Importance of Registry Forensics in Digital Crime Investigations Involving Windows Machines

Nagendar Rao Koppolu
Inspector of Police (In-charge State Cyber Vertical),
Telangana Police Department, Hyderabad, India

Abstract
Windows Registry is a centralised repository maintained by the Windows operating system to store configuration settings and related data that enable the smooth running of a computer and its applications. Applications installed on a computer may also use the Registry to store various application-specific settings. This paper discusses the role and importance of Windows Registry for an investigator when performing a forensic analysis of a Windows computer. The structure of Windows Registry, important datasets stored in the Registry by the operating system and applications, and locations of registry keys that need special attention of an investigator are highlighted. The methods to collect the artifacts available in the Registry and the challenges of Windows Registry forensics are also discussed.

Keywords
Windows Registry, Artifacts, forensics, cybercrime investigation, Microsoft Windows.

I. Introduction
Microsoft Windows is one of the most popular operating systems used approximately in 1 billion active Personal Computers (PCs), which accounts for around 75% of the PC market. Windows Server operating system is used approximately in 38% of servers globally. In the world of technology-driven crimes, understanding the technical aspects of Microsoft Windows is crucial for digital forensics investigators and law enforcement officers for enhanced investigative outcomes.
The Windows Registry is a customizable repository maintained by Windows operating system. It stores configurations for installed applications, hardware devices, and Windows operating systems. Any changes such as device customization, system up-gradation, user profiles, file type association with applications, user history, etc. can be found in Windows Registry.
Analysing the contents of Windows Registry would always help an investigator to understand the environment in which the computer was running and to fill the digital gaps considered necessary for investigation purposes. Hence, Windows Registry is a valuable tool for a diligent investigator [7].

II. Windows Architecture :
At a high level, Windows operating system comprises a kernel and a shell. Windows kernel creates and executes application processes and provides access to hardware resources, such as memory, storage, CPU, etc. Users can access applications, files, and folders using the shell. Both the shell and the running applications reside in the user space of the operating system.

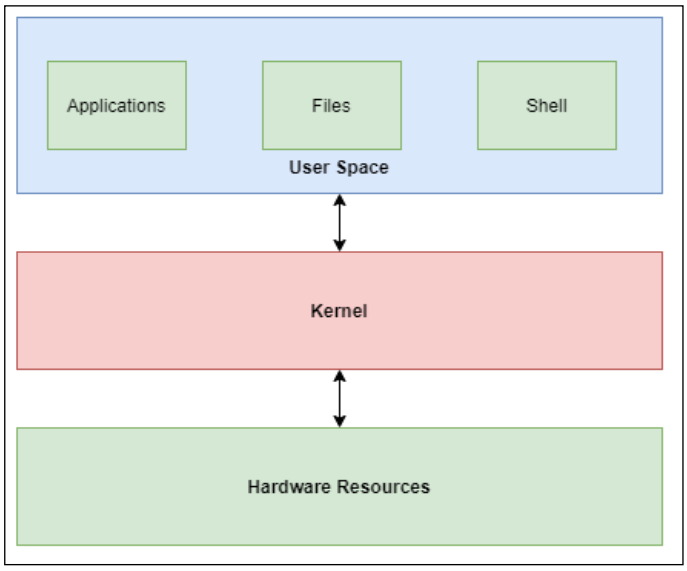


Fig. 1. Windows Architecture

In the above image (Figure 1), "Applications" refers to both third-party applications and applications bundled with the operating system, such as Windows Registry, Windows Event Viewer, Recycle Bin, Windows Explorer, Control Panel, etc.

III. Windows Registry
Windows Registry is a key-value database in which keys are stored in a hierarchical (tree) structure by the operating system. It is integral to the functioning of Microsoft Windows. Windows kernel, device drivers, operating system services, and applications use the Registry to store their configuration settings. Third-party applications installed on the computer may also use the Registry to store application-specific configurations and

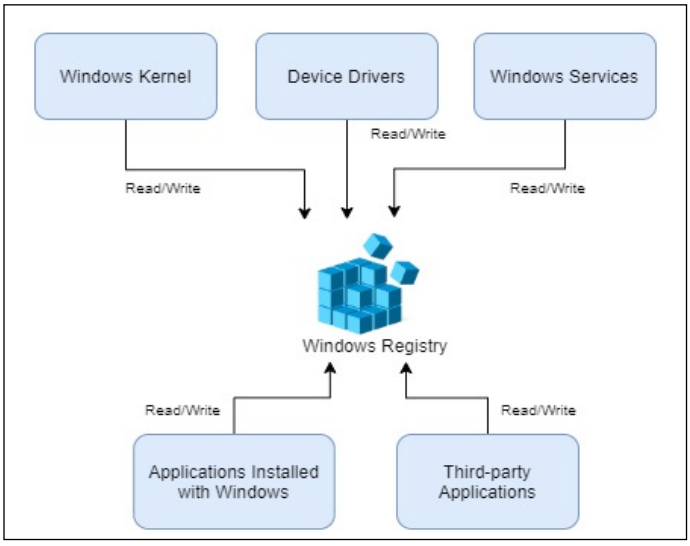


Fig.2. System Component Accessing Windows Registry

related data. Examples of configurations and related data that are stored by the operating system and applications may include a list of installed applications, a list of recently accessed files, details of hardware peripherals, and positions of application user interface components. Any application may use the Registry to store configurations and related data. Identifying such data, which is of investigative value, is the primary purpose of Windows Registry forensics [8].

Windows Registry is unique in many ways. No other operating system uses a centralized database to store an operating system and application-specific configurations and certain application data such as recently accessed files. Some applications on these operating systems may ignore this convention and store their configuration files in a different folder path. Configuration files in other operating systems are in text formats, whereas contents of files that form Windows Registry are in a binary format.

Windows uses the Registry to store key information such as:

1. List of file extensions and associated applications
2. List of COM and ActiveX controls registered by the operating system and applications
3. Installed applications
4. Installed services
5. Start-up applications
6. Hardware configuration and settings
7. Operating System configuration and settings.

A careful observation of the above-mentioned aspects will help the investigator understand the environment on the Windows machine and certain user actions.

A. Application-specific Settings

Applications can use some command-line parameters, which are data items that can be passed to the application when it is launched. Environment variables are variables with a name and value that are used by applications to obtain details such as the system path, temp folder path, etc. The Registry can be used to store these application launch parameters and environment variables.

Applications can also store their state in the Registry, such as the positions and sizes of various application frontend components (e.g., text fields, buttons, toolbars) and list of recently accessed files. Such settings can be stored at both the user and system levels. If an application is installed for multiple users on a computer, its settings for each user can be stored separately in the Registry. Global settings of the application (which are not user-specific) are also stored within the Registry, but in a separate location.

B. Significance of Windows Registry

Windows Registry is designed to be used by applications and not by end-users. Applications use the Registry, based on the needs of the application, to store application configurations and user activities.

As Windows Registry stores configuration details in a binary format, applications can use various data types (e.g., numeric, text, date/time) to store their configurations. Accessing the keys and values in the Registry is much faster in the binary format. Applications can also support multiple users on a computer easily by storing their user-specific configurations in separate locations within the Registry.

In a forensics investigation involving cybercrime, investigators focus on analysing the data (files, folders, and other records) created by the users. Additional analysis conducted on the contents of Windows Registry enables the investigators to understand the manner in which the users may have interacted with applications and the operating system. This may, sometimes, allow the investigator to connect the dots during the investigation.

Analysing the contents of Windows Registry is analogous to looking under the hood of a car involved in a crime to obtain details such as the make, model, and chassis number. Adding such supporting information to the evidence definitely strengthens the case.

C. Accessing Windows Registry

On a computer running Windows operating system, contents of Windows Registry can be explored using an in-built application called the Registry Editor, and it can be launched by *regedit* command. On a forensic disk image, *regedit* command cannot be used. Digital forensics applications provide their own mechanisms to explore the contents of the Registry of a disk image. Regedit command can only be used on a live system.

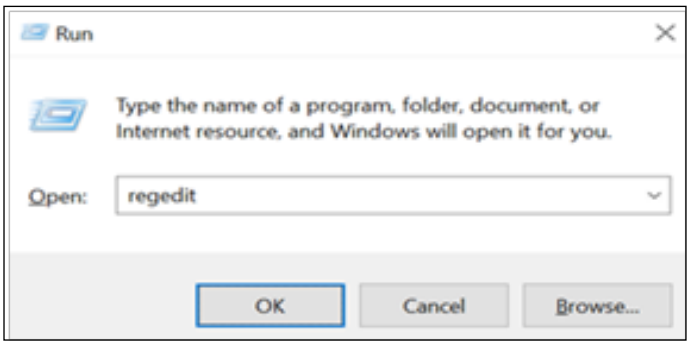


Fig. 3. Run Command Window

Administrator privileges are required to access the Registry Editor. Changes made to the Registry are auto-saved. There is no undo operation, and hence, registry operations using the Registry Editor should be handled carefully. When examining a forensic disk image, the contents of Windows Registry can be explored using a digital forensics software application. Windows stores entries of the Registry in several files. These files are located at:

<Windows Installation Folder>\System32\config (typically C:\Windows\System32\config)

As mentioned, the contents of the physical files containing the registry entries are in binary format. These files are collated by Windows and are shown in the Registry Editor in a tree structure. Digital forensics applications reverse engineer the binary formats to reconstruct the underlying tree structures and present the contents of the Registry within the digital forensics applications for investigator's understanding.

IV. Structure of Windows Registry

Windows Registry is a database containing keys and values. The keys are organized in a tree structure by the operating system. This section describes the organisation of the keys under specific categories called Hives. The hierarchical relationship among keys and their subkeys along with the associated list of values are also discussed in this section. Understanding the structure of the Registry is a prerequisite for any digital forensics professional.

A. Registry Hives

Following are the top-level nodes in the registry database under which specific categories of keys are stored:

1. HKEY_CLASSES_ROOT
2. HKEY_CURRENT_USER
3. HKEY_LOCAL_MACHINE
4. HKEY_USERS
5. HKEY_CURRENT_CONFIG

These nodes are called “Registry Hives” [1].
In figure 4, shown below, registry hives are organized under the parent node “Computer”.

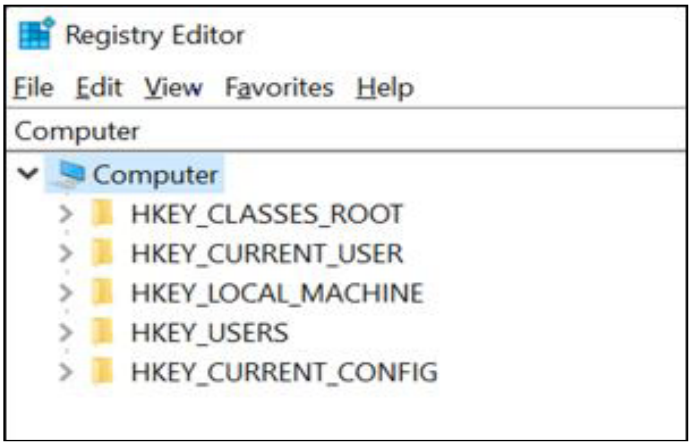


Fig. 4. Registry Editor with Hives

• HKEY_CLASSES_ROOT stores information related to file extensions (e.g., jpg, pdf), which are configured by installed applications. This hive also contains details of COM and ActiveX controls registered by the operating system and installed applications.
• HKEY_LOCAL_MACHINE contains data related to installed hardware and software. A list of hardware, network information and connected servers are also stored in this hive.
• HKEY_USERS stores environment variables (refer Section V-G: Environment Variables) and application settings of all the users of the system.
• HKEY_CURRENT_USER stores environment variables and application settings of the “current” user. In a forensics context, as there is no currently logged-in user within a disk image, the keys under the hives HKEY_USERS and HKEY_LOCAL_MACHINE can be used to retrieve environment variables, applications settings and other details for each of the system users.
• HKEY_CURRENT_USER is a direct reference to HKEY_USERS\ <<USER_SID>>. The configuration details and application settings of different users on the system are available under HKEY_USERS\<<USER_SID>>
• USER_SID refers to the security identifier which is assigned to each user by the operating system.
• HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ ProfileList
It contains a list of USER_SIDs along with respective profile paths.
• HKEY_CURRENT_CONFIG doesn’t store any information itself but instead acts as a pointer, or a shortcut, to a registry key that keeps the information about the hardware profile currently being used.
• HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\ Current.
This hive stores the hardware profile of the computer with information such as printers and other peripherals that were connected to the computer.

B. Registry Keys and Values

Each of the above-discussed hives may have multiple child keys. A child key is also referred to as a “subkey”. Each child key may further have multiple subkeys of its own and through such a parent-child relationship, a deep hierarchy evolves within a registry hive [2]

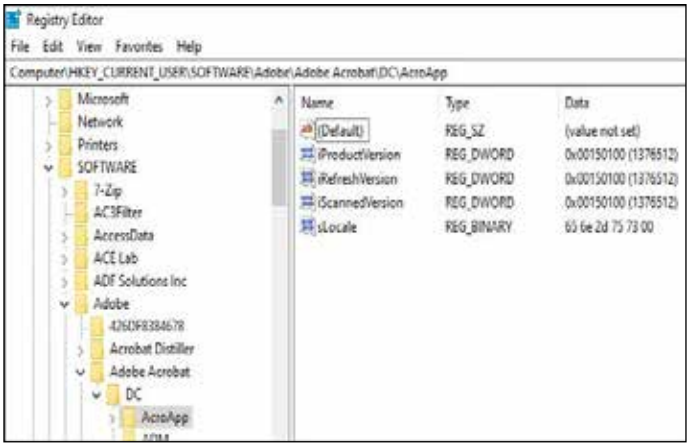


Fig. 5. Keys and Values in a Registry Hive

C. Keys and Subkeys

Understanding the keys and subkeys mechanism used by the Registry to store data is a prerequisite to understanding the overall structure of the Registry. Data within the Registry is always stored under one or more keys or subkeys within a hive.
In figure 5 (above), the tree nodes on the left pane represent the key hierarchy within the hive HKEY_CURRENT_USER. Referring again to figure 5, let us take an example of how the popular PDF viewer, Adobe Acrobat Reader uses the Registry. Its registry entries are stored under the following key path:
HKEY_CURRENT_USER → SOFTWARE→ Adobe → Acrobat Reader →DC →AcroApp
The key SOFTWARE is a subkey under the hive HKEY_CURRENT_USER. Its subkey is Adobe, whose subkey is Acrobat Reader. The company, Adobe, chose the above key path based on their preference. Windows do not enforce a naming convention or a key hierarchy for applications to store their registry entries. Each application chooses its own naming convention and key hierarchy based on its needs.
This ability of the Registry to store keys under the hives, and with the keys themselves having multiple subkeys, enables storing and presenting a deep hierarchy of keys and values. Such a mechanism helps application developers to store application settings and other such details within the Registry efficiently. As mentioned above, understanding such key hierarchy is important for an investigator to explore application-specific registry entries based on investigative needs

D. Values Associated with a Key

Values of a key or a subkey are the data stored in the registry key path by an application. Once a key path of an application is identified, retrieving the values stored under the key path helps the investigator in understanding the application-specific configurations and the actions performed by the user, wherever relevant.
Each key in the Registry, in addition to potentially having other subkeys, may also have multiple values associated

with it. In figure 5 above, the right pane has a list of items associated with the key "AcroApp". These items are called the values of the key.

For each value, there is a name, associated data type, and data. The data stored could be an application configuration or a user activity.

Following are some of the data types supported by the values of registry keys [3]:

- String
- Binary
- DWORD (32-bit) – 32-bit Unsigned Integer
- DWORD (64-bit) – 64-bit Unsigned Integer
- Multi-String – text with multiple lines
- Expandable String – text within these data items can refer to environment variables such as %USERPROFILE%, %PATH%.

Referring to figure 5, for the key AcroApp, the following are the details of its values:

Table 1. Example Registry Key Values

Value – Name	Data Type	Data
(Default)	REG_SZ (String)	(value not set)
iProductVersion	REG_DWORD (Unsigned Integer)	0x00150100
iRefreshVersion	REG_DWORD (Unsigned Integer)	0x00150100
iScannedVersion	REG_DWORD (Unsigned Integer)	0x00150100
sLocale	REG_BINARY (Binary)	65 6e 2d 75 73 00

From the above example, an investigator can understand the version of Adobe Acrobat Reader, the language used within the application, and other relevant data. Each set of registry keys, their subkeys and the values stored are very specific to how an application stores its configurations and other data. Some of the keys may store data pertaining to user actions and other keys may store application configurations. As mentioned, there is no enforcement from Windows on how applications may store their data within the Registry. Therefore, an investigator should explore different sections of the Registry to extract information useful for the investigation.

V. Windows Registry Forensics – Evidence from Keys Maintained by Windows :

This section provides details of important Windows Registry keys useful for an investigator. As mentioned in Section IV, Windows Registry is used by the operating system and applications installed on a computer. Windows Registry is not generally accessed by end-users. The data that is visible in Windows Registry is not directly created by a user but is created due to the user's interactions with applications and the operating system. By navigating through the registry entries, an investigator will be able to understand the interactions of the user with applications and the operating system.

Windows maintains a huge number of registry keys. It is very time-consuming to go through all the keys. The following sections highlight important areas of the Registry, which are useful from an investigation perspective as they indicate actions performed by the user of a computer.

Some important Registry Keys used by the Operating System are given in the following table:

Table 2: Important Registry Keys used by Windows

SN	Registry Path	Property
1	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ ProfileList	Contains a list of USER_SIDs along with respective profile paths
2	HKEY_USERS\<<USER_SID>>\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	Stores list of recently opened files.
3	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts	Stores list of file extensions with associated applications to open files with respective extensions.
4	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU	Stores list of recently opened and saved files from the Open/Save as dialog in applications
5	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	Stores list of applications and files that are launched from Windows Run dialog
6	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	Stores details of Windows installation
7	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	Stores details of applications installed on the computer
8	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services	Stores list of installed services
9	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	Stores list of applications that are launched whenever a user performs a login

10	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\Environment	Stores list of system-level environment variables
11	HKEY_USERS\<<USER_SID>>\Environment	Stores list of user-specific environment variables
12	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR	Stores list of USB devices connected to the computer
13	HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices	Stores mounted drive information
14	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation	Contains time zone information
15	HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS	Stores information related to the BIOS
16	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ NetworkList\ Profiles	Stores details of LAN/WiFi interfaces
17	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules	Contains rules configured on Windows Firewall
18	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2	Stores Mount Points/LAN Shares

A. List of Recently Launched Applications

Whenever a user launches an application, the operating system updates keys in the following location with the application path, last accessed date and time, and launch count (number of times the application was launched).

Locations:

1. HKEY_USERS\<<USER_SID>>\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\RecentApps
2. HKEY_USERS\<<USER_SID>>\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Search\RecentApps

From this list, an investigator can understand the activities performed by the user on the computer, especially those related to accessing various applications

B. List of Recently Accessed Files

Windows maintains a list of recently accessed files in the Registry. This list is updated whenever a user opens a file from Windows Explorer.

Location:

HKEY_USERS\<<USER_SID>>\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

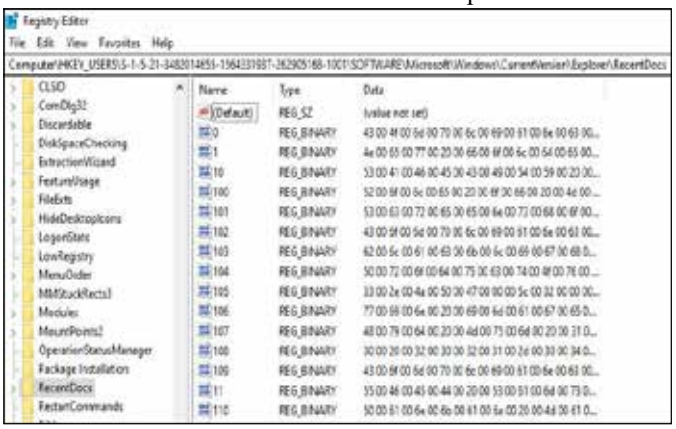


Fig. 6. RecentDocs Registry Key

The above-mentioned key stores a list of recently accessed files that are sorted and organized by file extension. The data component of the list items is in binary format. Digital forensics applications parse the binary format to extract the names and paths of the files. An investigator can use these registry entries to review files that were recently accessed by the user.

Many applications contain “Open” and “Save As” dialog boxes. When users run applications containing these dialog boxes and use the “Open” and “Save As” operations, the following subkeys are updated in the Registry:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32

The following key stores list of applications and files that were launched from the Windows Run dialog:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

Windows Run dialog is used by users when they would like to quickly launch an application or open a file, without clicking through the directory structure to reach the file in Windows Explorer

C. Windows Installation Related Information

Windows stores details of its own installation within the Registry. These registry keys contain details such as:

- Location of Windows installation
- Installation date and time
- Windows variant (Windows 10, Windows 10 Pro, etc.)
- Windows version and build number

Location:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

The investigator should append this information to their evidence of interest report as this information identifies the evidence computer.

D. Applications Installed on a Computer

Whenever a user installs an application, Windows creates a set of registry keys to store the details of the installed application. When an application is uninstalled, the corresponding registry keys are removed by the operating system. Hence, it is difficult for an investigator to identify uninstalled programs and their corresponding digital footprint in the computer system. In such cases, the investigator should rely on corroborative evidence created by such applications before uninstallation from the system. Uninstalled programs and their data may be available as deleted data on the disk. Digital forensics applications can recover such data if the clusters of the deleted data have not been overwritten.

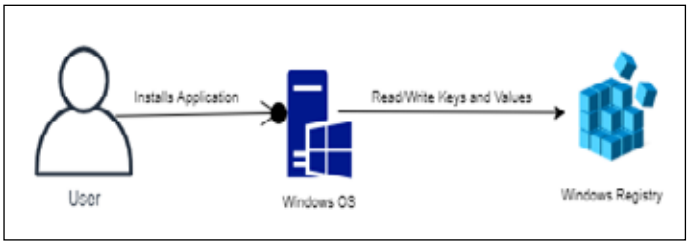


Fig. 7. Windows Registry and Installed Applications

Details of each installed application are stored as subkeys. The name of the application, its installation path, version number, and an installation date is stored for each of the application keys. Applications installed by the operating system may also have entries in the Registry. The Windows feature, "Add or remove programs", enumerates the list of installed applications using these registry keys.

Location:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

This data may be of immense value to an investigator in cases in which different types of applications were used to commit a cybercrime.

E. Installed Services

A service is a background application process that starts when a computer is booted. Services are used by the operating system and applications. Windows Print Service and Windows Update are examples of such services used by the operating system. Web servers and databases (such as MySQL) also run as services in the background. Windows maintains a list of configured services in the Registry along with their details such as:

- Name of the service
- Description
- Path to the executable that launches the service
- Dependencies to the service
- Start-up type of the service - whether the service is automatically or manually launched

Location:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

Details of each configured service are available as subkeys under the above key.

The list of services on a computer may help an investigator understand if there is a backend database or a web server or any other such application which may be storing user-generated data.

There may be other backend services that are installed by the operating system or applications but may not contain data that is generated by users. The investigator should focus on those services that capture data provided by the users.

Here are some examples of applications that run as backend services:

- Webservers such as Apache web server, Apache Tomcat application server, Microsoft Internet Information Services (IIS)
- Databases such as Oracle, MySQL, Microsoft SQL Server, etc.

Such services are typically configured on Windows Server systems and occasionally even on Windows consumer versions, such as Windows 10.

These services encapsulate applications that may process and store information pertaining to corporate operations and financial transactions. Companies use software systems such as CRM (Customer Relationship Management) and ERP (Enterprise Resource Planning) to store their transactions with customers and in various organisational processes, including payroll and procurement. These systems use backend databases and web servers to store data and to provide application access to end-users. Based on the nature of the investigation, extracting data from the services using vendor-specific tools may yield important evidence.

F. Start-up Applications

Some applications may have been configured to run automatically when a user logs-in. Windows maintains a list of such applications in the Registry.

Locations:

1. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
2. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

List of applications that are launched whenever a user performs a login is stored in the above keys. It may be of use for an investigator to review and analyse the files created by these applications.

RunOnce is a special key. This key is removed by the operating system automatically after the application mentioned in the key is run once. It is typically used by application installers to clean up files and folders after an application is installed or uninstalled and the system is rebooted. This key, if it exists, be of use to understand the last application installation or uninstallation made by the user.

G. Environment Variables

Environment variables are used by applications and the operating system to store values that they may use internally when performing certain operations. These variables are defined by the applications and the operating system based on their internal needs. Windows operating system uses environment variables to store details such as system path, temporary folder path, etc. Application-specific environment variables are created by applications to store information such as paths (folder locations) in which data is stored and other such parameters as required by the internal logic of the applications. Each environment variable has a name and value. The Registry is used to store these environment variables.

Environment variables can be created by the operating system and applications at system and user levels.

Location of system-level environment variables:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment

Location of user-specific environment variables:

HKEY_USERS\<<USER_SID>>\Environment
These variables may sometimes contain traces of information of applications that were uninstalled.

H. USB Devices

Whenever a USB device is connected to a system, the operating system recognizes the device and stores the serial number of the device, its name (as stored on the device), and the last connected and disconnected date and time stamps [4].
Locations:
1. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB
2. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR
Additionally, Windows stores the mounted drive information, such as the mount point (ID maintained by Windows) and the drive name.
Location:
HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices
From the above locations, an investigator can identify usage of other devices from which additional evidentiary data may be obtained. It is important to note here that the Registry does not store details of the files or operations performed on the USB device.

I. List of File Extensions and Associated Applications

Applications such as MS Word, MS Excel, Adobe Acrobat Reader, etc., support different file formats. Each file format has a distinct file extension, such as docx, xlsx, pdf etc.
HKEY_CLASSES_ROOT contains a list of all the file extensions supported by applications that were installed on the computer. A quick review of this list will provide valuable information to an investigator with the various types of files that were possibly created by the users on a system.

J. List of COM and ActiveX Controls

HKEY_CLASSES_ROOT also contains a list of all the COM and ActiveX controls registered on a system. These controls are binary software components that may have been configured either by the operating system or by installed applications.
In some cases, applications may not have been installed using a system installer. The user may have just copied an executable and ran it. The registry entries listed in Section V-D: Applications Installed on a Computer (above) will not store details of such applications. The list of COM and ActiveX controls may be of use to an investigator in such scenarios to identify such applications.
If an investigator finds a non-standard COM control in the Registry, they can explore the executables on the system and attempt to map the COM control with the executable. Subsequently, the data pertaining to that application stored on the machine on various files and folders can be explored to extract any potential evidence.

VI. Windows Registry Forensics – Evidence from Keys Maintained by Applications:

Applications that are installed on a Windows system may use Windows Registry to store application-specific configurations, a list of recently accessed files, and other such details.

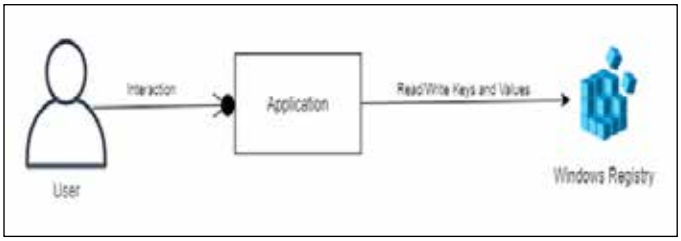


Fig. 8. Windows Registry and Application Interactions

Following are the registry locations for applications to store their configurations and data (such as recently accessed files).
HKEY_USERS\<<USER_SID>>\SOFTWARE
HKEY_LOCAL_MACHINE\SOFTWARE
Here is an example of an application that uses Windows Registry to store its settings:
Adobe Acrobat Reader stores its list of recent files under HKEY_USERS\<<USER_SID>>\SOFTWARE\Adobe\AcrobatReader\DC\AVGeneral\ cRecentFiles
Adobe, the company that has developed Acrobat Reader, generally stores all the keys of its applications under HKEY_USERS\<<USER_SID>>\SOFTWARE\Adobe. Adobe also keeps the keys of Acrobat Reader under HKEY_USERS\<<USER_SID>>\SOFTWARE\Adobe\Acrobat Reader. However, based on the specific version and variant of Acrobat Reader, the path of recently accessed files may change within the following location:
HKEY_USERS\<<USER_SID>>\SOFTWARE\Adobe\Acrobat Reader
Further, the hierarchy of keys maintained by Adobe Acrobat Reader within the Registry contains more than 100 keys. This includes a list of recently accessed files, configured languages, a list of recently accessed folders, and a whole range of application settings including positions and sizes of various application components, etc.
Each application creates its own distinct key hierarchy, which may also change over time based on the preferences of the application developers. This makes the job of the investigator all the more challenging, as they have to apply some guesswork during an investigation. Investigators should expand their knowledge on the usage of the Registry by various popular applications. This requires developing a habit of exploring the Registry and relating the various key paths to the applications installed on a computer.

VII. Methods to Extract Evidence from Windows Registry:

Digital forensics applications can reconstruct the contents of Windows Registry from a forensics disk image. Operating system-level information stored in the Registry can be directly extracted by these applications. Also, since the locations of important registry entries pertaining to the operating system are well-known, an investigator should be able to navigate to the specific locations and extract useful evidence (refer section V).
With regard to application-specific registry entries, search within the Registry is a valuable method to identify keys that contain useful values and data. The following screenshots depict a search operation using the Registry Editor on a live Windows system.

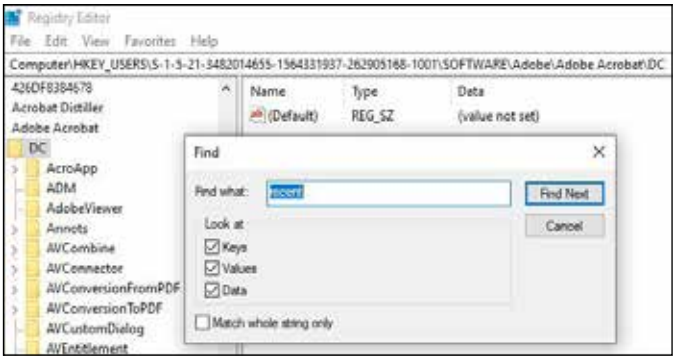


Fig. 9. Windows Registry Find Dialog

The "Find" dialog of Windows Registry can be launched from Edit → Find (Ctrl-F). Entering the search query in the dialog (refer figure 9), leads to the following result:

Fig. 10. Result from Find Operation

Expanding the key cRecentFiles would provide a list of recently accessed files by Adobe Acrobat Reader.

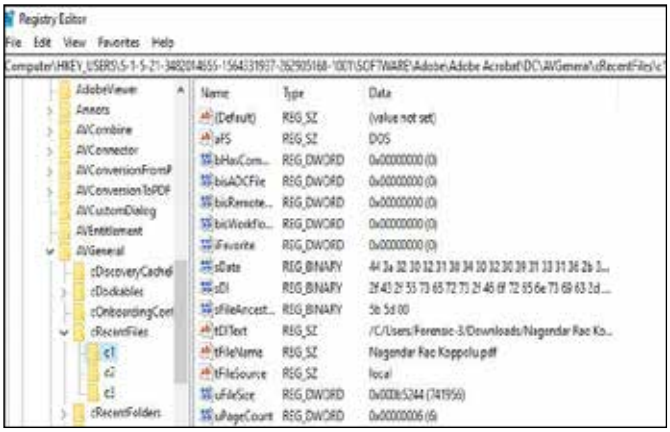


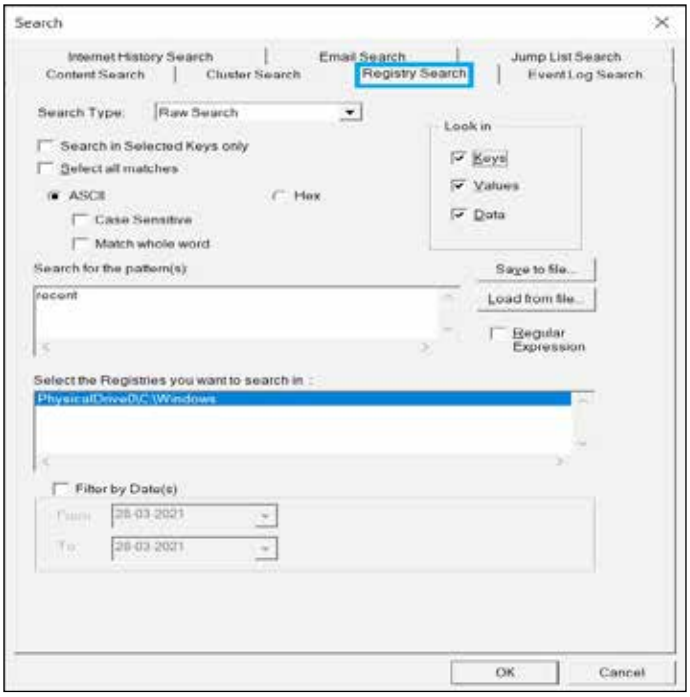
Fig. 11. cRecentFiles Key - List of Recently Accessed Adobe Acrobat Reader Files

Digital forensics applications provide search functions for registry entries within a disk image. A search screen from a digital forensics software product that provides an option to search within Windows Registry is shown below:

Fig. 12. Search in Registry Entries in a Digital Forensics Software

Since digital forensics software applications work on a disk image and retrieve data in a forensically sound manner, the registry entries retrieved using these applications can be used as evidence.

Wherever possible, an investigator should capture the



physical memory of the computer being investigated using digital forensics tools. Using memory forensics, the investigator should be able to recover the registry keys that are available within the memory when the memory was captured [5].

Following is a shortlist of digital forensics applications that support analysing contents of Windows Registry:

- Registry Recon (https://www.arsenalrecon.com/)
- Autopsy (https://www.autopsy.com/)
- Belkasoft Evidence Center (https://belkasoft.com/ec)
- Encase Forensics (https://security.opentext.com/encase-forensic)
- FTK- Forensic Tool Kit (https://accessdata.com/products-services/forensic-toolkit-ftk)
- Magnet AXIOM (https://www.magnetforensics.com/)
- ProDiscover (https://www.prodiscover.com/)
- X-Ways Forensics (http://www.x-ways.net/forensics/)

The above list is by no means exhaustive. Digital forensics investigators should develop skills in several digital forensics products to be effective in their work.

A. Another Approach for Registry Analysis

The Registry is a dynamic database containing configurations and application-specific data, it is not possible to maintain a universal index against which registry entries in an evidence disk image can be compared. Software tools may be developed to compare registry entries in an evidence disk image with registry entries in a baseline Windows image. The baseline Windows image, in this context, is a clean Windows installation, including all the latest Windows updates. Registry entries from the baseline Windows image may be copied to an index file. Registry entries in the evidence disk image can be compared and differentiated with the index file to identify the registry entries created specifically on the evidence disk image.

With such an approach, an investigator will be looking at a potentially smaller subset of registry entries from the evidence disk image, which can be efficiently analysed.

The baseline Windows image can also be updated with

registry entries of widely used applications such as MS Office, Adobe Acrobat Reader, different web browsers, etc. As described in the previous paragraph, the registry entries on this enhanced baseline image can be indexed to a file. Such an enhanced index file can be compared and differentiated with the registry entries from an evidence disk image to yield a much smaller subset of registry entries.

VIII. Challenges for Investigators

Windows Registry forensics requires analysing a huge amount of data stored within the Registry. Information such as installed applications at the operating system level can be easily retrieved, as key paths to such information is generally well known. However, application-specific configurations can be retrieved only after a detailed exploration of the Registry. Since applications create registry keys based on their particular requirements, a clear pattern of Registry key-value-data structure may not be easily discerned. Finding the right set of registry keys that are of investigative value is the main challenge for the investigator in Windows Registry analysis.

Iterative searching within the contents of the Registry can be of help in obtaining application-level registry entries. When performing these searches, to improve the accuracy of results, the investigator should apply their knowledge of the overall structure of Windows Registry and narrow down the scope of search parameters.

It should be noted that many applications may not even use Windows Registry. Such applications may be using their own configuration files. These files are generally available in %AppData%(C:\Users\<UserName>\AppData\Roaming) and %ProgramData% (defaults to C:\ProgramData). All such files should also be located and analysed along with other registry entries for enhanced evidentiary value.

Approaches mentioned in Section VII-A may also be employed to reduce the time and effort required during an investigation.

A. Anti-Forensics

Though Windows Registry is intended to be used by the operating system and installed applications, some users may use the Registry to store some private or secret data [6]. Such cases, though rare, require specialized searches and navigation through the registry entries to identify any hidden data. There may not be a direct solution to resolve such issues. Iterative searches within the Registry can be a possible method.

Some malicious users may even delete or alter some registry keys to hide their tracks. Unfortunately, edits or deletes to Windows Registry are not logged by the Operating System and hence, such actions cannot be traced.

Windows Registry yields information that supports other evidence captured on a disk image. Primary evidence generally comes from files and other data created on the computer.

IX. Conclusion

In an investigation, exploring files and folders on a digital device, including deleted data, enables an investigator to find any available evidence. Windows Registry, being a repository of operating system and application configurations, is a valuable utility for the investigator. These configuration settings may help the investigator understand the various peripherals connected to the device, the applications running on the computer and other such details. Information extracted from the Registry can help the investigator look for additional sources of evidence, such as other hard drives and USB devices that were connected to the computer. Configuration settings and other details stored in the Registry also provide supportive information to the evidence already gathered on the computer.

The various components in Windows, such as the file system, Windows Registry, Windows Event Viewer, System Resource Usage Monitor (SRUM), Prefetch, Windows Timeline, Recycle Bin, etc., store data that was directly or indirectly generated based on the activities performed by the user of the computer. Data that may not be available in the Registry may be visible in other areas, such as Windows Event Viewer, SRUM and Prefetch. Evidence should be collated and analysed from all such key sources to develop a comprehensive understanding of the activities performed by the user on an evidence computer.

References

[1] https://docs.microsoft.com/en-us/windows/win32/sysinfo/predefined-keys

[2] https://docs.microsoft.com/en-us/windows/win32/sysinfo/structure-of-the-registry

[3] https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-value-types

[4] T.Roy and A.Jain, “Windows Registry Forensics: An Imperative Step in Tracking Data Theft via USB Devices”, International Journal of Computer Science and information Technologies “, VoL3, issue 3, 2012, pp: 4427-4433

[5] Shuhui Zhang, Lianhai Wang and Lei Zhang, “Extracting windows registry information from physical memory,” 2011 3rd International Conference on Computer Research and Development, Shanghai, China, 2011, pp. 85-89, doi: 10.1109/ICCRD.2011.5764089.

[6] Y. Kim and D. Hong, “Windows Registry and Hiding Suspects’ Secret in Registry,” 2008 International Conference on Information Security and Assurance (isa 2008), Busan, Korea (South), 2008, pp. 393-398, doi: 10.1109/ISA.2008.8.

[7] Lih WernWong, “ Forensic Analysis of the Windows Registry”.

[8] Nagendar Rao Koppolu, “Role of Microsoft Windows Key Artifacts in Exploring Digital Evidence for Investigation Purposes,” 2021, IJCST Vol.12, Issue 1, Jan-March 2021, ISSN: 0976-8491 (Online)

Author’s Profile

Mr. Nagendar Rao Koppolu joined Police Service as Sub-Inspector of Police in the year 1998. In the police career spanning more than 23 years, Nagedar Rao has had the opportunity to handle a variety of assignments ranging from Law Enforcement, Central Bureau of Investigation (Anti-Corruption Wing), Intelligence, etc. Recently, in 2018, while he was working in Intelligence, he was posted as Inspector of Police, TS Police IT Cell, to render services for Cybercrime Vertical.

While in service, he obtained M.Sc (Information Technology) from Acharya Nagarjuna University, in 2014 and M.Tech (Computer Science) from Osmania University, Hyderabad in 2018. He has accomplished several certificate courses for improving his technological knowledge and skills; and

recently he also acquired a Certificate in Criminal Justice Data Analysis from IIT, Kanpur in 2020. His main study interests are Cyber Crime Investigation, Cyber Forensics, and Cyber Security.

He has been serving as a faculty at the Training Centre (State IT Cell) where police officers from all over the state are trained on Cyber Crime Investigation, Cyber Forensics, and Cyber Security, and related issues. Later, he held charge of monitoring the functioning of all CoE Cyber Crime Labs and guiding the concerned staff in all Districts /Commissionerates of Police.

He is co-author of books published - "Handbook on Cybercrime Investigation", and "Cybercrime Awareness for Cyber Warriors", and he also contributes articles on cybercrimes for publishing in SURAKSHA a monthly Police Magazine to educate all police personnel.