Journal of Criminology and Forensic Studies
ISSN: 2640-6578

Academic Strive
Researcher's perception is our reality

Review Article *Volume 6 Issue 1*

Cybercrimes and Digital Evidence Object's Locations in Window Operating Systems for Forensic Analysis

Singh MK and Meshram BB*

Department of Law, NIMS University, India

***Corresponding author:** Bandu Meshram B, RS NIMS, School of Law, NIMS University, Rajasthan, Jaipur, India, Email: bbmeshram.jes@gmail.com

Received Date: July 05, 2024; **Published Date:** July 19, 2024

Abstract

Currently many computer forensic tools are available for digital forensic work, but the investigators do not know the software architecture of the forensic tools, hence the researcher performed the experimentation to examine the attack paths to analyze the objects to know about the attacker on the basis of which tools are build. This article offers a comprehensive background of the Windows Registry, guiding users through the structure of registry hive files and details the crucial information stored within keys and values, highlighting their significant impact on forensic investigations. The paper explores the cyber-attack on computer window Operating Systems registry, memory, process, file systems and devices and cybercrimes access paths of the window operating systems registry and correlation of the objects in memory, process, files and devices attached for victim's computer machine. By understanding these elements, users can enhance their investigative skills and improve their ability to analyze and interpret registry data and provides foundational knowledge and guidance that helps users develop their own window forensic tools.

Keywords: Cyber-Attacks; Registry; Memory; Process; File Systems; Devices; Artifacts Paths

Introduction

Computer Forensics is a scientific method of data collection, preservation, examination and analysis with maintenance of documented chain of custody to obtain evidence from digital devices or computer networks and their hardware, systems programs applications programs infrastructure components. In Computer forensic, OS Forensics encompasses a range of techniques and tools, including process forensics, memory forensics, file system forensics, and registry forensics. The information they uncover may then be used by the prosecution to create a compelling case against the suspect. Types of potential evidence include evidence from computer systems and any primary memory and secondary memory (like USB pen drives), Documents, Email (Non-web-based), Files stored locally or on a media card, Internet Search History and Social Media accounts.

Both internal and external bad actors compromise the cyber security of the organization's software and hardware assets having high impact of cost drivers for cyber security. The digital forensic tools are used to examine the organizations technological computing systems to know about the attacker and vulnerabilities into the computing systems for the recommendation of cyber security of web applications.

A window operating system (OS) acts as a resource manager by efficiently allocating and managing the computer's hardware and software resources. It handles processor management through scheduling algorithms, ensuring optimal CPU usage by prioritizing tasks and managing interrupts. Memory management involves allocating RAM to processes and managing virtual memory, which ensures efficient use of available memory and maintains system stability and security.

In addition, the OS manages storage through file system operations, organizing, reading, and writing data on storage devices while ensuring data integrity and quick access. It also handles device management by coordinating communication between software and hardware peripherals, managing input and output operations, and ensuring efficient device utilization. Network management is another critical function, with the OS handling network connections, communication protocols, data packet routing, and network security.

The OS provides a graphical user interface (GUI) that allows users to interact easily with the system, managing windowing, multitasking, and user input. It also implements security measures such as user authentication, access control, and encryption to protect system resources.

The OS Forensic experimentation explore Memory Forensic Analysis, File System Forensic Analysis, Process Forensic Analysis, Information Forensic Analysis by observing the effects of attacks on registry keys of window OS The ultimate goal of digital forensic is to provide sufficient evidence to allow the perpetrator to be prosecuted. This research paper answers various question with practical look such

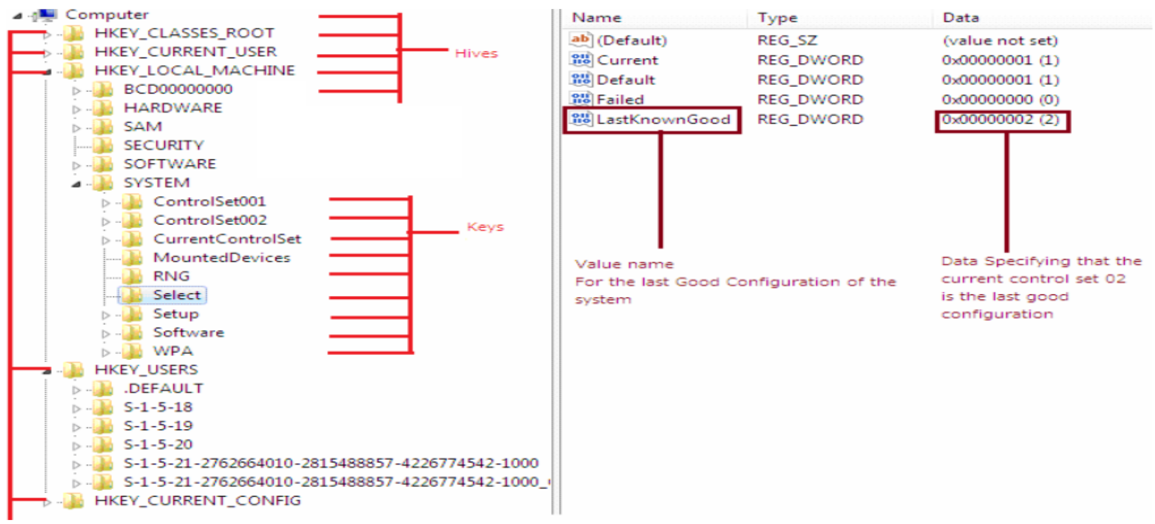
Question 1: What is the significance of window registry Hives to the forensic investigator?
B What are the window attacks on registry, memory process, file systems and devices attached to computer?
Question 3: What are the Artifacts of forensic Investigation?
Question 4: Give the location paths for the keys to obtain the evidence of attacks of computer access?

Victim's Computer Machine Forensic

The forensic proofs are fragile and may be altered, damaged, or destroyed by improper handling or examination. Use strong passwords and multi-factor authentication, Digital Signature and Access Control Mechanism to safeguard the integrity of the proof and render it acceptable during a court of law.

Windows Registry Based Attack and Forensics

The root keys form the basic structure of Window Registry. There are five root keys, HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, and HKEY_CURRENT_CONFIG. By examining the key Path and analyzing the object an investigator can understand the various activities performed by the user or attacker on victims computer. The exact paths and details may vary in different Windows versions. Always check the documentation for your specific operating system version for the most accurate information (Figure 1).



```
Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
    BCD00000000
    HARDWARE
    SAM
    SECURITY
    SOFTWARE
    SYSTEM
      ControlSet001
      ControlSet002
      CurrentControlSet
      MountedDevices
      RNG
      Select
      Setup
      Software
      WPA
  HKEY_USERS
    .DEFAULT
    S-1-5-18
    S-1-5-19
    S-1-5-20
    S-1-5-21-2762664010-2815488857-4226774542-1000
    S-1-5-21-2762664010-2815488857-4226774542-1000_
  HKEY_CURRENT_CONFIG
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Current	REG_DWORD	0x00000001 (1)
Default	REG_DWORD	0x00000001 (1)
Failed	REG_DWORD	0x00000000 (0)
LastKnownGood	REG_DWORD	0x00000002 (2)

Hives
Keys
Value name
For the last Good Configuration of the system
Data Specifying that the current control set 02 is the last good configuration

Figure 1: Structure of window Registry [1,2].

Among these five root keys, only two root keys, HKEY_LOCAL_MACHINE and HKEY_USERS, have physical files or hives. These two keys are called master keys. HKEY_LOCAL_MACHINE contains data related to installed hardware and software, network information and connected servers information. Unlike the above two keys, The other three keys are derived keys since they are derived from the two master keys and their subkeys, or, they only offer symbolic links to the two master keys and their subkeys. HKEY_CLASSES_ROOT (abbr. HKCR), HKEY_CURRENT_USER (abbr. HKCU), and HKEY_CURRENT_CONFIG (abbr. HKCC) are derived keys and they only link to the two master keys and their subkeys. 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_CURRENT_USER is a direct reference to HKEY_USERS\

The configuration details and application settings of different users on the system are available under HKEY_USERS\<>. USER_SID refers to the security identifier which is assigned to each user by the operating system. HKEY_USERS (HKU) stores environment variables and application settings of all the users of the system. The hives of HKLM's subkeys are stored at SYSTEMROOT%System32\config, and the hives of HKU's subkeys are stored at %USERPFOFILE%. The some of the important. 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 [3,4].

Registry Based Attacks

This section lists the common attacks that can be performed on the registry module of the Windows subsystem [5,6].

Registry Malware: Malicious software can modify or inject entries into the registry to achieve various objectives, such as persistence, privilege escalation, or executing malicious code. This can be done through techniques like registry key hijacking, where malware replaces or modifies legitimate registry entries to gain control over specific system functions.
Registry Poisoning: Attackers can manipulate registry values or keys to trick legitimate applications or the operating system into behaving unexpectedly. This can lead to system instability, crashes, or even privilege escalation, depending on the vulnerability being exploited.
Registry Denial-of-Service (DoS): Attackers may flood the registry with a massive number of entries, overwhelming its capacity and causing performance issues or crashing the system. This can disrupt normal system operation and deny legitimate users access to the affected system.
Registry Access Control Attacks: If an attacker gains unauthorized access to modify the registry, they can alter critical settings or permissions, which can lead to the compromise of system security. For example, an attacker may modify registry permissions to grant themselves elevated privileges or to disable security mechanisms. Windows Registry keys with forensic Evidence maintained by windows are illustrated below using manual access.

HKEY_LOCAL_MACHINE

HKLM is the first master key. It contains all of the configuration settings of a computer. When a computer startups, the local machine settings will boot before the individual user settings [7-9].

If we double-click this entry in Windows Registry Editor, five subkeys will be listed: HARDWARE, SAM, SECURITY, SOFTWARE, and SYSTEM (Figure 2).

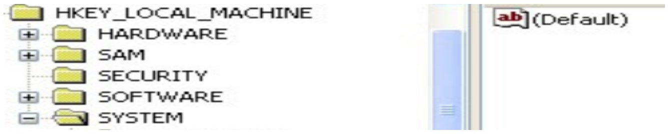


Figure 2: Sub keys of HKEY_LOCAL_MACHINE.

HKEY_LOCAL_MACHINE PATH	FORENSIC IMPORTANCE
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR	The list of various USB devices that have been connected to the system.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	The list of the software installed on the system
HKEY_LOCAL_MACHINE\SOFTWARE\Registered Applications.	The list of the register application with the system
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Services	Installed Services such as databases, application server services or malware etc is background application process that starts when a computer is booted.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 2. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	This key contains list of applications that are launched whenever a user performs a login. It may be of use for an investigator to review and analyse the files created by these applications.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList	The list of the user profiles created on the system.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Profiles	The list of the network accessed by the user and their GUID.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Net workCards	The list of the cards to establish network connection
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName	The active name of the Computer being used by the user
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows	The active name of the Computer being used by the user
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows	This key provides the last shutdown time of the Computer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	The program which are executed automatically when the system is booted
HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names	The list of the users using the system.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI	The last logged on user
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System HKEY_LOCAL_MACHINE\HARDWARE\DEVICEMAP	The list of the hardware devices attached to the system
HKEY_LOCAL_MACHINE\SAM\Domains\Account\Users	The last login time of the user
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces	The information about the DHCP IP address of the system
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\GUID	The system IP address and the default gateway address for the respective network adapter
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\	The list of the Widows services. The malicious program might run as service.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon	The suspects could run malicious program by modifying the value named shell under this subkey
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image FileExecution Options\	The suspect could modify this key to run its malicious program
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor	If the value named Auto run created under this key, malicious program can be executed covertly.
HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices	The information about the mounted devices
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\Memory Management	It maintain Windows virtual memory configuration. The suspects may change the contents of a value name clearPageFileAtShutdown to 1 to clear page file at shutdown

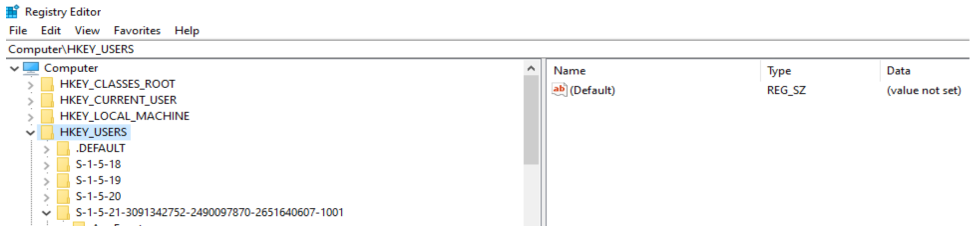
Table 1: Hkey_Local_Machine Path and Forensic Importance.

Table 1 shows Hkey_Local_Machine Path and Forensic Importance [10].

Hkey_Users (HkU)

HKU [10] stores environment variables and application settings of all the users of the system with Security Identifier (SID). It contains all of the per-user settings such as current console user and other users who logged on this computer before.Double-click this entry, we can see at least three kinds of subkeys listed: DEFAUTL, SID, and SID_CLASS. SID is security.

Identifier which refers to the current console. SID-CLASSES contains per user class registration and file association. Usually, we could see S-1-5-18, S-1-5-19, and S-1-5-20, which represents Local System Account, Local Service Account, and Network Service Account respectively (Figure 3).

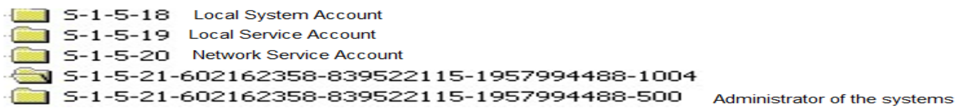


Computer\HKEY_USERS

- Computer
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
  - HKEY_LOCAL_MACHINE
  - HKEY_USERS
    - .DEFAULT
    - S-1-5-18
    - S-1-5-19
    - S-1-5-20
    - S-1-5-21-3091342752-2490097870-2651640607-1001

Name	Type	Data
(Default)	REG_SZ	(value not set)

Figure 3: HKEY_USERS.



S-1-5-18	Local System Account
S-1-5-19	Local Service Account
S-1-5-20	Network Service Account
S-1-5-21-602162358-839522115-1957994488-1004	
S-1-5-21-602162358-839522115-1957994488-500	Administrator of the systems

Figure 4: Administration Of The Systems [8,10].

Usually the long strings stand for different users as below screen.

Each user, group, and computer is assigned a Security Identifier (SID). Access Control List also uses SIDs to distinguish different users and groups (Figure 4). In most real cases, it's impossible to know the usernames or group names in a computer. SIDs are the only identifiers for different users and groups. The longest string is S-1-5-21-602162358- 839522115-1957994488-1004. "S" indicates that the following string is a SID, The first number "1" is the revision number, The third part is the authorized level which ranges from 0 to 5, The fourth part is the local or domain machine identifier. In this example, 602162358-839522115-1957994488 is the local computer identifier. The last part "1004" is a relative identifier which is also a unique number within a local computer or domain. The other SID ended with 500 is the default username "administrator". The mapping between SIDs and users is stored in SAM, a local security database (Table 2).

HKEY_USERS PATH	FORENSIC IMPORTANCE
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell-Folders	The history value provides the path where the information about the documents that have been recently accessed is stored
HKEY_USERS\SID\Software	The details of the software installed on the system
HKEY_USERS\<>\SOFTWARE\ Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	List of Recently Accessed Files files that are sorted and organized by file extension.
HKEY_USERS\<< USER_SID>>\SOFTWARE\ Microsoft \Windows\Current Version\Search\ RecentApps	the activities performed by the user on the computer, especially those related to accessing various applications. List of Recently Launched Applications.

Table 2: Hkey_Users Path And Forensic Importance [5,11].

Hkey_Current_Users

In Windows Registry, most of the user activities are recorded in “ntuser.dat”. Just as the software hive stores all of the configuration settings of local machine, the “ntuser.dat” stores all of the settings for specific users.HKCU\Software subkey contains information about the. Installed software and the major activities that the users performed on the software. The software subkey also includes specific user data such as searches, command, username, password, and so on [11,5].

Hkey_Current_Users Path	Forensic Importance
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	Stores the information in the “run” command drop down list
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F- 11D0-9888-006097DEACF9}\Count,	Investigator check UserAssist key which includes significant information about users’ activities.
HKEY_CURRENT_USERS\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	Recent Document that the user has accessed.
HKEY_CURRENT_USERS\Software\Classses\Local\settings \MuiCache\31\52C64B7E\	When a Malware runs a value is created in the MuiCache
HKEY_CURRENT_USERS\Software\Microsoft\Protected Storage System Provider	The authentication credential for MSN Explorer, Messanger, Outlook Express stored
HKEY_CURRENT_USERS\Software\Microsoft\Internet Explorer\TypedURLs	Websites visited by the suspects
HKEY_CURRENT_USERS\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist	The list of system objects such as program, shortcut, and control panel applet that the user has accessed.
HKEY_CURRENT_USERS\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	The program that have been recently accessed by the user.
HKEY_CURRENT_USERS\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume	The information about the mounted volume and associated drive letter, including USB devices and external DVD/CDROM devices
HKEY_CURRENT_USERS\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU	The recently used program executable program and the file it opened.

Table 3: Hkey_Current_Users Path and Forensic Importance.

Memory Surface Area Attacks and Forensic

The attacks are based on memory, network, website and mobile where the traces of the attacks are stored in the memory of “Windows” system. In this section, we have enumerated the attacks on the Windows operating system. Our attacks are focused specifically on the memory, registry, disk and network aspects of the computer (Table 3).

Memory Attack Surface Area

Attack surface is the aggregate of all known, unknown, and potential vulnerabilities, and controls across all hardware, software, and network components known as the sum of all possible security risk exposures. Tapping into different locations, components, and layers (including hardware/software) of the target system, an attacker can exploit one or more vulnerabilities and mount an attack, for example, extract secret information from a system. Table illustrates major attack [12-14,3] surfaces of a smartphone, composed of software, network, data, and hardware components.

Components	Examples of Attacks
Memory Management Unit	Privilege Escalation Attack
Cache	DNS Spoofing / Poisoning, DNS server locator Man-in-the-Middle Attack, Side Channel Attack
TLB	Buffer Overflow

Memory	Memory Dump, Buffer Overflow ,Phishing Email, Pegasus Malware
DMA Controller	DMA Attack
Disk Controller	Cold Boot Attack
USB Controller	Default Gateway Override, Cold Boot Attack Buffer Overflow Attack & Password Attack
Firewire card PCI	DMA Attack

Table 4: attacks on memory Components.

Mapping Memory Components with their Attacks is shown in Table 4. The following are the attacks made on memory.

Misconfiguration Attack: Misconfiguration arises when Security settings are defined, implemented, and maintained as defaults. Hackers can use Automated software's or scanners like bigfix, acunetics, burp suit enterprise edition and the like for detecting misconfigurations, missing patches, unnecessary services and the vulnerabilities in the OS.

Impact of Misconfiguration of Window OS	Attack scenario by Hacker
Security Weakness	Attack can be done on any level-plat form, web server, application server, database, framework, custom code
Technical Impact	Data can be hacked at any time-Create, update, retrieve and delete operation can be performed by hacker. Recovery cost can be expensive
Business Impact	Computing resources can be compromised without the knowledge of systems owner.
Attackers Approach	Attacker can gain the unauthorised access of default accounts, unprotected directories and files, unpatched flaws and unused pages and the like.
Threat Agents	Authorised Users with their own accounts &Anonymous external attackers may compromise the systems.

Table 5: Impact of misconfiguration attack on windows system.

Example(i)If Directory listing is not disabled on the server and if attacker discovers the same then the attacker can simply list directories. (ii)App servers usually come with sample apps that are not well secured. If not removed from production server would result in compromising your server (Table 5).

Dump LSASS.exe Memory using direct system calls and API unhooking: Local Security Authority Subsystem Service (Lsass.exe) is the process [15] on an Active Directory domain controller which is responsible for providing active directory database lookups, authentication, and replication. It stores data, keys and critical information about the system. Because lsass.exe is a crucial system file, it is often faked by malware. The lsass.exe file used by Windows is located in the directory %\Windir%\System32. If it is running in any other location, the lsass.exe is most likely a virus, spyware, trojan or worm. The memory of lsass.exe is often dumped for offline credential theft attacks. This can be achieved using direct system calls and API unhooking in an effort to avoid detection.

DNS Cache Poisoning: DNS spoofing, referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g. an IP address [16].

Memory Dump Attack: A memory dump attack [17] is the capture and use of RAM content that is written to a storage drive during an unrecoverable error, which is typically triggered by the attacker. Memory dump attacks can be thwarted by a number of means like (i) Programs that use password hashes instead of storing clear text passwords (ii) Tokenization so that only representative data will be in memory and sensitive data is stored elsewhere (iii) NET based applications can use Secure String and Data Protection to limit the time that passwords are available unencrypted (iv) Some Microsoft and other operating systems allow for memory dumps that contain less information and may also make it possible to turn off memory dumps. Memory dump attacks have recently gained attention due to their capability to expose sensitive data from the memory of running applications. One notable instance involved the KeePass password manager, where an attacker could potentially recover a cleartext master password from a memory dump, even if the application was not actively running.

Shrink Wrap Code Attack On Windows System: is the act of exploiting holes in unpatched or poorly-configured software. Some general descriptions of what might be categorized as a "Shrink Wrap vulnerability [18,19]": are (i) A software bug present in the original version of a product, for which the vendor has released an update but the system admin has not patched. Example: CVE-2012-1528 in Windows 8, if the target system does not have the KB2727528 update installed. (ii) In insecure default configuration option still in place after the system has been put into production. Example: Default (esp. when publicly known or easily calculated) account usernames & passwords left unchanged. (iii) Debugging scripts or insecure test pages that are bundled with the software, which should have been removed prior to production use. Example: A "Hello World" script or page left in place, with XSS vulnerability.

Phishing Attack In Windows System: Phishing attacks attempt to steal sensitive information through emails, websites, text messages, or other forms of electronic communication [20].

SQL Injection Attack: SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution of input script.

Pegasus Spyware Attack: Pegasus is the hacking software or spyware that is developed, marketed, and licensed to governments around the world by the Israeli company NSO Group. It has the capability to hack, infect billions of phones running either iOS or Android operating systems [20].

Password Attack: Password attacks [18] in Microsoft's Windows Operating System are commonly performed with the use of the procedure called password cracking. The procedure is carried out by retrieving the passwords that are kept within a data or the password sent by a computer system to another.

Privilege Escalation Attack: Privilege escalation for privacy leakage [18] is a type of network attack used to gain unauthorized access to systems within a security perimeter. Privilege escalations allow attackers to open up new attack vectors on a target system. For example, it can involve [21]: (i) gaining access to other connected systems, (ii) deploying additional malicious payloads on a target system (iii) adjusting security settings or privileges (iv) gaining access to applications or data on a system beyond the privileges of the original compromised account (v) in extreme cases, gaining root access to a target system or an entire network.

Too many logons: Too many logons means that someone has been trying to gain access into the system just by guessing the user passwords. This process is performed with the use of the "dictionary attack".

Man In The Middle Attack: Man in Middle Attack using ARP spoofing [22] allows us to redirect the flow of packets in a computer network. But when a hacker becomes Man-In-The-Middle by ARP Spoofing then all the requests and responses start flowing through the hacker's system.By doing this a hacker spoof's the router by pretending to be the victim, and similarly, he spoofs the victim by pretending to be the router.

DMA Attack: PCI devices are DMA-capable [13], which allows them to read and write to system memory at will, without having to engage the system processor in any operations.

Drive by Attack: A drive-by download attack [13] involves the involuntary download of malicious code, file or software onto a computer or mobile device. Cybercriminals may use drive-by downloads to harvest victims' personal information, spy on you, inject banking Trojans, or infect your entire network with malware.

Social Engineering Attack: Social engineering [23] preys on the fact that humans are the weakest link in information security. Window attacks refer to windows appearing on the victim's screen informing the connection is lost. The user reacts by re-entering the login information, which runs a malicious program already installed with the window appearance.

Backdoor Attack: The simplest backdoor attack is using any malware/virus/technology to gain unauthorized access to the application/system/network while bypassing all the implemented security measures to mitigate backdoor attacks. The memory dump dataset called "Dumpware10" involving 10 malware classes together [24].

Buffer Overflow Attack: A buffer overflow [25] occurs when the volume of data exceeds the storage capacity of the memory buffer

Ransom ware Attacks: Ransom ware [23,24] is a type of malicious software that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker.

Memory Forensic Paths to know the attack forensic

Component	Attack Name	Registry Keys Affected
Memory	Lsass memory dump attack	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Svchost
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LSASS
Memory (Cache)	DNS Cache Attack	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DnsCacheConfig
		HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DnsCacheMaximumAge
		HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DnsCacheMaxNegativeCacheTtl
		HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DnsCacheMaxNegativeSOACacheTtl
		HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DnsCacheMaxSOACacheTtl
Memory (Windows Credential Locker)	Windows Credential Dumping Attack	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount
		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsList
		HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData
		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\LastLoggedOnUser

Table 6: The Effects of Attacks on Registry Keys of window OS:

Table 6 to examine the object location of the attacks and you can analyse the content of the object for forensic [2].

Window Process Based Attacks and Forensic

The content available in the volatile memory remains as long as the power is on. Once the power is turned off, the contents in the volatile memory is lost. However, if the periodic dump of the volatile memory is taken, then it can be of immense help to the forensic investigator in identifying the malicious insider and the malicious code injection or unknown. exe file. The running processes in Windows volatile memory access the registry keys and its values for their execution. The registry keys and its values are useful in reconstructing the activities performed by the user on the computer systems. The suspicious activities can be identified from the reconstructed user activities to identify the malicious insider performing such suspicious activities [21,26].

OS Process Based Attack Vectors

This section presents the attacks on the Process of the window operating systems.

Process Memory Hollowing: Adversaries may inject malicious code into suspended and hollowed processes

[27] in order to evade process-based defences. Process hollowing [27] is a method of executing arbitrary code in the address space of a separate live process. Process hollowing is commonly performed by creating a process in a suspended state then unmapping/hollowing its memory, which can then be replaced with malicious code. A victim process can be created with native Windows API calls such as Create Process, which includes a flag to suspend the processes primary thread. At this point the process can be unmapped using APIs calls such as Zw Unmap View of Section or Nt Unmap View of Section before being written to, realigned to the injected code, and resumed via Virtual Alloc Ex, Write Process Memory, Set Thread Context, and then Resume Thread respectively.

Process Injection: Asynchronous Procedure Call: Adversaries may inject malicious code into processes via the asynchronous procedure call (APC) queue [28] in order to evade process-based defenses as well as possibly elevate privileges. APC injection is a method of executing arbitrary code in the address space of a separate live process. APC injection is commonly performed by attaching malicious code to the APC Queue of a process's thread. Queued APC functions are executed when the thread enters an alterable state. A handle to an existing victim process is first created with native Windows API calls such as Open Thread. At this point Queue User APC can be used to invoke a function (such as Load Library A pointing to a malicious DLL).

Process Forensic

Attack on Process and Registry Path Affected		
Component	**Attack**	**Registry Path Affected**
Process	Process Memory Hollowing	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\SystemRoot
		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
Process	Process Injection	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
		HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
		HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
		KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnceEx

Process (Service)	Windows Privilege Escalation using Service Exploit	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
		KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Appcompatcache
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters

Table 7: Attack on Process and Registry Path Affected [29].

The Table 7 shows attack on process and registry path affected by the attacks [30-33].

File Systems Attacks and Forensic Paths

This section identify the file systems attacks [34,25] and its forensic with respect to registry path affected by the access of disk file system.

Disk Based Attack

Master File Table (MFT): The MFT is a complex data structure stored on the NTFS volume itself. It is managed by the NTFS file system driver and is not directly accessible through the Windows Registry.

Registry for File Associations: The HKEY_CLASSES_ROOT key in the Registry contains information about file types and their associations with specific applications. Changes in file associations can impact how files are opened or executed. The file system metadata, including information about files, directories, and their attributes, in Windows operating systems, is primarily stored in the Master File Table (MFT) for NTFS (New Technology File System).

This section lists the common attacks that can be performed on the disk module which is known as file systems of the Windows subsystem.

Hide Artifacts: NTFS File Attributes: Adversaries may use NTFS file attributes to hide their malicious data in order to evade detection. Every New Technology File System (NTFS) formatted partition contains a Master File Table (MFT) that maintains a record for every file/directory on the partition. Within MFT entries are file attributes, such as Extended Attributes (EA) and Data [known as Alternate Data Streams (ADSs) when more than one Data attribute is present], that can be used to store arbitrary data (and even complete files). Adversaries may store malicious data or binaries in file attribute metadata instead of directly in files. This may be done to evade some defenses, such as static indicator scanning tools and anti-virus.

Masquerading: Rename System Utilities: Adversaries may rename legitimate system utilities [32] to try to evade security mechanisms concerning the usage of those utilities. Security monitoring and control mechanisms may be in place for system utilities adversaries are capable of abusing. It may be possible to bypass those security mechanisms by renaming the utility prior to utilization (ex: rename rundll32.exe). An alternative case occurs when a legitimate utility is copied or moved to a different directory and renamed to avoid detections based on system utilities executing from non-standard paths.

File Access Attack: The information about creating, updating, retrieving, and deleting files in Windows operating systems is spread across various locations

File Attacks Forensic

File attack forensic analyze the NTFS, FAT file system and describe detailed analysis of existing files, detailed analysis of deleted files, and tracing a deleted file back to its original position and analysis of hidden data under any file. This section discusses the registry path affected by the user by using file Systems as shown in Table 8.

File System	Hide Artifacts : NTFS File Attributes	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsHideDotFileAttributes
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsHideFileAttributes
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsHideReadOnlyFileAttributes
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsHideSystemFileAttributes
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsHideHiddenFileAttributes
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsHideCompressedFileAttributes
File system	Local File Inclusion	HKEY_LOCAL_MACHINE\SOFTWARE\
		HKEY_LOCAL_MACHINE\SYSTEM\
		HKEY_CURRENT_USER\SOFTWARE\
		HKEY_CURRENT_USER\SYSTEM\
		HKEY_USERS\
File system	Application execution, CURD operations on File & file associations	HKEY_CLASSES_ROOT
		HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU.

Table 8: Attack on File Systems and Registry Path Affected.

Table 8 shows various Attack On File Systems And Registry Path Affected [2,34-36]. The metadata about files, including their creation, modification, and access timestamps, is stored within the file system. For NTFS (New Technology File System) [37]: Information is stored in the Master File Table (MFT).For FAT32 (File Allocation Table): File allocation tables contain metadata. The Windows Registry, however, does not directly store this file system metadata. Hence we have to identify different locations for file systems CURD operations as below:

Windows Event Logs: Windows logs events related to file system activities in the “Security” and “System” logs. Look for events with Event IDs such as 4663 (file or folder access), 4660 (file or folder deletion), and others.

You can check Open Event Viewer (eventvwr.msc) to observe events related to file system activities.

Prefetch Folder: The Prefetch folder contains information about files accessed during the boot process and application launches in Location: C:\Windows\Prefetch

Recycle Bin: Deleted files are moved to the Recycle Bin. Each user has their own Recycle Bin, and information about deleted files is stored here until the bin is emptied. The **Location is :** C:\$Recycle.Bin

MRU, or ‘most recently used’ lists contain entries made due to specific actions performed by the user. The chronological order of applications executed via ‘Run’ can be determined by looking at the Data column of the ‘MRUList’ value.

System Volume Information: This folder is used by Windows for systems restore points. It may contain information related to changes in the file system. The location is C:\System Volume Information

Windows Search Index: The index contains information about the files on the system, including their contents and metadata. The search index is usually stored in the C:\

ProgramData\Microsoft\Search\Data directory.

Security Logs: Events related to file system activities [38] are often found in the Security log in Event Viewer.

Audit Policies: Windows allows you to configure audit policies to log specific events, including file and folder access. Use the Group Policy Editor (gpedit.msc) to configure audit policies.

Timestamp Analysis: Timestamps [39] on files and directories (created, modified, and accessed) are crucial for establishing a timeline of file system events.

File Access Logs: Monitor file access logs or file metadata [40] to see if specific files were accessed or modified around the time of the suspected access.

Hash Values: Calculate hash values of files before and after the suspected access period. Any changes can indicate potential tampering or access.

For forensic purposes related to file system metadata, investigators typically analyze the file system directly, focusing on the MFT for NTFS volumes. The metadata analysis of compromised systems by analyzing following categories [41]: File System Category, Content Category, Metadata Category, File Name Category and Application Category. Many proprietary and free software tools available for file system forensics analysis like Sleuth kit, Autopsy, AccessData, FTK Imager etc.

Devices and its Access of Systems Forensic

The section presents the device attachment and its evidence to know about the devices attached to the systems.

Devices Communication with Computer Systems

Windows-based computer systems support a wide range of devices through various ports and interfaces. The various common types of devices that can be connected to Windows computers are as below:

(i)USB Devices: (ii) External Storage Devices (iii) Networking Devices: (iv) Input Devices:,

(v) Display Devices: (v) Audio Devices (vi) Printers and Scanners (vii) Card Readers (viii) Cameras: (ix) Mobile Devices: (x) External Peripherals (xi) Storage Devices: (xii) Input/output Devices (xiii) Power Devices (xiv) Security Devices: (xv) Gaming Devices (xvi) Miscellaneous Devices.

Device Forensic

On Windows-based computers, information about USB device connections and disconnections can be found in the Windows Registry and Event Logs. Detecting whether a printer, USB device, or mobile device has accessed data from a computer for digital forensic purposes involves examining various artifacts and logs [37,42,43].

Here are some methods for investigating these scenarios:

(i) Printer Access can be checked using printer logs and spooler files.

Printer Logs: Printer Logs check the logs of the printer, if available, to see if any print jobs were sent from the computer. Print logs can provide details about the files printed, time, and user.

Spooler Files: Examine the print spooler files on the computer. The spooler stores print jobs temporarily before sending them to the printer. Investigating these files might reveal information about the printed documents.

USB Device Access can be checked using USB Device Logs, System Event Logs and Forensic Tools

USB Device Logs: Windows keeps logs of connected USB devices in the registry. You can examine the Windows Registry to identify USB devices that have been connected to the computer. Tools like USBDe view can assist in extracting this information.

System Event Logs: Check the Windows Event Logs for entries related to USB devices. Events may include information about when a USB device was connected or disconnected.

Mobile Device Communication: The Mobile Device Communication is stored in Wi-Fi Logs, Router Logs, Device Logs

Wi-Fi Logs: Examine Wi-Fi logs on the computer to see if any mobile devices have connected to the computer's Wi-Fi network. Event logs or wireless network management tools can provide this information.

Router Logs: Check router logs to see if the mobile device has connected to the network. Routers often maintain logs that include information about connected devices.

Device Logs: On the mobile device itself, look for logs that may indicate a connection to the computer. For example, on Android devices, you can check system logs using tools like ADB (Android Debug Bridge).

Domain expert can also opt for timestamp analysis by Correlating timestamps across various logs to establish a timeline of events. This can help in determining if the printer, USB device, or mobile device access coincided with specific activities on the computer (Table 9).

Device	Cold Boot Attack	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivedef
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivebak
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivef
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivex
		HKEY_LOCAL_MACHINE\SECURITY
		HKEY_LOCAL_MACHINE\SAM
		HKEY_LOCAL_MACHINE\SYSTEM
		HKEY_USERS\DEFAULT
		HKEY_USERS\.DEFAULT
Network Adopters attached	installed network adapters, including both Ethernet and Wi-Fi adapters	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}
USB Devices and their drivers	Software installed for Devices or any. exe file	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB.
USB Device Logs	Illegal USB Attached	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR
connected USB devices, including non-storage devices like keyboards, mice, etc.		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB
information about installed printers, including their configuration		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers

Table 9: Attack on Device and Registry Path Affected

User's Interactions Forensics: 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 .The evidence of user interaction is provided from Keys Maintained by Windows as shown in Table 10.

Evidence About	Location
List of Recently Launched Applications	HKEY_USERS\<<USER_SID>>\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\RecentApps
	HKEYUSERS\<<USER_SID>>\SOFTWARE_Wow6432Node\Microsoft\Windows\CurrentVersion\ Search\RecentApps
List of Recently Accessed Files	HKEY_USERS\<>\SOFTWARE\ Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
	HKEY_USERS\<>\SOFTWARE\ Microsoft\Windows\CurrentVersion\Explorer\RecentDocs -When user run applications using save and open operaations, key is updated as below:
	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32-List of applications and files launch in run commond
	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

Windows Installation Related Information.	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
	Windows NT\CurrentVersion
Applications Installed on a Computer	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
Installed Services	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Services
Start-up Applications	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ RunOnce

Table 10: User's interactions with applications and the operating system

Table 10 shows the attack or activity paths about User's interactions with applications and the operating system [44].

Windows Diagnostic Experimentation

Event Log: During experimentation, the researcher observe the following diagnostic experimentation: The windows Event Viewer [43,28,45] will show customs views, windows logs and application and services logs. Events logged by Windows and many different Windows apps are viewable with Event Viewer and EaseUS LockMyFile. Event viewer can be used using customs views, windows logs and application and services logs. One can use event Logging Functions for forensic preparedness [46].

Firstly Windows Event Viewer application can be accessed by choosing Control Panel ➤ System and Security ➤ Administrative Tools ➤ Event Viewer.

The various directories locations for forensic artefacts are given below:

USB Device Connected: Second Event Viewer procedure for path finding is

Open Event Viewer (Win + X and select "Event Viewer"), then Navigate to "Windows Logs" > "System."

In the right-hand pane, click on "Filter Current Log." And In the "Event sources" dropdown, select "Kernel-General." Look for events with the event ID 219. These events indicate that a USB device was connected.

Specific USBHub Event Logs can be viewed using procedure: Open Event Viewer, then Navigate to "Applications and Services Logs" > "Microsoft" > "Windows." and Look for the "USB-USBHUB" log and Check for events related to USB device connections.

The event logs are located in Windows or WINNT directory under %WinDir%\system32\config. Windows Vista allows administrators to continue using Pfirewall.log, although it is now stored in %windir%\system32\LogFiles\Firewall\ Pfirewall.log.

The Windows Firewall in Windows XP SP2 and Windows Server 2003 SP1 keeps firewall log information in two locations: %windir%\Pfirewall. Log and Security event log.

You can also view the Windows logs using EaseUS LockMyFile. By Launching EaseUS LockMyFile, enter your valid email, and set password to register and then click "Folder Monitor" on the left panel and. then, choose "Add" on the right pane to select the folder or drive that you want to view logs. And then click ok and refresh to view the logs.

The forensic locations of drivers for various devices attached to a computer are typically stored in specific directories on the Windows operating system. Here are common locations where drivers can be found:

USB Devices are located at:\Windows\System32\drivers

GPS Devices: GPS device drivers are usually stored in the system's driver repository, which is typically located in C:\ Windows\System32\DriverStore\FileRepository.

Barcode Scanners: Barcode scanner drivers may also be stored in the system's driver repository (C:\Windows\ System32\DriverStore\FileRepository), or they could be included with the software provided by the barcode scanner manufacturer.

Headphones, Speakers, Microphones: Audio drivers for headphones, speakers, and microphones are usually stored in the system's driver repository (C:\Windows\System32\ DriverStore\FileRepository). The specific driver files can also be found in C:\Windows\System32\drivers.

Driver Store: The DriverStore folder (C:\Windows\ System32\DriverStore) is a critical location for storing driver packages on Windows systems. However, navigating this folder directly may not provide easy visibility into specific devices.

Printer Logs: The location of printer logs on a Windows-based computer can vary depending on the version of the operating system. Here are some common locations to find printer-related logs [47]:

Print Spooler Logs: The print spooler logs are often stored in the Windows\System32\spool\PRINTERS directory. You can find both the spooler files and logs here.

Printer-related events are recorded in the Windows Event Viewer. Follow these steps to access printer-related logs:

Open Event Viewer: Press Win + X and select "Event Viewer, then Navigate to "Windows Logs" > "System."

Filter Events: In the right-hand pane, click on "Filter Current Log.", then In the "Event sources" dropdown, select "PrintService." And Click "OK" to apply the filter.

View Printer Events: Look for events with the source

"PrintService." You can find information about print jobs, printer connections, and errors.

Spooler Subfolder: Another location related to the print spooler is:C:\Windows\System32\spool\PRINTERS .In this directory, you may find files related to print jobs and logs.

Device Manager provides a graphical interface for viewing and managing hardware devices. Navigate to the "Network adapters" section to see a list of installed network adapters. Right-clicking on an adapter and selecting "Properties" provides details about the device, including driver information. For Location of device manager: Open Device Manager (devmgmt.msc).

For Network Adapters the Network configuration files are stored in various locations, and the specifics depend on the Windows version.

For Ethernet: Look for files related to network configurations in the C:\Windows\System32\config directory.

For Wi-Fi: Configuration files are often found in the C:\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces directory.

Ethernet Logs: Check logs related to the specific network adapter, such as Intel PROSet logs.

For Networking Events: Open Event Viewer (eventvwr.msc).

And Navigate to "Windows Logs" > "System" for a variety of system events, including those related to networking and. Look for events from the source "Microsoft-Windows-NetworkProfile" for Wi-Fi events and "e1iexpress" for Intel Ethernet adapter events, for example.

Various logs and diagnostic tools can provide additional information about networking events.

Wi-Fi Logs [48]: C:\Windows\System32\winevt\Logs\Microsoft-Windows-WLAN-AutoConfig/Operational.evtx

Router: Routers often store logs [11] related to network activity, including device connections and disconnections. Log locations and access methods depend on the router make and model. The details are provided in section Examination and Analysis of Router Logs.

Command Level Access of Window Services Forensic Artifacts'

Window Forensic Artifacts'	Command Level Access
Window Registry	To access the Windows Registry, press the Windows key + R, type regedit.exe in open dialogue box, and press Enter
Backup of Window Registry	To back up the existing, current state of the Windows Registry, open the Registry and choose File ➤ Export. Then save the file in a safe location.
Restore of Window Registry	To restore a previously saved state of the Windows Registry, open the Registry and choose File ➤ Import. Then select the backup file that you want to restore.
Window Logs	Windows Event Viewer application can be accessed by choosing Control Panel ➤ System and Security ➤ Administrative Tools ➤ Event Viewer. Then press event viewer, you will get – ➤customs views, window logs and application and services logs, subscriptions
Windows Services like virus scan	To manage Windows Services, press the Windows key + R, type services.msc in open dialogue box, and press Enter.
Windows Security Policies	To get started, press the Windows key + R, type gpedit.msc in open dialogue box, and press Enter.
Windows Firewall	To open Windows Firewall, press the Windows Key + R, type wf.msc, and press Enter.
Microsoft windows Malicious software Removal Tool(mrt)	To open Microsoft windows Malicious software Removal Tool, press the Windows Key + R, type mrt
Device Manager	You can use the Windows Device Manager, press the Windows Key + R, type devmgmt.msc in open dialogue box, to view installed drivers.

Table 11: Window Services Forensic Artifacts.

The Command Level Access of various services [38,43] provided by window are shown in Table 11.

There are hundreds of Useful Commands to Be Run from the Windows Command Prompt that are used in day-to-day Windows administration commands that are useful from a security perspective like tasklist, driverquery, ping, tracert, nslookup, ipconfig /all, netstat and the like. Table 11 explore the command level access of window services forensic artifacts' [17, 19,4].

Tools for Analyzing Contents Of Windows Registry

Digital forensics applications (TOOLS) 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 Digital forensics 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 from HIVES [49]. The Registry Explorer Tool is used for registry forensics. Using memory forensics, the investigator should be able to recover the registry keys that are available within the memory when the memory was captured.Digital forensics Tools provide search functions for registry entries within a disk image [50].

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

1. Registry Recon (https://www.arsenalrecon.com/)
2. Autopsy (https://www.autopsy.com/)
3. Belkasoft Evidence Center (https://belkasoft.com/ ec)

Encase Forensics (https://security.opentext.com/encase-forensic)
FTK-ForensicToolKit https://accessdata.com/products-services/forensic-toolkit-ftk)
ProDiscover:ttps://www.prodiscover.com/)(vii)
X-WaysForensics (http://www.xways.net/forensics/)
Windows Event Log Analyser Tool

Conclusion

The Operating System creates artifacts, objects that enhance efficiency and user experience while recording crucial user activity data. These artifacts are vital for forensic investigations as they provide essential leads for forensic triage [51]. Windows artifact locations can vary significantly between different versions of the operating system. Investigators often need to determine these paths through a process of trial and error to ensure accuracy [52]. This means manually checking and verifying the location of artifacts in the specific Windows version they are analyzing. By doing so, they can correctly identify and analyze the necessary data, which is crucial for accurate forensic investigations. This meticulous approach helps investigators adapt to the changes and variations in artifact locations across different Windows versions, ultimately improving the reliability of their findings [32].

By exploring into the architecture of hives content and examining the attack paths, researchers can better analyze artifacts such as registry hives, memory, processes, file systems, and connected devices. The detailed exploration of the Windows Registry, with its critical information stored in keys and values, highlights the significant role these elements play in forensic investigations [35]. By gaining a thorough understanding of these components, investigators can enhance their skills, improve their ability to interpret registry data, and develop effective forensic tools tailored to Windows operating systems. This foundational knowledge is crucial for accurately identifying and addressing cyber-attacks, thereby strengthening the overall process of digital forensics [33].

Future Directions: This experimentation research discover identification of various logs from, victims machine call for explanations based on collected facts, measurements, observations and not on reasoning alone and explore the forensic analysis based on verified experimentations. This strategy shall act as a foundation used to analyses, design of data structure, algorithms, GUI, implementation of AI based automated forensic tool used for critical infrastructure computing systems forensic [53,54].

References

4. Carvey H (2007) Windows Forensic Analysis. MA: Syngress.

5. Carvey H (2016) Windows Registry Forensics, Advanced Digital Forensic Analysis of the Windows Registry. 2nd (Edn.), Elsevier, USA.

6. Zhu N, Chen XY, Zhang Y (2011) Construction of Overflow Attacks Based on Attack Element and Attack,Template. 2011 Seventh International Conference on Computational Intelligence and Security, China, 540-544.

7. Microsoft doc (2022) Windows 11 release information.

8. Splunk Threat Research Team (2023) From Registry with Love: Malware Registry Abuses.

9. (2021) How to Open and Edit the Windows Registry.

10. Patil DN, Meshram BB (2015) Forensic Investigation of User Activities on Windows7 & Ubuntu12 Operating System. International Journal of Innovations in Engineering and Technology (IJIET) 5(3).

11. Koppolu NR (2021) Importance of Registry Forensics in Digital Crime Investigations Involving Windows Machines. InternatIonal Journal of Computer SCience and Technology (IJCST) 12(2): 9-18.

12. Hasan SMR, Dhakal A (2024) Obfuscated Malware Detection: Investigating Real-world Scenarios through Memory Analysis. Cryptography and Security.

13. Budhrani A, Singh U, Singh B (2022) Forensic Analysis

of Windows 11 Prefetch Artifact. 2022 IEEE Bombay Section Signature Conference (IBSSC), India, pp: 1-6.

14. Weafer V (2015) Detecting the Undetectable Widows Registry Attacks. Cyberattacks & Data Breaches.

15. Rathnayaka C, Jamdagi A (2017) Efficient Approach for Advanced Malware Analysis using Memory Forensic Technique. 2017 IEEE, Australia, pp: 1145-1150.

16. Ankush B (2023) What are Direct Memory Access (DMA) Drive-By Attacks?.

17. Cohen M Digital Investigation: Scanning memory.

18. Williams, Trustwave, SpiderLabs, Millington E, (2020) OS Credential Dumping: LSASS Memory.

19. Wikipedia (2023) Detailed Information on DNS Spoofing.

20. Al-Qudah M, Ashi Z, Alnabhan M, Al-Haija QA (2023) Effective One-Class Classifier Model for Memory Dump Malware Detection. Edge Computing for the Internet of Things (IoT) 12(1): 5.

21. John TM, Haider SK, Omar H (2017) Transactions on Dependable and Secure Computing Connecting the Dots: Privacy Leakage via Write-Access Patterns to the Main Memory pg. 79 IEEE 2017.

22. Esq MRO (2011) Legal Quicksand: Shrink-Wrap and Click-Wrap Agreements. CSO.

23. Cohen M (2017) Scanning memory with Yara. Digital Investigation 20: 34-43.

24. (2020) Process Injection: Process Hollowing.

25. (2021) Man in the Middle Attack Using ARP Spoofing. Geeks for Geeks.

26. Meshram BB (2022) Cyber Attack On AIIMS, Delhi Interview.

27. Bozkir A, Tahillioglu E, Aydos M, Kara I (2021) Catch Them Alive: A Malware Detection Approach Through Memory Forensics, Manifold Learning and Computer Vision. Computers & Security 103: 102116.

28. Patil DN, Meshram BB (2017) Extraction of Forensic Evidences from Windows Volatile Memory. 2nd International Conference for Convergence in Technology (I2CT), India, pp: 421-425.

29. Hosseini A (2017) Ten Process Injection Techniques: A Technical Survey of Common and Trending Process Injection Techniques. Elastic.

30. Pingios A, Beek C, Becwar R (2017) Process Injection : Process Hollowing.

31. White S, Sharkey K, Batchelor D, Coulter D, Satran M (2021) Asynchronous Procedure Calls. Synchronization.

32. Li Z, Liang Z, Wang M, Zou X (2019) A Study on Windows OS Process Object Paths and Attack Path Analysis. Journal of Information Security and Applications 44: 13-24.

33. Carrier AB (2005) File System Forensic Analysis. Addison Wesley Professional.

34. Cui Q, Liu J (2020) Evasion Techniques: Masquerading and Renaming System Utilities to Bypass Security Measures. Journal of Cybersecurity Research 15(3): 245-257.

35. Eo S, Jo W, Lee S, Shon T (2015) A Phase of Deleted File Recovery for Digital Forensics Research in Tizen. 2015 5th International Conference on IT Convergence and Security, Malaysia, pp: 1-3.

36. Arffin KAZ, Mahmood AK, Jaafar J, Shamasuddin S (2015) Tracking File's Metadata from Computer Memory Analysis. 2015 IEEE International Conference on Computer and Information Technology, UK, pp: 975-980.

37. Ligh MH, Case A, Levy J, Walters A (2014) The Art of Memory Forensics: Detecting Malware and Threats in Windows, A. Linux, And Mac Memory. Goodreads, pp: 912.

38. (2019) Computer Forensics: Media & File System Forensics. Digital Forensics.

39. HoneyCutt J (2005) Microsoft Windows Registry Guide. 2nd (Edn.), Microsoft Press.

40. (2020) Windows Registry Forensic.

41. Casey E (2011) Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, USA.

42. Lin X (2018) Introductory Computer Forensics: A Hands-on Practical Approach. 1st (Edn.), Springer Nature, Switzerland, pp: 577.

43. Chow KP, Law F, Kwan M, Lai P (2007) The Rules of Time on NTFS File System. Second International Workshop on Systematic Approaches to Digital Forensic Engineering, USA, 71-85.

44. Harlan C (2004) Windows Incident Response.

45. Shaaban A, Sapronov K (2016) Practical Windows Forensics, Leverage the Power of Digital Forensics for

Windows System. 1st (Edn.), PACKT Publishing, pp: 322.

46. Turner P (2005) Uncovering Forensic Artifacts of Digital Printers. Journal of Digital Forensics, Security and Law 1(2): 27-36.

47. Liao TC, Huang YP (2018) Wi-Fi Forensics: Analysis of Wi-Fi Logs and Reconstruction of Device Activities. Digital Investigation 26: S72-S79.

48. Encyclopaedia Windows Security Log Events.

49. Liu J, Cheng Y (2020) Router Log Analysis for Network Security Forensics. Journal of Network and Computer Applications 165: 102705.

50. Harlan C, Altheide C (2005) Tracking USB Storage: Analysis of Windows Artifacts Generated by USB Storage Devices. Digital Investigation. The International Journal of Digital Forensics & Incident Response 2: 94-100.

51. Sabir F, Saleem S (2019) Microsoft Word Forensic Artifacts in Windows 10 Registry. International Conference on Applied and Engineering Mathematics, Pakistan, pp: 215-219.

52. Marczak B, Scott-Railton J, McKune S, Razzak BA, Deibert R (2018) Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. University of Toronto.

53. Mitre ATT&CK (2018) Defense Evasion and Techniques.

54. Mansfield-Devine S (2017) Understanding the NTFS $MFT and $MFTMirr files for forensic purposes. Digital Investigation 20: 23-31.

55. Domingues P, Andrade L, Frade M (2022) A Digital Forensic View of Windows 10 Notifications. Forensic Sci 2: 88-106.

56. (2024) Decoding Windows Event Logs: A Definitive Guide for Incident Responders.

57. (2021) Event Logging Functions. Event Logging.