOFTWARE**
○ This hive is mounted under: **HKEY_LOCAL_MACHINE\SOFTWARE**
5. **SYSTEM**
○ This hive is mounted under: **HKEY_LOCAL_MACHINE\SYSTEM**

These hives contain vital information about the system, including software configurations, security settings, user accounts, and more.

Hives Containing User Information

There are additional **hives** that contain user-specific information. These hives are located in the user's profile directory. For **Windows 7 and later versions**, a user's profile directory is typically:

C:\Users\<username>



The two user-specific hives are:

1. NTUSER.DAT

- Location: C:\Users\<username>\
- Mounted on: HKEY_CURRENT_USER when the user logs in.
- This hive contains personal settings, configurations, and information specific to that user.

📁 .dotnet	10/15/2021 11:20 PM	File folder	
📁 .ipython	9/6/2021 8:55 AM	File folder	
📁 .ssh	8/11/2021 2:01 PM	File folder	
📁 .templateengine	10/15/2021 11:23 PM	File folder	
📁 .vscode	8/7/2021 6:55 PM	File folder	
📦 3D Objects	8/7/2021 5:46 PM	File folder	
📁 ansel	8/7/2021 6:30 PM	File folder	
📁 AppData	10/16/2021 11:36 AM	File folder	
📁 Contacts	10/16/2021 11:38 AM	File folder	
📁 Desktop	12/21/2021 7:32 PM	File folder	
📁 Documents	12/21/2021 7:33 PM	File folder	
⬇️ Downloads	12/22/2021 3:14 PM	File folder	
📁 Favorites	10/16/2021 11:38 AM	File folder	
📁 Links	10/16/2021 11:38 AM	File folder	
🎵 Music	10/16/2021 11:38 AM	File folder	
☁️ OneDrive	10/16/2021 11:40 AM	File folder	
🖼️ Pictures	10/16/2021 11:38 AM	File folder	
📁 PycharmProjects	11/24/2021 2:01 PM	File folder	
📁 Saved Games	10/16/2021 11:38 AM	File folder	
📁 Searches	10/16/2021 11:38 AM	File folder	
📁 source	10/15/2021 11:17 PM	File folder	
🎥 Videos	10/23/2021 9:44 AM	File folder	
📄 .pagerc	8/23/2021 11:09 AM	PAGERC File	4 KB
NTUSER.DAT	12/26/2021 2:47 AM	DAT File	2,560 KB



2. USRCLASS.DAT

 0	10/16/2021 11:38 AM	File folder
 1024	10/21/2021 10:56 AM	File folder
 1033	10/16/2021 11:38 AM	File folder
 ActionCenterCache	12/26/2021 2:47 AM	File folder
 Application Shortcuts	10/16/2021 11:38 AM	File folder
 Burn	10/16/2021 11:39 AM	File folder
 Caches	12/26/2021 11:40 AM	File folder
 CloudStore	6/5/2021 8:10 AM	File folder
 Explorer	10/23/2021 11:45 AM	File folder
 Fonts	9/3/2021 9:32 PM	File folder
 GameExplorer	6/5/2021 8:10 AM	File folder
 History	10/16/2021 11:36 AM	File folder
 Notifications	8/7/2021 5:46 PM	File folder
 PowerShell	10/21/2021 10:51 AM	File folder
 PPBCompatCache	10/16/2021 11:55 AM	File folder
 PPBCompatUaCache	10/16/2021 11:55 AM	File folder
 Ringtones	10/16/2021 11:38 AM	File folder
 RoamingTiles	8/7/2021 5:46 PM	File folder
 Safety	10/24/2021 10:12 PM	File folder
 Shell	9/13/2021 11:40 AM	File folder
 Themes	8/8/2021 7:36 PM	File folder
 WinX	12/7/2019 4:14 AM	File folder
 usrClass.dat	12/26/2021 2:47 AM	DAT File
		5,120 KB

- Location: `C:\Users\<username>\AppData\Local\Microsoft\Windows`
- Mountedon: `HKEY_CURRENT_USER\Software\CLASSES`.
- This hive stores additional user-specific settings related to software.



Both **NTUSER.DAT** and **USRCLASS.DAT** are **hidden files**, so you may need to enable the option to view hidden files in Windows to see them.

The AmCache Hive

Another important hive is the **AmCache hive**, which is located at:

C:\Windows\AppCompat\Programs\Amcache.hve

The **AmCache hive** is crucial because it contains information about **programs recently run** on the system. This is highly useful for forensic investigations to determine which programs were executed and when.

Transaction Logs and Backups

1. Transaction Logs

- These are **log files** that act as a **journal** for changes made to registry hives.
- When changes are made to a registry hive, they are first written to these **transaction logs** before being applied to the hive itself. This means that the transaction logs might contain the **most recent changes** that haven't yet been applied to the registry hive.
- The transaction logs for each hive are restored in the same directory as the hive and have the same name but with a **.LOG** extension.
For example:
 - The transaction log for the SAM hive is located at:
C:\Windows\System32\Config\SAM.LOG
 - If there are multiple logs, they will be named as **SAM.LOG1, SAM.LOG2, etc.**

Why Are Transaction Logs Important?

Transaction logs are valuable in forensic investigations as they may contain critical information about recent changes that are not visible in the main registry hives.



2. Registry Backups

- Windows automatically creates **backups of registry hives** every ten days.
- These backups are stored in:
 - C:\Windows\System32\Config\RegBack**
- If registry keys have been **deleted or modified**, you can check these backups to see the earlier state of the registry.

Why Are Backups Useful?

Backups allow investigators to compare the current state of the registry with the past state to detect modifications or deletions.

Summary of Key Locations

Hive/File	Location	Mounted Under
DEFAULT	C:\Windows\System32\Config	HKEY_USERS\DEFAULT
SAM	C:\Windows\System32\Config	HKEY_LOCAL_MACHINE\SAM
SECURITY	C:\Windows\System32\Config	HKEY_LOCAL_MACHINE\SECURITY
SOFTWARE	C:\Windows\System32\Config	HKEY_LOCAL_MACHINE\SOFTWARE
SYSTEM	C:\Windows\System32\Config	HKEY_LOCAL_MACHINE\SYSTEM
NTUSER.DAT	C:\Users\<username>\	HKEY_CURRENT_USER
USRCLASS.DAT	C:\Users\<username>\AppData\Local\Microsoft\Windows	HKEY_CURRENT_USER\Software\CLASSES



AmCache.hve	C:\Windows\AppCompat\Programs\Amcache.hve	Not directly mounted; useful for recent program info
Transaction Logs	Same directory as registry hives, with .LOG	Stores recent changes
Registry Backups	C:\Windows\System32\Config\RegBack	Contains backups of registry hives

Final Notes

- **Live system:** Use regedit.exe to explore registry keys.
- **Disk image:** Look for hives in the specified directories.
- **Hidden files:** NTUSER.DAT and USRCLASS.DAT require enabling hidden file visibility.
- **AmCache hive:** Critical for identifying recently run programs.
- **Transaction logs and backups:** Essential for forensic investigations to track changes and restore deleted/modified registry data.

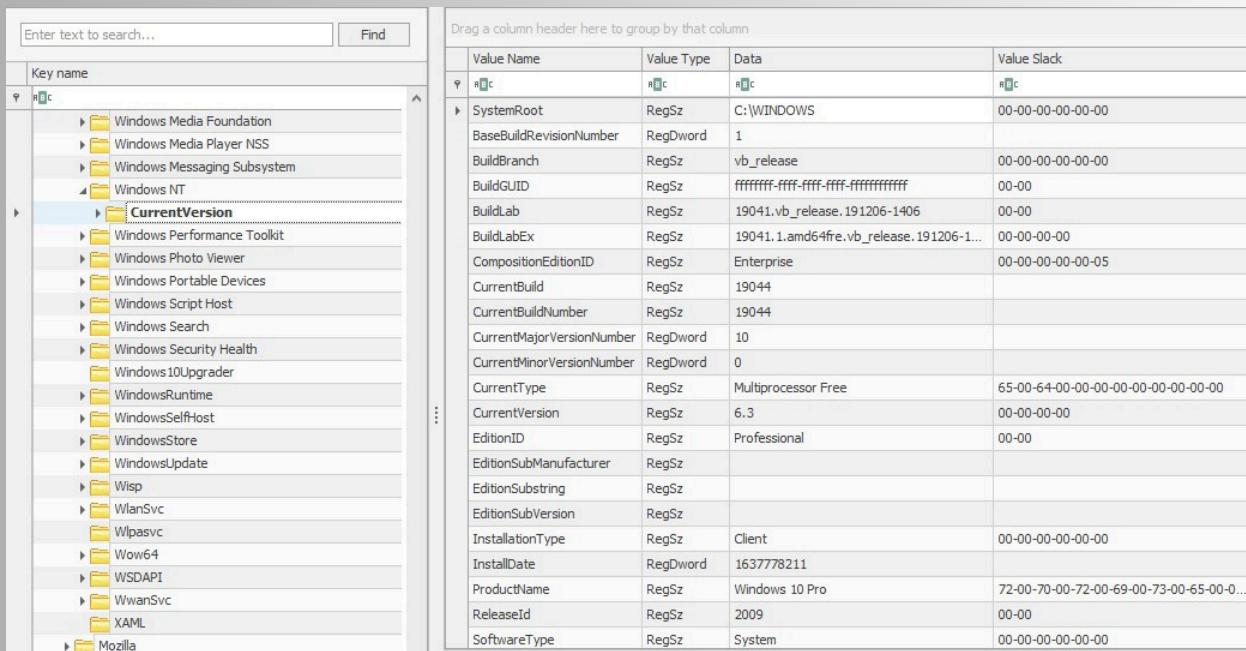


Simplified Explanation for Forensic Analysis Using the Windows Registry

When investigating a Windows system for forensic purposes, we can use the **Windows Registry** to gather important information about the system. Below are the key steps and what each part of the registry tells us:

1. Finding the OS Version

- To determine the **Operating System version** (e.g., Windows 10, Windows 11), we check the registry key:
SOFTWARE\Microsoft\Windows NT\CurrentVersion
- This key tells us the OS version from which the forensic data was collected.



Value Name	Value Type	Data	Value Slack
SystemRoot	RegSz	C:\WINDOWS	00-00-00-00-00-00
BaseBuildRevisionNumber	RegDword	1	
BuildBranch	RegSz	vb_release	00-00-00-00-00-00
BuildGUID	RegSz	ffffffff-ffff-ffff-ffff-ffffffff	00-00
BuildLab	RegSz	19041.vb_release.191206-1406	00-00
BuildLabEx	RegSz	19041.1.amd64fre.vb_release.191206-1...	00-00-00-00
CompositionEditionID	RegSz	Enterprise	00-00-00-00-00-05
CurrentBuild	RegSz	19044	
CurrentBuildNumber	RegSz	19044	
CurrentMajorVersionNumber	RegDword	10	
CurrentMinorVersionNumber	RegDword	0	
CurrentType	RegSz	Multiprocessor Free	65-00-64-00-00-00-00-00-00-00-00-00-00-00
CurrentVersion	RegSz	6.3	00-00-00-00
EditionID	RegSz	Professional	00-00
EditionSubManufacturer	RegSz		
EditionSubstring	RegSz		
EditionSubVersion	RegSz		
InstallationType	RegSz	Client	00-00-00-00-00-00
InstallDate	RegDword	1637778211	
ProductName	RegSz	Windows 10 Pro	72-00-70-00-72-00-69-00-73-00-65-00-0...
ReleaseId	RegSz	2009	00-00
SoftwareType	RegSz	System	00-00-00-00-00-00

2. Finding the Current Control Set

- Control Sets** store the system's configuration for startup. Commonly, there are two:
 - ControlSet001**: Represents the current configuration used during startup.
 - ControlSet002**: Stores the last known good configuration.
- To find the **CurrentControlSet** (the active one), look at: **SYSTEM\Select\Current**



- The **last known good configuration** is located at:
SYSTEM\Select\LastKnownGood

The screenshot shows a Windows registry editor window. At the top left is a search bar with placeholder text "Enter text to search..." and a "Find" button. To the right of the search bar is a table header row with columns "Value Name", "Value Type", and "Data". Below the header, there are four rows of data: "Current" (RegDword, 1), "Default" (RegDword, 1), "Failed" (RegDword, 0), and "LastKnownGood" (RegDword, 1). The main pane displays a tree view of registry keys under "Key name". A context menu is open over the "Select" key, listing options: "Select", "Setup", "Software", "State", "WaaS", and "WPA". A red asterisk icon with the text "Unassociated deleted values" is visible at the bottom left of the tree view.

3. Finding the Computer Name

- The **computer's name** helps confirm that we're investigating the right machine.
 - The registry key to find the computer name is:
SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName

<input type="text" value="Enter text to search..."/>	<input type="button" value="Find"/>				
Drag a column header here to group by that column					
Value Name	Value Type	Data	Value Slack		
Key name					
ComputerName	RegSz	a\c	a\c	a\c	a\c
(default)	RegSz	mmnsrvc	02-00-B0-00		
ComputerName	RegSz	THM-4N6	00-00-00-00		
ContentIndex					

4. Finding Time Zone Information

- Knowing the **time zone** helps us interpret timestamps (some are in UTC, others in local time).
 - Time zone information is found at:
SYSTEM\CurrentControlSet\Control\TimeZoneInformation



5. Finding Network Interfaces

- To see the **network interfaces** (like Wi-Fi or Ethernet adapters) on the machine, look at:
SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
- Each interface has a unique ID (GUID) with details like:
 - IPAddresses
 - SubnetMask
 - DNSServers
 - DHCPdetails

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
EnableDHCP	RegDword	1			
Domain	RegSz				
NameServer	RegSz				
DhcpIpAddress	RegSz	192.168.100.58	BA-00-B8-16-0A-00		
DhcpSubnetMask	RegSz	255.255.255.0			
DhcpServer	RegSz	192.168.100.1	35-00-00-00-65-00-7...		
Lease	RegDword	86400			
LeaseObtainedTime	RegDword	1637778828			
T1	RegDword	1637822028			
T2	RegDword	1637854428			
LeaseTerminatesTime	RegDword	1637865228			
AddressType	RegDword	0			
IsServerNapAware	RegDword	0			
DhcpConnForceBroadcastFlag	RegDword	0			
DhcpNameServer	RegSz	192.168.100.1			
DhcpDefaultGateway	RegMultiSz	192.168.100.1	00-00-00-00-00-00		
DhcpSubnetMaskOpt	RegMultiSz	255.255.255.0	00-00-00-00-00-00		
DhcpInterfaceOptions	RegBinary	FC-00-00-00-00-0...	00-00-00-00		
DhcpGatewayHardware	RegBinary	C0-A8-64-01-06-00-	2E-00-30-00-00-00		
DhcpGatewayHardwareCount	RegDword	1			

6. Finding Past Networks

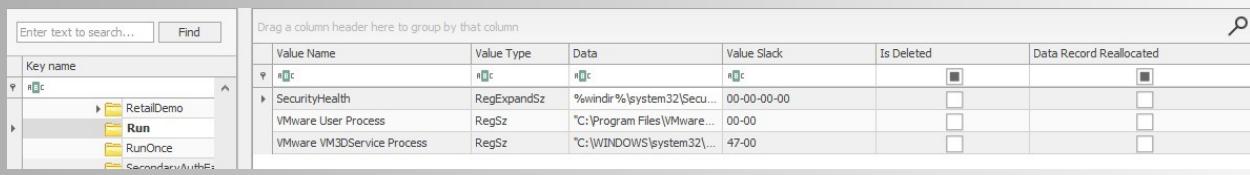
- To find **networks the machine was connected to previously**, use:
 - Unmanaged Networks:**
SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged
 - Managed Networks:**
SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed
- The last write time shows when the machine last connected to these networks.

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
ProfileGuid	RegSz	{A3D7C922-7D34-4688...}	CA-63-7F-00-CA-99		
Description	RegSz	Network 2			
Source	RegDword	8			
DnsSuffix	RegSz	eu-west-1.compute.int...	F5-48-81-00-F5-57		
FirstNetwork	RegSz	Network 2			
DefaultGatewayMac	RegBinary	02-D4-DB-FF-33-74	87-01-C0-51-87-01		



7. Finding Programs that Start Automatically (Autoruns)

- Programs or commands that run automatically during login can be found at:
 - NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run**
 - SOFTWARE\Microsoft\Windows\CurrentVersion\Run**
 - SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce**
- To check for **services that start at boot**, look at:
SYSTEM\CurrentControlSet\Services
 ○ If the **Startkey** is set to **0x02**, it means the service starts at boot.

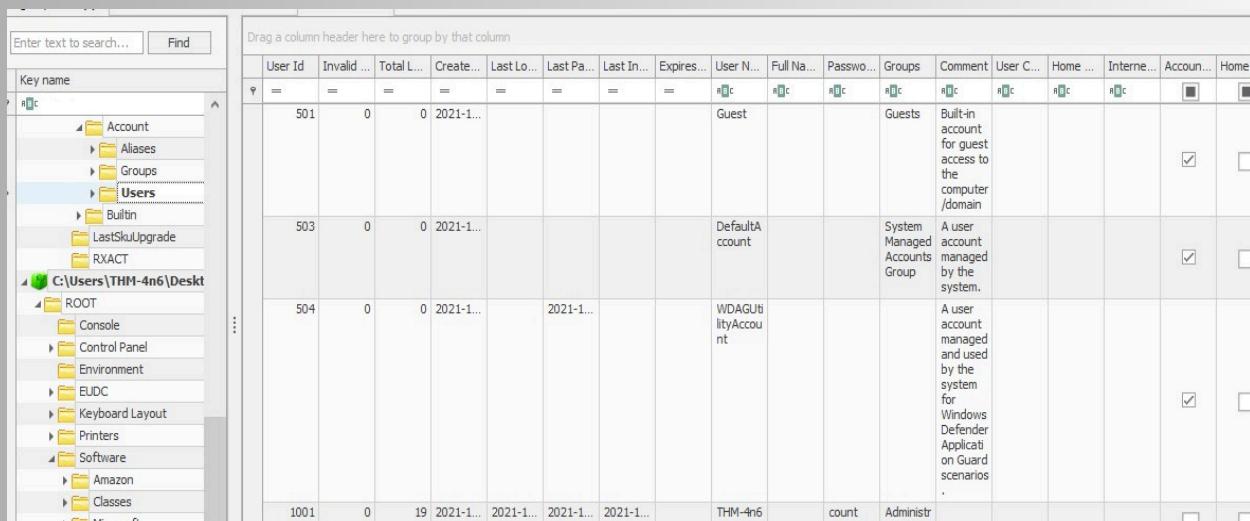


The screenshot shows the Autoruns interface. On the left, there's a tree view of registry keys under 'Key name'. On the right, a table lists registry entries with columns for Value Name, Value Type, Data, Value Slack, Is Deleted, and Data Record Reallocated.

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
RetailDemo	RegSz	%windir%\system32\Secu...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Run	RegExpandSz	VMware User Process	00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
RunOnce	RegSz	VMware VM3DService Process	47-00	<input type="checkbox"/>	<input type="checkbox"/>
SecondaryAuthEz					

8. Finding User Information (SAM Hive)

- The **SAM hive** (Security Accounts Manager) contains user account details such as:
 - Usernames and IDs (RIDs)**
 - Number of logins
 - Last login and failed login times
 - Password policy (e.g., expiry, hints, etc.)
 - Groups the user belongs to
- This information is located at:
SAM\Domains\Account\Users



The screenshot shows the Windows Registry Editor with the path 'C:\Users\THM-4n6\Desktop' selected. On the left, a tree view shows various registry keys like Account, Aliases, Groups, and Users. On the right, a table lists user accounts with columns for User Id, Invalid..., Total L..., Create..., Last Lo..., Last Pa..., Last In..., Expires..., User N..., Full Na..., Passwo..., Groups, Comment, User C..., Home ..., Interne..., Accoun..., and Home .

User Id	Invalid...	Total L...	Create...	Last Lo...	Last Pa...	Last In...	Expires...	User N...	Full Na...	Passwo...	Groups	Comment	User C...	Home ...	Interne...	Accoun...	Home .
501	0	0	2021-1...					Guest			Guests	Built-in account for guest access to the computer /domain			<input checked="" type="checkbox"/>	<input type="checkbox"/>	
503	0	0	2021-1...					DefaultA			System Managed Accounts Group	A user account managed by the system.			<input checked="" type="checkbox"/>	<input type="checkbox"/>	
504	0	0	2021-1...		2021-1...			WDAGUtilityAccou				A user account managed and used by the system for Windows Defender Application Guard scenarios.			<input checked="" type="checkbox"/>	<input type="checkbox"/>	
1001	0	19	2021-1...	2021-1...	2021-1...	2021-1...		THM-4n6		count	Administrators				<input type="checkbox"/>	<input type="checkbox"/>	



Why Is This Information Important?

- **OSVersion:** Helps identify the type of system you're analyzing.
- **ControlSets:** Determines system configurations during startup.
- **ComputerName:** Confirms the machine's identity.
- **TimeZone:** Helps create a timeline of events.
- **NetworkInterfaces and Past Networks:** Tracks network connections and IP addresses.
- **Autoruns:** Finds programs/services that run on startup (potentially malicious ones).
- **SAMHive:** Provides detailed user account and login activity information.

This data is critical for piecing together evidence during a forensic investigation

Recent Files

- **What is it?**

Windows keeps a record of files that a user recently opened. This is visible in "Recent Files" in Windows Explorer.

- **Where is it stored?**

This information is stored in the **NTUSER.DAT** file under the registry path:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Drag a column header here to group by that column						
	Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On
RecentDocs	7	EZtools	EZtools.lnk	=	0	2021-12-01 13:00:34
RecentDocs	6	Settings	Settings.lnk	=	1	2021-11-30 10:56:23
RecentDocs	5	WallpaperSettings.xml	WallpaperSettings.lnk	=	2	2021-11-30 10:56:21
RecentDocs	4	System and Security	System and Security.lnk	=	3	
RecentDocs	3	::{BB06C0E4-D293-4F75-8A90-CB05B6477EEE}	System.lnk	=	4	
RecentDocs	1	KAPE	KAPE.lnk	=	5	
RecentDocs	0	Get-KAPEUpdate.ps1	Get-KAPEUpdate.lnk	=	6	2021-11-24 18:18:48
RecentDocs	2	ChangeLog.txt	ChangeLog.lnk	=	7	2021-11-24 18:18:48
Folder	2	Settings	Settings.lnk	=	0	2021-11-30 10:56:23
Folder	1	System and Security	System and Security.lnk	=	1	
Folder	0	KAPE	KAPE.lnk	=	2	
.xml	0	WallpaperSettings.xml	WallpaperSettings.lnk	=	0	2021-11-30 10:56:21
.txt	0	ChangeLog.txt	ChangeLog.lnk	=	0	2021-11-24 18:18:48
.ps1	0	Get-KAPEUpdate.ps1	Get-KAPEUpdate.lnk	=	0	2021-11-24 18:18:48

- **How does it work?**

Registry Explorer organizes these files, showing the **Most Recently Used (MRU)** file at the top. You can also check specific file types, such as PDFs or Word documents.



For example:

`NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf`

This shows a list of recently opened PDF files.

- **What else can we find?**

It even includes the **last opened time** for each file.

Office Recent Files

- **What is it?** Microsoft Office also keeps a list of recently opened files (like Word documents, Excel sheets, etc.). **Where is it stored?** This information is stored in the **NTUSER.DAT** file under paths like:
 - `NTUSER.DAT\Software\Microsoft\Office\VERSION`
Here, "VERSION" depends on the Office version. For example: Office 2013 = **15.0** Office 2016 = **16.0** Office 365 uses the user's **Live ID** for storing recent files.
What does it include? The registry stores the **complete path** of recently opened files.
 -
 -
 -
-

ShellBags

- **What is it?**

Windows remembers the layout and view settings (e.g., list, details, icons) for folders that users open.

- **Why is it important?**

This data can show **folders recently accessed** by a user, which is useful in forensic analysis.

- **Where is it stored?**

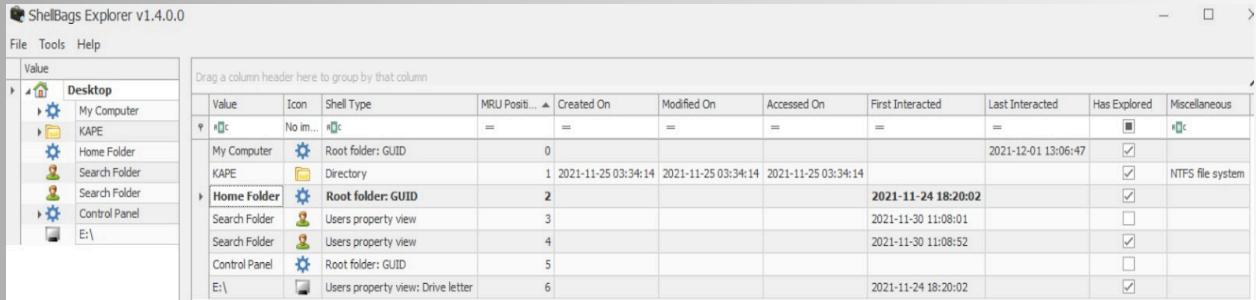
The information is in the following registry keys:

1. `USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags`
2. `USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU`
3. `NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU`
4. `NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags`



- **How do we analyze it?**

Tools like **ShellBag Explorer** (by Eric Zimmerman) make it easy to interpret this data.



The screenshot shows the ShellBag Explorer interface. On the left, there's a sidebar with icons for Desktop, My Computer, KAPE, Home Folder, Search Folder, and Control Panel. The main area displays a table of MRU items:

Value	Icon	Shell Type	MRU Positi...	Created On	Modified On	Accessed On	First Interacted	Last Interacted	Has Explored	Miscellaneous
My Computer	My Computer	No im...	=	=	=	=	=	=	<input checked="" type="checkbox"/>	
KAPE	KAPE	Root folder: GUID	0					2021-12-01 13:06:47	<input checked="" type="checkbox"/>	
Home Folder	Home Folder	Directory	1	2021-11-25 03:34:14	2021-11-25 03:34:14	2021-11-25 03:34:14			<input checked="" type="checkbox"/>	NTFS file system
Search Folder	Search Folder	Root folder: GUID	2				2021-11-24 18:20:02		<input checked="" type="checkbox"/>	
Search Folder	Search Folder	Users property view	3				2021-11-30 11:08:01		<input type="checkbox"/>	
Control Panel	Control Panel	Users property view	4				2021-11-30 11:08:52		<input checked="" type="checkbox"/>	
E:\	E:\	Control Panel	5						<input type="checkbox"/>	
		Control Panel	6				2021-11-24 18:20:02		<input checked="" type="checkbox"/>	
		E:\								

Open/Save and LastVisited Dialog MRUs

- **What is it?**

When you open or save a file in Windows, a dialog box appears. Windows **remembers the last location** where you opened/saved files.

- **Where is it stored?**

This data is saved in the following registry keys:

1. NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU
2. NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU



The screenshot shows the Windows Registry Editor. The left pane shows a tree structure with a search bar and a 'Find' button. The right pane shows a table of registry entries:

Value Name	MrU Position	Executable	Absolute Path	Opened On
0	0	notepad.exe	My Computer\C:\Program Files\Amazon\Ec2ConfigService\Settings	2021-11-30 10:56:19

- **Why is it important?**

It helps forensic analysts find **recently opened/saved files** and their locations.

Windows Explorer Address/Search Bars

- **What is it?**

Windows Explorer keeps a record of:

1. Paths typed in the address bar (e.g., "C:\Users\Documents").
2. Searches made in the search bar.



● Where is it stored?

1. Address bar paths:

`NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths`

2. Search bar queries:

`NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery`

● Why is it useful?

This data provides insights into user activity, such as **locations accessed** and **queries searched**.

Drag a column header here to group by that column					
Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
url1	RegSz	C:\	72-00-6F-00-67-00-72-00-61-	<input type="checkbox"/>	<input checked="" type="checkbox"/>
url2	RegSz	C:\Program Files	33-00-32-00-00-00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
url3	RegSz	C:\Windows\System32	60-53-09-00	<input type="checkbox"/>	<input type="checkbox"/>

Key Takeaways

1. **RecentFiles**: Tracks files opened recently by type and time.
2. **OfficeRecentFiles**: Tracks recent Microsoft Office documents.
3. **ShellBags**: Records folder layouts and access history.
4. **Open/SaveDialogs**: Shows recently accessed file locations.
5. **ExplorerActivity**: Tracks typed paths and search queries.

Each of these can provide critical information about a user's activities on a system during forensic analysis.

Here's a simplified explanation of these Windows artifacts and their purposes, written in easy-to-understand language:



1. UserAssist

- **What it is:** Windows keeps track of programs you open using Windows Explorer. This is saved in the **UserAssist** registry key for each user. It helps Windows know which programs you use most often.

Location in Registry:

`NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count`

Registry hives (1) Available bookmarks (31/0)		Values	UserAssist			
		Enter text to search...	Find			
Key name		Program Name	Run Counter	Focus Count	Focus Time	Last Executed
↳	↳	UEME_CTLCUACount:ctor	=	=	=	=
↳	↳	(Common Programs)\Accessories\Snipping Tool.lnk	9	0	0d, 0h, 00m, 00s	2021-11-25 03:14:34
↳	↳	UEME_CTLSESSION	54	0	0d, 0h, 00m, 00s	2021-11-25 03:14:34
↳	↳	(Common Programs)\Accessories\Paint.lnk	7	0	0d, 0h, 00m, 00s	2021-11-25 03:14:34
↳	↳	(Programs)\Accessories\Notepad.lnk	6	0	0d, 0h, 00m, 00s	2021-11-25 03:14:34
↳	↳	(User Pinned)\Taskbar\File Explorer.lnk	26	0	0d, 0h, 00m, 00s	2021-12-01 13:02:43
↳	↳	(Program)\Windows PowerShell\Windows PowerShell.lnk	1	0	0d, 0h, 00m, 00s	2021-11-25 03:37:24
↳	↳	(User Pinned)\Taskbar\Firefox.lnk	2	0	0d, 0h, 00m, 00s	2021-12-01 12:32:34
↳	↳	(Common Programs)\Accessories\Remote Desktop Connection.lnk	1	0	0d, 0h, 00m, 00s	2021-11-25 03:59:55
↳	↳	(User Pinned)\Taskbar\Opera Browser.lnk	1	0	0d, 0h, 00m, 00s	2021-11-25 04:10:02
↳	↳	(Common Programs)\Accessories\Notepad.lnk	1	0	0d, 0h, 00m, 00s	2021-11-30 10:55:21

- **What it stores:**
 - The name of the program.
 - The number of times the program was opened.
 - The last time the program was launched.
- **Limitations:** Programs launched from the command line are **not** recorded here.
- **Tools to View:** Use **Registry Explorer** to view this data.

2. ShimCache (Application Compatibility Cache)

- **What it is:** ShimCache tracks all programs launched on your system. It was designed to help old programs work with newer versions of Windows (backward compatibility).

Location in Registry:

`SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache`

- **What it stores:**
 - Filenames of the programs.
 - File size.
 - Last modified time (not the execution time).



- **How to Read:** ShimCache data is not easy to read directly in Registry Explorer. Instead, use the **AppCompatCache Parser** tool. It can convert the data into a CSV (spreadsheet) file that shows the information clearly.

EZViewer v1.0.0.0 - 20211202213532_Windows10Creators_SYSTEM_clean_AppCompatCache.csv						
File	Tools	Help				
A	B	C	D	E	F	G
1 ControlSet	CacheEntry Path		LastModifiedTimeUTC	Executed	Duplicate SourceFile	
2 1	0 C:\Users\THM-4n6\Desktop\KAPE\kape.exe		6/24/2021 6:23 NA	FALSE	C:\Users\THM-4n6\Desktop\SYSTEM_clean	
3 1	1 C:\Users\THM-4n6\Desktop\KAPE\kape.exe		6/24/2021 6:23 NA	FALSE	C:\Users\THM-4n6\Desktop\SYSTEM_clean	
4 1	2 C:\Program Files\Common Files\microsoft shared\ink\TabTip.exe		10/6/2021 13:52 NA	FALSE	C:\Users\THM-4n6\Desktop\SYSTEM_clean	
5 1	3 C:\Windows\System32\rdpinput.EXE		12/7/2019 9:09 NA	FALSE	C:\Users\THM-4n6\Desktop\SYSTEM_clean	
6 1	4 C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsv.exe		10/6/2021 13:45 NA	FALSE	C:\Users\THM-4n6\Desktop\SYSTEM_clean	
7 1	5 C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorwv.exe		10/6/2021 13:45 NA	FALSE	C:\Users\THM-4n6\Desktop\SYSTEM_clean	

Command to Use Parser:

```
AppCompatCacheParser.exe --csv <output file path> -f <SYSTEM hive file path> -c <control set>
```

3. AmCache

- **What it is:** AmCache is similar to ShimCache but provides more detailed information about programs that were run on the system.

Location in File System:

C:\Windows\appcompat\Programs\Amcache.hve

- **What it stores:**
 - Execution path (where the program was launched from).
 - Installation, execution, and deletion times of the program.
 - The SHA-1 hash of the program (used for security checks).

Registry Key for Last Run Programs:

Amcache.hve\Root\File\{Volume GUID}\

- **Tools to Use:** Use **Registry Explorer** to view AmCache data.

Registry hives (3) Available bookmarks (6,1)							
Values		Amcache-InventoryApplicationFile					
Enter text to search... <input type="text"/>		Find <input type="button" value="Find"/>					
<i>Drag a column header here to group by that column</i>							
Key name	Path	Timestamp	Path	Name	Product Name	Publisher	Version
+	+ C:\Users\THM-4n6\Desktop\WUSERL...	2021-12-01 12:45:37	+ C:\program files\windows\microsoft\micros...	3DViewer.exe	view 3d	microsoft corporation	7.2107.7012.0
+	+ C:\Users\THM-4n6\Desktop\SYSTEM...	2021-12-01 12:55:19	+ C:\program files\7-zip\7z.exe	7z.exe	7-zip	igor pavlov	19.00
+	+ C:\Users\THM-4n6\Desktop\Amcache...	2021-12-01 12:55:19	+ C:\program files\7-zip\7zfm.exe	7ZFM.exe	7-zip	igor pavlov	19.00
+	+ C:\Users\THM-4n6\Desktop\Amcache...	2021-12-01 12:55:19	+ C:\program files\7-zip\7zq.exe	7Zq.exe	7-zip	igor pavlov	19.00
+	+ C:\Users\THM-4n6\Desktop\Amcache...	2021-12-01 13:00:29	+ C:\program files\x86\google\Update\download\{0e69345-d...	96.0.4664.45_chrome_installer.exe		google llc	96.0.4664.45
+	+ C:\Users\THM-4n6\Desktop\Amcache...	2021-12-01 12:55:49	+ C:\program files\amazon\ssm\amazon-ssm-agent.exe	amazon-ssm-agent.exe			e576619157059378588d702385f45707a3089
+	+ C:\Users\THM-4n6\Desktop\Amcache...	2021-12-01 12:57:38	+ C:\programdata\package cache\71aad04f-4efc-78d4-6f7f21aa...	AmazonSSMagentSetup.exe	Amazon ssm agent	amazon web services	3.1.338.0
+	+ C:\Users\THM-4n6\Desktop\Amcache...	2021-12-01 13:00:20	+ C:\users\thm-4n6\desktop\amcacheparser.exe	AmcacheParser.exe	amcacheparser	eric zimmerman	14.0.0



4. BAM/DAM

● What is:

- **BAM(BackgroundActivityMonitor):** Keeps track of programs running in the background.
- **DAM/DesktopActivityModerator:** Manages power consumption by controlling app activities.

Location in Registry:

sql

Copy code

`SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}`

`SYSTEM\CurrentControlSet\Services\dam\UserSettings\{SID}`

- Here, **SID** refers to the unique user ID on the computer.
- **What it stores:**
 - Program names and their full paths.
 - The last time the program was executed.
- **Tools to Use:** Use **Registry Explorer** to view this data.

Registry hives (3) Available bookmarks (61/0)		Values	BamDam
<input type="text"/> Enter text to search... <input type="button" value="Find"/>			
Key name		Program	Execution Time
bam		Microsoft.Windows.ShellExperienceHost_cw5n1h2bxwyewy	2021-11-24 18:02:15
State		Microsoft.Windows.Cortana_cw5n1h2bxwyewy	2021-11-24 18:02:15
UserSettings		[Device]\HarddiskVolume2\Windows\explorer.exe	2021-11-24 18:02:15
S-1-5-18		[Device]\HarddiskVolume2\Windows\System32\ApplicationFrameHost.exe	2021-11-24 18:02:15
S-1-5-21-417449583-1		windows.immersivecontrolpanel_cw5n1h2bxwyewy	2021-11-24 15:40:31
S-1-5-90-0-1		[Device]\HarddiskVolume2\Program Files\VMware\VMware Tools\vmtoolsd.exe	2021-11-24 18:02:14
S-1-5-90-0-2		[Device]\HarddiskVolume2\Windows\System32\cmd.exe	2021-11-25 03:23:14
BasicDisplay		[Device]\HarddiskVolume2\Program Files(x86)\Mozilla\Firefox\firefox.exe	2021-11-25 03:46:20
BasicRender		[Device]\HarddiskVolume2\Program Files(x86)\Google\Update\GoogleUpdate.exe	2021-11-25 03:43:40
BattC		[Device]\HarddiskVolume2\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	2021-11-24 17:56:18
BcastDVRUserService		[Device]\HarddiskVolume2\Windows\System32\notepad.exe	2021-11-25 03:42:53
BcastDVRUserService_7a6b6		[Device]\HarddiskVolume2\Users\THM-493\AppData\Local\Programs\Opera\opera.exe	2021-11-25 04:12:35
bcmf2		[Device]\HarddiskVolume2\Program Files\Google\Chrome\Application\chrome.exe	2021-11-25 03:43:50
BDESVIC		[Device]\HarddiskVolume2\Windows\System32\instreq.exe	2021-11-25 04:00:04
Beep		[Device]\HarddiskVolume2\Windows\System32\systemSettingsAdminFlows.exe	2021-11-25 04:00:54
BFE		[Device]\HarddiskVolume2\Windows\System32\SystemPropertiesComputerName.exe	2021-11-25 04:01:35
bindit		[Device]\HarddiskVolume2\Windows\System32\undll32.exe	2021-11-24 17:38:19
BTTS		[Device]\HarddiskVolume2\Program Files(x86)\Windows\InstallationAssistant\Windows10UpgraderApp.exe	2021-11-24 18:01:52
BluetoothUserService		[Device]\HarddiskVolume2\Program Files(x86)\Microsoft\Edge\Update\MicrosoftEdgeUpdate.exe	2021-11-24 15:21:35
BluetoothUserService_7a6b6		[Device]\HarddiskVolume2\Program Files(x86)\Microsoft\Edge\Application\msedge.exe	2021-11-24 15:23:43
bowser			
Total rows: 21		
			Export ?

Summary:

- **UserAssist:** Tracks programs opened using Windows Explorer.
- **ShimCache:** Tracks all launched programs for compatibility purposes.
- **AmCache:** Stores more detailed data about executed programs, including their installation times and security hashes.
- **BAM/DAM:** Monitors background apps and optimizes power usage.



1. Device Identification

- **Purpose:** Tracks USB devices connected to the system, including their **Vendor ID**, **Product ID**, and **Version**.

Registry Keys:

SYSTEM\CurrentControlSet\Enum\USBSTOR

SYSTEM\CurrentControlSet\Enum\USB

Registry hives (3) Available bookmarks (61 0)		Values	USBSTOR
Enter text to search... <input type="button" value="Find"/>			
Drag a column header here to group by that column.			
Key name	Timestamp	Manufacturer	Title
USB\VEN_KINGSTON\Prod_DataTraveler Rev_PMAP	2021-11-24 18:25...	Ven_Kingston	Prod_DataTraveler Rev_PMAP
USB\VEN_USBS3.0\Prod_External_Device Rev_SDKM1	2021-11-24 18:27...	Ven_USB3.0	Prod_External_Device Rev_SDKM1

- **What it shows:**
 - Unique device details (e.g., vendor, product).
 - Connection timestamps.
 - **Tool:** Use **Registry Explorer** to view this information in a readable format.

2. First/Last Connection and Removal Times

- **Purpose:** Tracks the first connection, last connection, and last removal times of USB devices.

Registry Key:

SYSTEM\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USBSerial#\Properties\{83da6326-97a6-4088-9453-a19231573b29}\####

- Replace ##### with:
 - 0064→Firstconnectiontime.
 - 0066→Lastconnectiontime.
 - 0067→Lastremovaltime.
 - **Tool: Registry Explorer** automatically shows this data under the **USBSTOR** key.



3. USB Device Volume Name

- **Purpose:** Identifies the **volumename** of the connected USB device.

Registry Key:

SOFTWARE\Microsoft\Windows Portable Devices\Devices

- **What to do:** Match the **GUID** here with the **Disk ID** from the **USBSTOR** key to link the volume name with the specific USB device.

Timestamp	Device	Serial Number	Guid	Friendly Name
2021-11-25 07:16:54			{E251921F-4DA2-11EC-A783-001A7DDA7110}	USB
2021-11-25 07:16:54			{F529A9D6-4D9E-11EC-A782-001A7DDA7110}	New Volume

