

# Role of Microsoft Windows Key Artifacts in Exploring Digital Evidence for Investigation Purposes

**Nagendar Rao Koppolu**

Inspector of Police, Telangana Police Department, Hyderabad, India

## Abstract

This paper discusses key artifacts generated by Microsoft Windows which may be examined during a forensic investigation. A brief history of Microsoft Windows operating system is presented, followed by a description of the internal structure of hard disks. An analysis of artifacts created due to user’s interaction with applications and the subsequent interfacing of these applications with the operating system and the underlying hardware (primarily the hard disk and volatile memory) are detailed out from an investigator’s perspective.

## Keywords

Artifacts, Filesystem, Forensics, Cybercrime Investigation, Operating System, Windows.

## I. Introduction

The importance of Microsoft Windows cannot be overstated. Contrary to the narratives from certain mobile device vendors asserting that we are in a post-PC era, there are still around 1 billion active Windows 10 devices [1]. Windows market share is claimed to be around 75% of the PC (both desktop and laptop) market and nearly 38% of the server market [2-3]. Windows is the preferred operating system in corporate environments. Understanding the artifacts and digital footprint generated by users of Microsoft Windows is still a critical area of study for Cyber Forensics experts and law enforcement personnel.

Microsoft Windows, due to its deep entrenchment in the corporate world, has a well-documented architecture. Windows has been designed to enable programmers who use its extensive APIs to develop desktop applications for end users and device drivers to connect to a wide range of peripherals. It also provides in-depth information, through Windows Registry, event logs and other such mechanisms, to enable corporate IT support multiple deployment scenarios. Microsoft Windows provides a treasure trove of data for IT administrators and forensics investigators.

## II. Microsoft Windows Architecture

At a high level, Windows operating system comprises of a kernel and a shell [4]. Windows kernel creates and executes application processes and provides access to hardware resources, such as memory, storage, CPU and so on. 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.

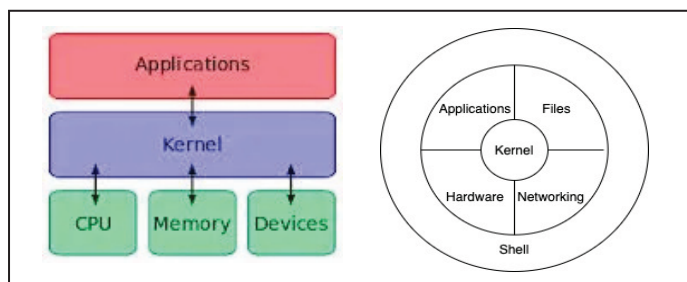


Fig. 1: Windows Architecture

Earlier versions of Windows (until Windows 9x) allowed application processes to access memory locations of any other running process. This caused severe insecurities. From Windows NT onwards, such design flaws were addressed, and strict process boundaries were enforced. However, many vulnerabilities remained due to insecure defaults and certain design choices that were made to enhance configurability and backward compatibility. With continuous enhancements, Windows remains the most widely utilised PC operating system, and hence has been an attractive target for attacks. Individuals, corporate entities and government organisations can be victims of cybercrime.

Microsoft Windows, being a flexible and powerful operating system, also provides wealth of information that can help investigators understand the various actions performed by its users resulting in creation of a variety of artifacts

## III. Disk Layout and File Systems

Storage and memory provide vital information and hence investigators should understand how data is internally organised on hard disks and within system memory.

Within a hard disk, physical tracks (A) can be visualised as concentric circles. Depending on the capacity of the hard disk, there could be a varying number of sectors (B) which segment the physical tracks.

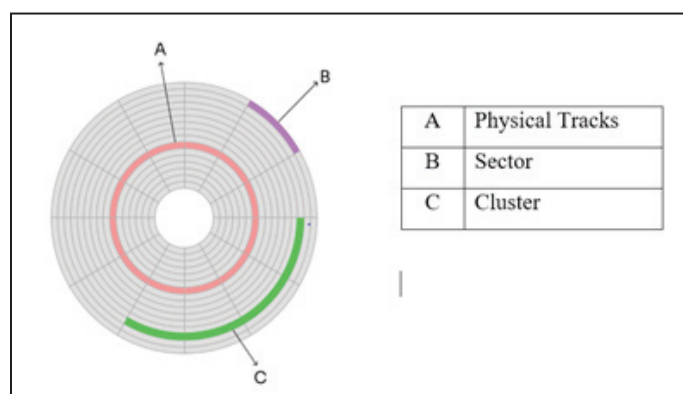


Fig. 2: Hard Disk Layout

The disk may be divided into one or more partitions. A partition comprises of pre-allocated sectors, which are generally contiguous. It is possible that different partitions may have different operating systems.

The file system organises the content on a partition into files and folders, and associates these with related metadata. Modern Windows supports file systems such as FAT32, NTFS and exFAT; older versions of Windows supported FAT and FAT16. The major differences between the older file systems and the recent ones are in the areas of handling larger partitions and files. In addition, NTFS supports journaling, which has improved reliability of the file system.

A cluster (C in fig. 2) is a logical grouping of contiguous sectors. File systems maintain a table of contents which map file contents with cluster addresses. Files that are fragmented will have clusters that are spread across a partition, whereas files that are not fragmented, will have clusters that are contiguous.

Applications running in the user space of Windows depend on its APIs to read and write data. The operating system APIs (such as CreateFile, ReadFile, WriteFile and so on, of Windows Software Development Kit), in turn, rely on the kernel APIs which are exposed by the file system drivers to execute read and write operations on files and folders. Windows Explorer, for example, uses these APIs to process file and folder information. Digital forensics applications, however, do not rely on the file system APIs. Rather, they access the physical disk directly and enumerate the clusters and sectors. With this approach, digital forensics applications obtain data on the disk that is not available through file system APIs.

Sector and cluster data is analysed by digital forensics applications to identify partitions, and operating systems and file systems in those partitions. Digital forensics applications reconstruct files and folders in the partitions, and the data within the files, using multiple algorithms and heuristics.

When a user deletes files and folders from the Recycle Bin, system applications such as Windows Explorer do not show such data. The data may still reside in the corresponding clusters if the operating system has not yet overwritten those clusters. The process of reconstructing files and folders by extracting data at cluster level enables digital forensics applications to identify partitions, files and folders that may be invisible through Windows APIs and Windows Explorer. Digital forensics applications also use cluster level data to recover deleted partitions and files.

**IV. Windows Artifacts and Digital Forensics**

In the context of digital forensics, the term artifact is used to identify any piece of information or data that has forensic value. Digital artifacts may include files and data created by users of the devices. Event logs, registry entries, application settings, environment variables, path settings, system state information and any other data created by applications and the operating system may also be considered as digital artifacts.

During an investigation, when a computer system is examined by digital forensics professionals, the first steps are to collect and preserve the evidence. To ensure that the investigation is conducted in forensically sound manner, a disk image of the evidence hard disk should be created. An image file is a bit-by-bit copy of an evidence hard disk. The bit stream copy includes entire hard disk contents, including slack and unused space. A checksum (hash) of the entire hard disk should be created to demonstrate the integrity of the evidence. During this process, the investigator should avoid any contamination of the evidence. Sometimes, the operating system or an application running on the forensics server may inadvertently write some data on the evidence disk. Therefore, a Write Blocker, a hardware device which prevents any write operations on the evidence disk, must always be used while imaging the data.

Digital forensics applications can read disk images and reconstruct the underlying partitions and file systems. These applications also

provide means to explore details of the applications installed on the system and information stored by the operating system in relation to user and application activity. The state of the operating system can also be evaluated, which may result in finding some important clues.

**V. Artifacts Generated by Actions of Users and Applications**

**A. Files and Folders**

Forensics applications reconstruct files and folders of a partition. These files and folders may have been created by the user of the computer or may have been downloaded from a website or received as an email attachment. These can be examined to collect valuable evidence.

In many cases, multiple users may be using a single computer system. Data from user profiles can be directly accessed using a forensics application. Users may also have stored their data in various other folders across a partition. Cloud storage solutions, such Google Drive and Dropbox may create sync folders which contain files backed up by the users.

Most common locations to find useful files and folders in the Windows Operating System are:

- 1.C:\Users\<<user name>\Desktop
- 2.C:\Users\<<user name>\Documents
- 3.C:\Users\<<user name>\Downloads
- 4.C:\Users\<<user name>\Pictures
- 5.C:\Users\<<user name>\Videos
6. C:\Users\<<user name>\AppData\Local\Temp

Checksum is calculated by forensics applications for each evidence file. This ensures integrity of evidence and therefore forms necessary component of investigative reports presented to a court of law [5].

**B. Extension Mismatch of Files**

Users of a system may sometimes try to obfuscate their actions by renaming the extension of a file. Identifying such files and examining them with their original extensions may help uncover critical evidence.

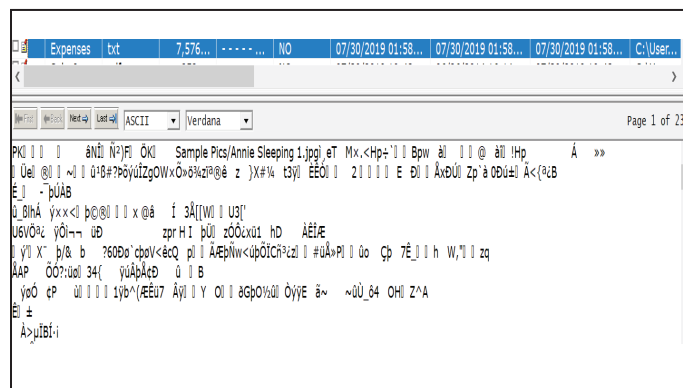


Fig. 3: File with Mismatched Extension

In the fig. 3, above, the file name is visible as Expenses.txt. The file content, when viewed as raw bytes, indicates that it is a compressed file (rather than a text file). The raw content starts with the letters PK, which is one of the signatures of compressed files. The investigator should now treat the file as a compressed file to further investigate its contents

### C. Deleted Files

The Recycle Bin (\$Recycle.Bin) is created in every partition installed with Windows. It contains files and folders that were deleted by a user. The deleted files and folders stay in the Recycle Bin until they are purged by the user.

Within the Recycle Bin, Windows creates a folder on the user's Security Identifier (SID) to store all the files and folders that were deleted by that user. For each deleted file or folder residing in the Recycle Bin, Windows creates two files - one with its name starting with \$R and followed by a random string and the other with its name starting with \$I followed by the same random string. The \$R file stores file or folder contents, whereas the \$I file stores the metadata of the file or folder. Deleted date and time of the file or folder and its original location are also available in the Recycle Bin.

Location: <Drive Letter>:\\$Recycle.Bin

Example: C:\\$Recycle.Bin

### D. Purged Files and Deleted Partitions

The files that are purged from the Recycle Bin, files that are deleted by applications and files that are purged directly by the user from Windows Explorer (shift + delete) may not be immediately cleared by the operating system from the disk. Such files, whose clusters may still contain the data, can be identified and retrieved using forensics applications.

When a partition is quick formatted or when the file allocation table entries are lost, data carving techniques may be applied to recover the lost data. Data carving techniques may also be used to recover deleted partitions by scanning the disk slack (space not allocated to any identified partition).

### E. Web Browser Artifacts

Users of Windows operating system may use several web browsers to access websites. Each web browser stores information pertaining to the visited websites in their internal databases[6]. When these databases are read, details such as the web site URL, the URL parameters, cookies and access date/time can be retrieved.

A cookie may contain data strings (such as session information) that are used by a web application and is stored temporarily on the user's system.

Search engine queries may be retrieved using the URL parameters. Details of social media accounts and relevant cookies may be extracted from the web browser cache using appropriate forensics applications.

Login information of a website (username and password) is stored by a web browser when a user opts to store these details. Website access details are encrypted using Windows Data Protection Application Programming Interface (DPAPI) and pose a challenge for an investigator to retrieve the original credentials. Details of websites visited in private browsing mode further add to the limitations of web browser forensics.

Here is a list of folder locations of different web browsers in which user's web browsing data is stored:

#### 1. Chrome:

%USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\History

(%USERPROFILE% points to the user profile folder. Typically, user profile folder will be in C:\Users\

#### 2. Firefox:

%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\

#### 3. IE 9/10, Edge:

%USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache

Names of cache files have an extension "DAT".

### F. Emails and Web-centric Applications

Emails and email attachments may form key sources of investigation in many cases. Accessing locally stored email content (such as from MS Outlook PST and OST files, Thunderbird MBOX format and so on) can accelerate an investigation.

Location: %USERPROFILE%\AppData\Local\Microsoft\Outlook

### G. Application Settings

Typically, application settings are found in folders such as %AppData%

(C:\Users\

and

%ProgramData% (defaults to C:\ProgramData).

Some applications may also place their configuration files in their installation folders. Application settings may sometimes contain passwords and encryption keys which can be used to access application data.

### H. Databases

Many applications store data within relational databases. More recently NoSQL databases are also being used. Configuration files of databases may sometimes contain database passwords which may be used to access the database system to retrieve information useful for an investigation.

Exploring relational databases requires knowledge of Structured Query Language (SQL). NoSQL databases, on the other hand, use various proprietary formats internally and requires appropriate tools to explore the data.

### VI. Artifacts Generated by Windows Operating System

Following are some of the artifacts generated by Microsoft Windows operating system. These artifacts are generated due to user and application activity, triggering associated actions in the operating system:

#### A. File Properties and Metadata

Files properties and metadata help in understanding how and when files were accessed.

Each file and folder in a partition can have the following properties:

Modified, Accessed and Created (MAC) dates

Shares

In case of certain image formats (JPG/PNG and so on), EXIF data may be part of the file metadata. EXIF contains information such as geolocation, camera model, camera settings and so on [7].

Thumbs.db: When investigating disks that contain image files, it may be useful to explore the Thumbs.db file created by the operating system in the folders containing images. Thumbnails of images may sometimes be retained in Thumbs.db even if original image files were deleted.

Alternative Data Stream (ADS): When a file is downloaded from a website or received as an email attachment, the origin details may be added by Windows to ADS as “Zone Information”. Applications may also use ADS to add additional metadata to files [8].

In NTFS, contents of ADS of a file are also transferred when the file is copied to another folder or partition.

**B. Windows Registry**

Registry is unique to Windows, wherein it stores details of the state of the operating system and installed applications

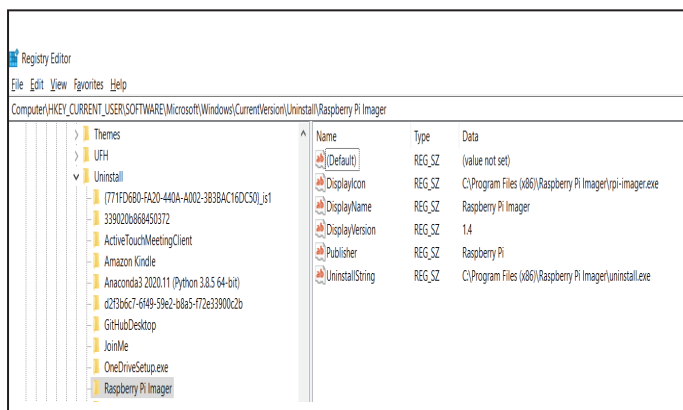


Fig. 4: Windows Registry

Windows Registry can be launched by running RegEdit command from Run dialog or command line. Following information can be retrieved from Windows Registry:

1. Installed applications, Application settings, Association of file extensions with applications, Startup applications, RunOnce applications
2. Installed services, State of services (started, stopped and so on), Windows Install information
3. List of USB drives connected, WiFi networks connected
4. Most recently browsed folders and their settings (Shell Bags)
5. Windows Background Activity Moderator (BAM/DAM) - provides details of applications executed, along with their path.
6. Open/Save MRU - recently opened and saved files from Open/Save dialogs of applications.
7. Drive Letter – the mounted drive name of the partition (C:, D: and so on), Volume Name of partitions

**C. Windows Event Log**

Windows Event Log stores events generated by the operating system and applications. These contain messages that are classified as “Information” and “Error”. Using Windows Event Log, an investigator can recreate a timeline of system events.

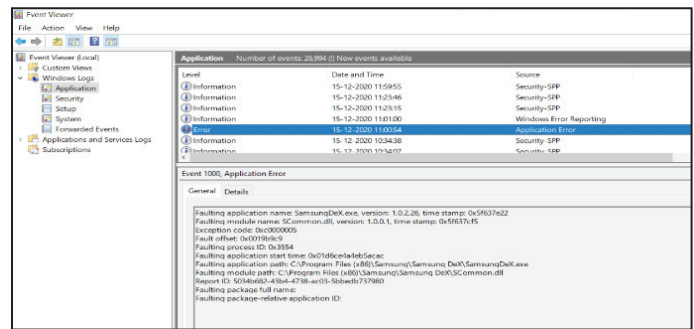


Fig. 5: Event Viewer

Windows Event Log Viewer can be launched by running %WinDir%\system32\eventvwr.msc /s (%WinDir% indicates Windows installation folder at C:\Windows).

Following additional details may also be retrieved from Event Log files:

- WLAN Event Log - historical record of wireless access
- RDP Usage - remote desktop sessions

**D. System Resource Usage Monitor (SRUM)**

SRUM is a file maintained by Windows which collects and stores the following information [9]:

1. Application Resources - application ID, application name, disk I/O, background and foreground activity metrics and so on
2. Network Connectivity – application ID and network interface used
3. Network Usage - bytes sent and received by applications
4. Windows Push Notifications
5. Energy Usage
6. Energy (LT) Usage

Location: %WinDir%\System32\winevt\logs\\*.evtx

**E. System Account Manager (SAM)**

SAM is a file which contains:

1. List of local Windows user accounts
2. Password hashes
3. Last Login date/time
4. Password reset date
5. Failed login date/time

SAM file is located in the folder: %WinDir%\system32\config

**F. System Activity**

**1. Most Recently Used (MRU) files:**

Windows stores shortcuts for files (and applications) accessed by a user so that the user can retrieve these files in an efficient manner. Applications such as Microsoft Office also stores MRU data.

Location: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDIMRU

**2. Jump Lists:**

These maintain a list of recently launched files from Windows Taskbar.

Location: C:\Users\<<profile>\AppData\Roaming\Microsoft\Windows\Recent

### 3. Prefetch:

This folder stores details of applications launched, with information such as:

- List of timestamps when an application was executed
- The number of times an application was executed
- Files used by an application
- Folders accessed by an application[10]

Location: %WinDir%\Prefetch

### 4. System Timeline:

This is an SQLite database containing details of applications and files that were recently launched.

Location: C:\Users\<<UserName>\AppData\Local\ConnectedDevices

### 5. LNK Files:

These are shortcut files to recently launched applications and files.

Location: %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent

### VII. Volatile Memory

When investigating a computer system, if it is not shut down, its volatile memory can also be captured. The resulting memory dump can be explored to obtain valuable information such as unencrypted passwords and any other data that running applications may have stored in memory. List of processes that were running at the point of memory capture can also be enumerated. This list may be used to compare with the list of running applications that are visible in the Task Manager to identify any hidden processes.

The operating system may also cache contents of the volatile memory into pagefile.sys and hibernate.sys files.

Digital forensics applications provide facilities to explore the contents of volatile memory. Investigators may use text search, including regular expressions, to capture snippets of data strings from the contents of a memory dump.

### VIII. Windows Forensics Software

Windows operating system provides various methods to extract key artifacts. The locations of these artifacts are spread across the file system, Windows Registry, Application History, Event Log and so on. There are several forensics applications, both commercial and open source, which can help an investigator to extract evidence from these sources. Following are some popular forensics applications:

1. Autopsy (<https://www.autopsy.com/>)
2. Belkasoft Evidence Center (<https://belkasoft.com/ec>)
3. Encase (<https://security.opentext.com/encase-forensic>)
4. FTK (<https://accessdata.com/products-services/forensic-toolkit-ftk>)
5. Magnet AXIOM (<https://www.magnetforensics.com/>)
6. ProDiscover (<https://www.prodiscover.com/>)
7. Volatility (<https://www.volatilityfoundation.org/>)
8. X-Ways Forensics (<http://www.x-ways.net/forensics/>)

The above list is not an exhaustive one, and a good investigator should explore several such cyber forensics tools and develop a sense of their advantages and limitations.

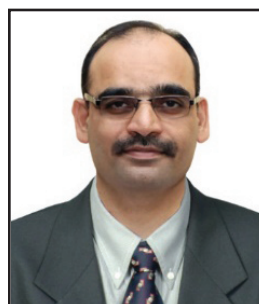
### IX. Conclusion

In Windows, application and user files are spread over several folder hierarchies. Developing a knowledge of these folder structures is critical for an investigator to form a cohesive understanding of user actions and behaviour. The various artifacts generated by Windows Operating System provide a wealth of information on data, applications, timelines and user actions, which in turn, can illuminate the operations performed by the users.

Understanding the internals of Microsoft Windows can help an investigator uncover potential evidence by collating and analysing discrete pieces of information. File and folder structures, deleted files and partitions, web browser artifacts, emails and system logs can provide valuable inputs. File contents should be thoroughly examined using file viewers and full text search queries. Timelines of user actions can be reconstructed during this process.

### References

- [1] [Online] Available: <https://news.microsoft.com/bythenumbers/en/windowsdevices>
- [2] [Online] Available: <https://gs.statcounter.com/os-version-market-share/windows/desktop/worldwide>
- [3] [Online] Available: <https://www.t4.ai/industry/server-operating-system-market-share>
- [4] [Online] Available: [https://docs.microsoft.com/en-us/previous-versions/cc768129\(v=technet.10\)](https://docs.microsoft.com/en-us/previous-versions/cc768129(v=technet.10))
- [5] [Online] Available: <https://blog.pagefreezer.com/importance-hash-values-evidence-collection-digital-forensics>
- [6] [Online] Available: <https://nasbench.medium.com/web-browsers-forensics-7e99940c579a>
- [7] [Online] Available: <https://www.sciencedirect.com/science/article/pii/S174228761930026X>
- [8] [Online] Available: <https://www.sciencedirect.com/topics/computer-science/alternate-data-stream>
- [9] [Online] Available: <https://medium.com/@esmyl/srum-forensics-dfir-aa9522a925c5>
- [10] [Online] Available: <https://cquireacademy.com/blog/hacks/prefetch-parser>



Mr. Nagendar Rao Koppolu joined Police force in the year 1998 as Sub-Inspector of Police. He is currently posted in State IT Cell of Telangana State Police as Inspector of Police, in-charge cyber-crime vertical. He Supervises and Mentors 26 Cyber Forensic Labs across Telangana State. He worked in Central Bureau of Investigation (Anti-corruption wing), Hyderabad from 2008 to

2013 in the capacity of Inspector. He completed Master of Technology (Computer Science Engineering), from Osmania University, Hyderabad, Telangana in 2018. He completed Master of Science (Information Technology) from Acharya Nagarjuna University, Nagarjuna Nagar, Andhra Pradesh in 2014. He has completed Certificate course in Criminal Justice Data Analysis

from IIT, Kanpur in 2020. His research interests are Cybercrime investigation, Internet Investigation, Dark-net Investigation, Cyber Forensics and Cyber Security. He has been teaching Cybercrime Investigation, Cyber Forensics and Social Media Analysis at various Police Training Institutes & Police Headquarters of Telangana State since 2008.

**His Publications include following:**

- Co-authored 'Handbook on Cybercrime Investigation', TSP IT Cell, Telangana State Police, February 2019
- Co-authored 'Cybercrime Awareness for Cyber Warriors, TSP IT Cell, Telangana State Police (2021)
- Writing articles to Police magazine SURAKSHA on Cybercrime related issues