Forensics of Registry:

UsrClass.dat.hive:

C:\Users<username>\AppData\Local\Microsoft\Windows\UsrClass.dat

NTUSER.dat hive :

Located under HKEY_CURRENT_USER

Registry Hive transaction logs:

The transaction log is named after the ntuser.dat.LOG 1 and ntuserdat.LOG2. The transaction log files are used to cache writes to the registry before they are permanently written to the hive.

Important registries:

MRU Lists (Most recent used lists):

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\

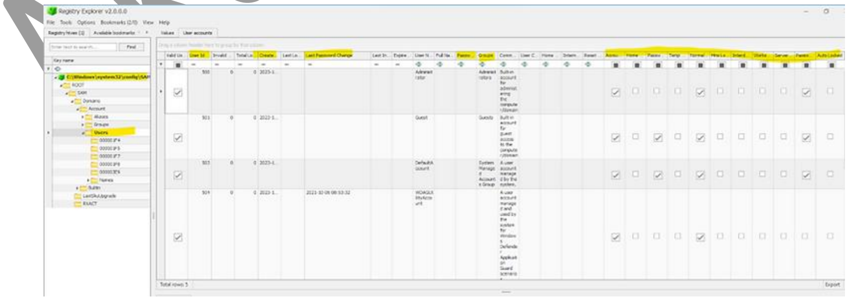
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\

Run Registry:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run

SAM profiling user/groups:

C:\Windows\System32\config\SAM



Valid Us...	User Id	Invalid...	Total Lo...	Create...	Last Lo...	Last Password Change	Last In...	Expire...	User N...	Full Na...	Passw...	Groups	Comm...	User C...	Home...	Intern...	Reset...	Accou...	Home...	Passw...	Temp...	Normal	Mns Lo...	Interd...	Worksta...	Server...	Passw...	Auto Locked
☑	500	0	0	2023-1...					Administrator			Administrators	Built-in account for administering the computer/domain					☑	☐	☐	☐	☑	☐	☐	☐	☐	☑	☐
☑	501	0	0	2023-1...					Guest			Guests	Built-in account for guest access to the computer/domain					☑	☐	☑	☐	☑	☐	☐	☐	☐	☑	☐
☑	503	0	0	2023-1...					DefaultAccount			System Managed Accounts Group	A user account managed by the system.					☑	☐	☑	☐	☑	☐	☐	☐	☐	☑	☐
☑	504	0	0	2023-1...		2023-10-06 08:53:32			WDAGUtilityAccount				A user account managed and used by the system for Windows Defender Application Guard scenario					☑	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐

Total rows: 5

System configuration:

Identify the Microsoft version:

SOFTWARE\Microsoft\Windows NT\CurrentVersion\

Identify current control set:

ControlSet001 represents the configuration used in the last successful boot, while ControlSet002 serves as a backup that can be used to recover from boot issues.

SYSTEM\Select

Computer name:

SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName

Time zone information:

SYSTEM\CurrentControlSet\Control\TimeZoneinformation

NTFS last access time on/off:

For instance, Microsoft disabled updates to last access timestamps in Windows Vista and subsequent versions for NTFS file systems to enhance performance. However, it's crucial to note that this setting only affects NTFS file systems, while other file systems like ExFAT and FAT continue to update access timestamps normally.

SYSTEM\CurrentControlSet\Control\FileSystem

Network interfaces:

This key contains a plethora of invaluable details, including TCP/IP configurations, IP addresses, gateways, and DHCP-related information. For machines configured with DHCP, it reveals the assigned IP address, subnet mask, and DHCP server's IP address.

SYSTEM\CurrentContro1Set\Services\Tcpip\Parameters\Interfaces

Historical network-network list keys:

https://www.cyberengage.org/post/part-2-important-registries-related-to-system-configuration-overview

HKLM\Software\Microsoft\Windows NT\CurrentVersion\NetworkList

SOFTWARE\Microsoft\ Windows NT\ CurrentVersion \NetworkList\Signatures\ Unmanaged

SOFTWARE\Microsoft\ Windows NT\ CurrentVersion \NetworkList\Signatures\Managed

Historical data, including connection times, can be found under the Cache key:

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

Network profile key: -First and last name connected:

Windows XP: SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces{GUID}

Windows 7-10 : SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

Shares and offline locations:

SYSTEM\CurrentControlSet\Services\lanmanserver\Shares\

For detailed Client-Side cashing:

https://www.cyberengage.org/post/part-3-important-registries-related-to-system-configuration-overview

System Boot autostart programs:

NTUSER.DAT

NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\Run

NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion \Run Once

Software Hive

Software\Microsoft\ Windows\CurrentVersion\RunOnce

Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run

Software\Microsoft\ Windows\CurrentVersion \Run

System Hive:

SYSTEM\CurrentControlSet\Services

Shutdown information: System hive:

SYSTEM\CurrentControlSet\Control\Windows (Shutdown Time)

SYSTEM\CurrentControlSet\Control\Watchdog\Display (Shutdown Count)

User Activity:

Search History:

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

Typed Path:

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

Recent Docs:

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

Microsoft Office Recent Docs:

https://www.cyberengage.org/post/part-1-windows-registry-artifacts-insights-into-user-activity

NTUSER.DAT\Software\Microsoft\Office\VERSION

This key stores information about the Office version, where VERSION can be either 16.0 or 14.0.

NTUSER.DAT\Software\Microsoft\Office\VERSION\User MRU\LiveID_####\File MRU

This key contains information about recently accessed files and documents within specific Office applications.

"PlaceMRU," which shows the path of the location of the previously opened file in that directory.

Software\Microsoft\Office\14.0\Word\File MRU

Software\Microsoft\Office\14.0\Excel\File MRU

Software\Microsoft\Office\16 0\Powerpoint\User MRU\LiveID_####\File MRU

Last Visited MRU/ Open Save MRU:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\

Last Visited Pid MRU:- Track application executable used to open files in Open save MRU and the last file path used (Program execution)

Open save pid MRU"- Values under this show items input in open save dialog without an extension (File knowledge)

* :-(track the most recent files of any extension input in open save dialog).

Last Commands executed:

NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

BAM/DAM:

Record information about executed programs, including the path of the executable and the date/time of the last execution.

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

SYSTEM\CurrentControlSet\Services\Dam\UserSettings\{SID}

UserAssist Key:

https://www.cyberengage.org/post/program-execution-userassist-registry-key-shimcache-amcache-bam-dam

The UserAssist key, located within the NTUSER.DAT hive of the Windows registry, contains valuable information about GUI program executions initiated by users.