DIGITAL FORENSICS

Lecture 7

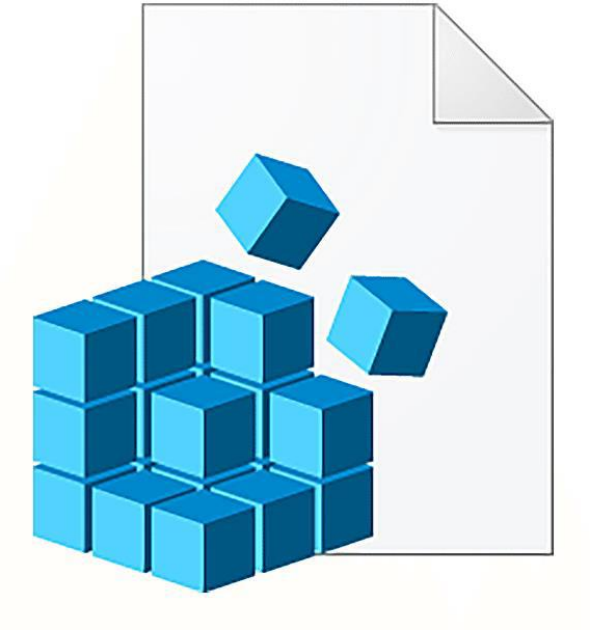
Course Instructor: Dr. Marwa Zamzam
Email: marwa.zamzam@giu-uni.de
Instructor Office: A214
Teaching Assistants
Eng. Salma Abubakr

These slides are based on the updated version of those by Assoc. Prof. Dr. Amr ElMougy.

What is the Windows Registry?

- The Registry is considered a central **nervous system** of a computer.

- It's like a great **administrative assistant**. It knows your desktop settings, it understands your **preferences**, what you like to run in startup versus with the system likes to run in startup.



Importance of Windows Registry

- The Windows registry is a **hierarchical database** that stores information about users, installed application, and the Windows system itself.
- It keeps track of **settings** for both the **users** and the **system**, it keeps track of **historical information.**
- You may be able to see **programs** within the Registry that **no longer reside on the system.**
- You may be able to see **USB devices** that were attached at one time that are no longer attached to the system.
- The registry can be thought of as a kind of DNA for the Windows operating system. It can provide an infinite amount of evidence.

Registry Artifacts

- What **type of case** are you investigating:
  - Intellectual property theft
  - Fraud
  - Harassment
  - Child exploitation
  - Incident response

- The type of case will determine what **kind of info** to look for in the registry:
  - Program execution
  - Last logged-on user
  - Network settings
  - File associations
  - Run lists
  - Time zone
  - Typed URL Information
  - Machine shutdown dates and times
  - User accounts/profile information
  - Wi-Fi information
  - Browsing-related information
  - USB connections dates and times
  - Web Searches

Registry Artifacts

- Windows registry is a tree structure where each node in the tree is called **a key** and every key may have a **value or sub-keys.**

- The **registry** contains:
  - **User** information:
    - What has the user typed into the search bar, MRU (Most Recently Used applications).
  - **System** information:
    - computer name, last shutdown, WiFi information.
  - **Application**-specific information
    - configurations, licensing information.

- The registry acts as a sort of **log file**. System changes and user-created changes are often tracked in the registry.

- The registry is made up of several files called **hives.** When the computer is booted up, The Hive files are booted into the memory.

- A hive is a logical group of **keys, subkeys, and values** in the registry that has a set of supporting files loaded into memory when the operating system is started or a user logs in.

How the Registry Works: Handle Keys

- **HKEY_LOCAL_MACHINE (HKLM):** Contains information about the system's installed hardware, software, and general system settings, which is useful for understanding the setup of the computer.

- **HKEY_CLASSES_ROOT (HKCR):** Describes define file associations (which application opens each file type) and file extension. This can help investigators understand which programs are set to open certain file types, indicating a user's preferred software.

- **HKEY_CURRENT_CONFIG (HKCC):** The details about the real time information current configuration of hardware attached to the computer.

- **HKEY_USERS (HKU):** Contains information about all the users who log on to the computer. This can help in reconstruct user-specific activity.

- **HKEY_CURRENT_USER (HKCU):** Contains user who is currently logged in to Windows and their settings. This provides a snapshot of the user's recent activity and environment.

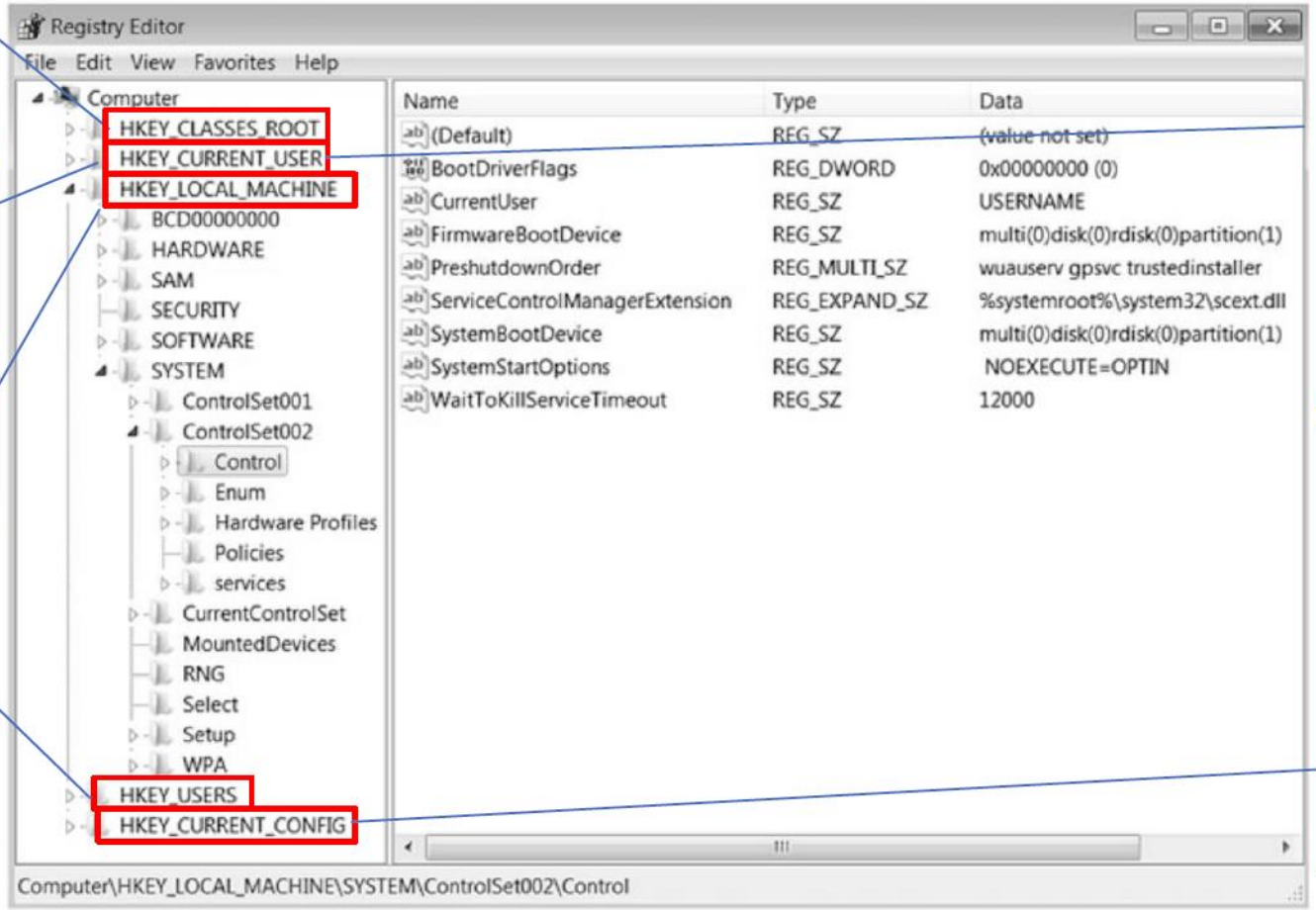
How the Registry Works: Handle Keys

Contains information about registered applications.

Contains the data stored for the current user

Contains settings that are specific to the local computer.

Contains subkeys corresponding to the HKEY_CURRENT_USER keys for **each user profile** actively loaded on the machine.

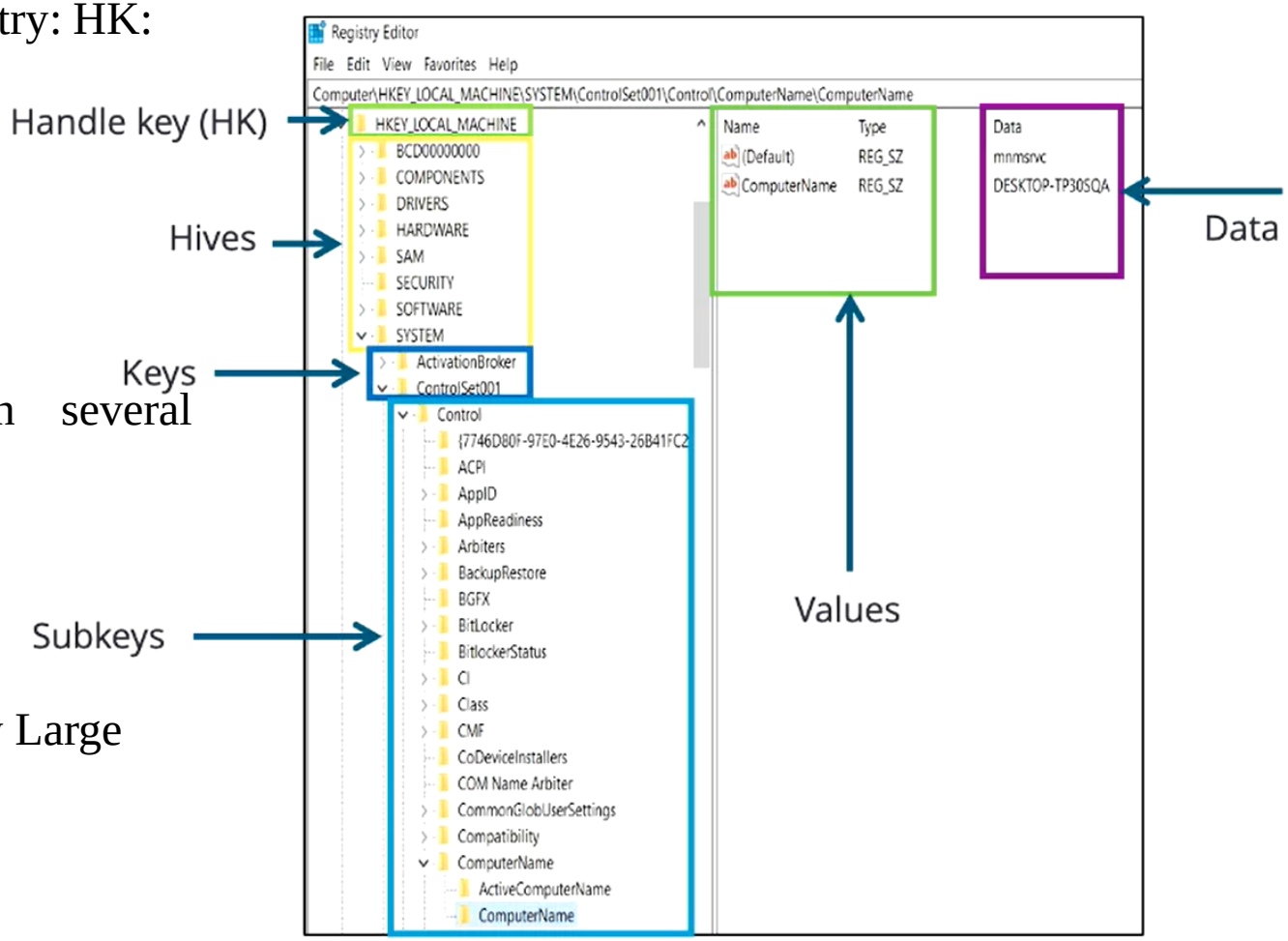


Stores information about a specific user account. This hive can contain information such as the user's browser settings and history and data related to user applications.

It 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.

Structure of the Windows Registry

- Layout of the registry: HK:
  - Hives
  - Keys
  - Sub-keys
  - Values
  - Data
- Data can be in several **different forms:**
  - Binary data
  - String data
  - Hex data
  - BLOB (Binary Large Object) data



Registry Hive Files

- We will need to use specialized tools to view the registry files (FTK manager).

- The Hive files that make up the Windows registry can be divided into two types of classes:

1. **System files:** The system files will dictate system-wide settings.
   - SAM
   - System
   - Security
   - Software

2. **User files:** The user files are going to be specific to that individual user.
   - NT User.dat
   - User Class.dat

Registry Hive Files

- We will need to use specialized tools to view the registry files (FTK manager).

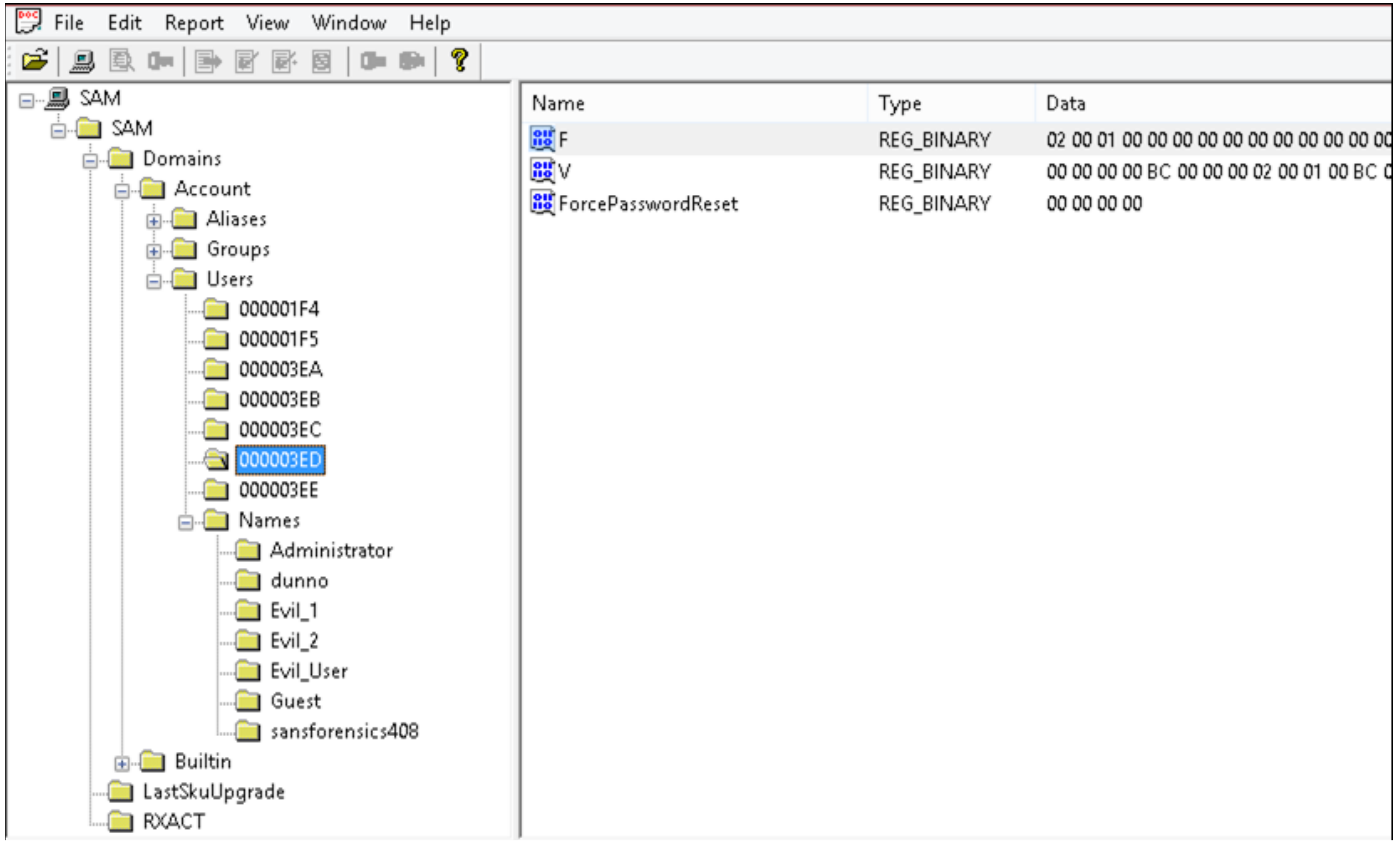
- The Hive files that make up the Windows registry can be divided into two types of classes:

1. **System files:** The system files will dictate system-wide settings.
   - SAM
   - System
   - Security
   - Software

2. **User files:** The user files are going to be specific to that individual user.
   - NT User.dat
   - User Class.dat

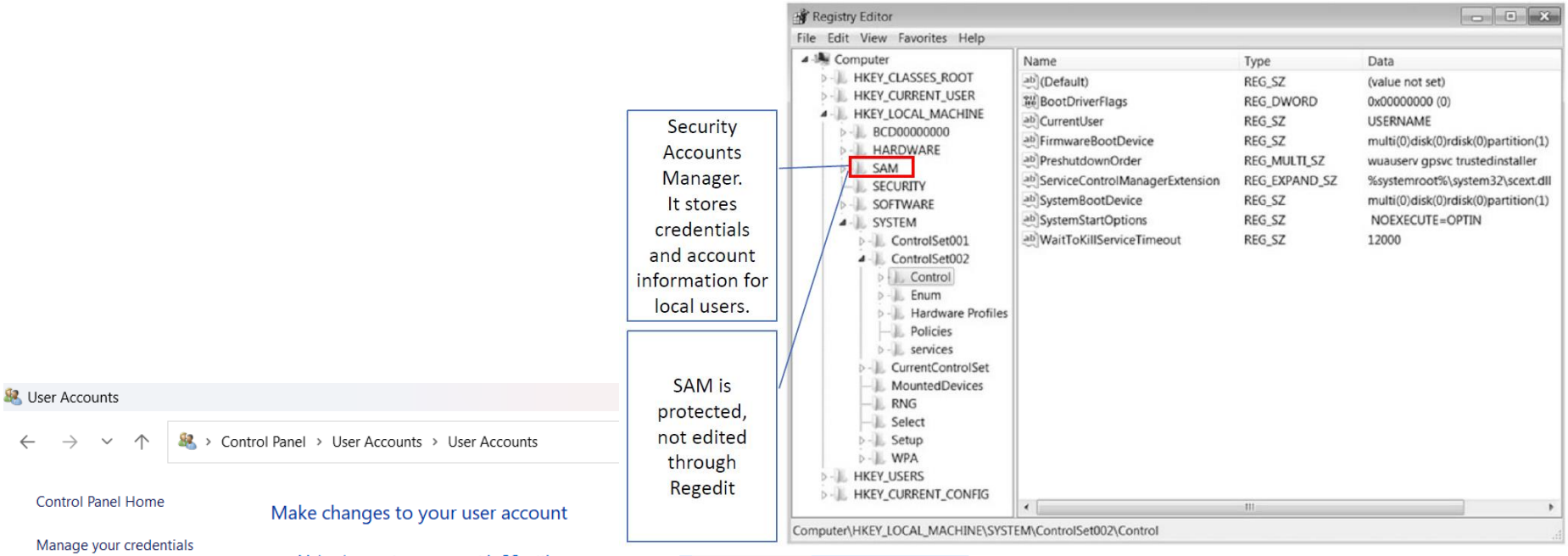
System Files: SAM

- The SAM is a database file stores and organizes information about each user, such as login information and login password hashes.



System Files: SAM

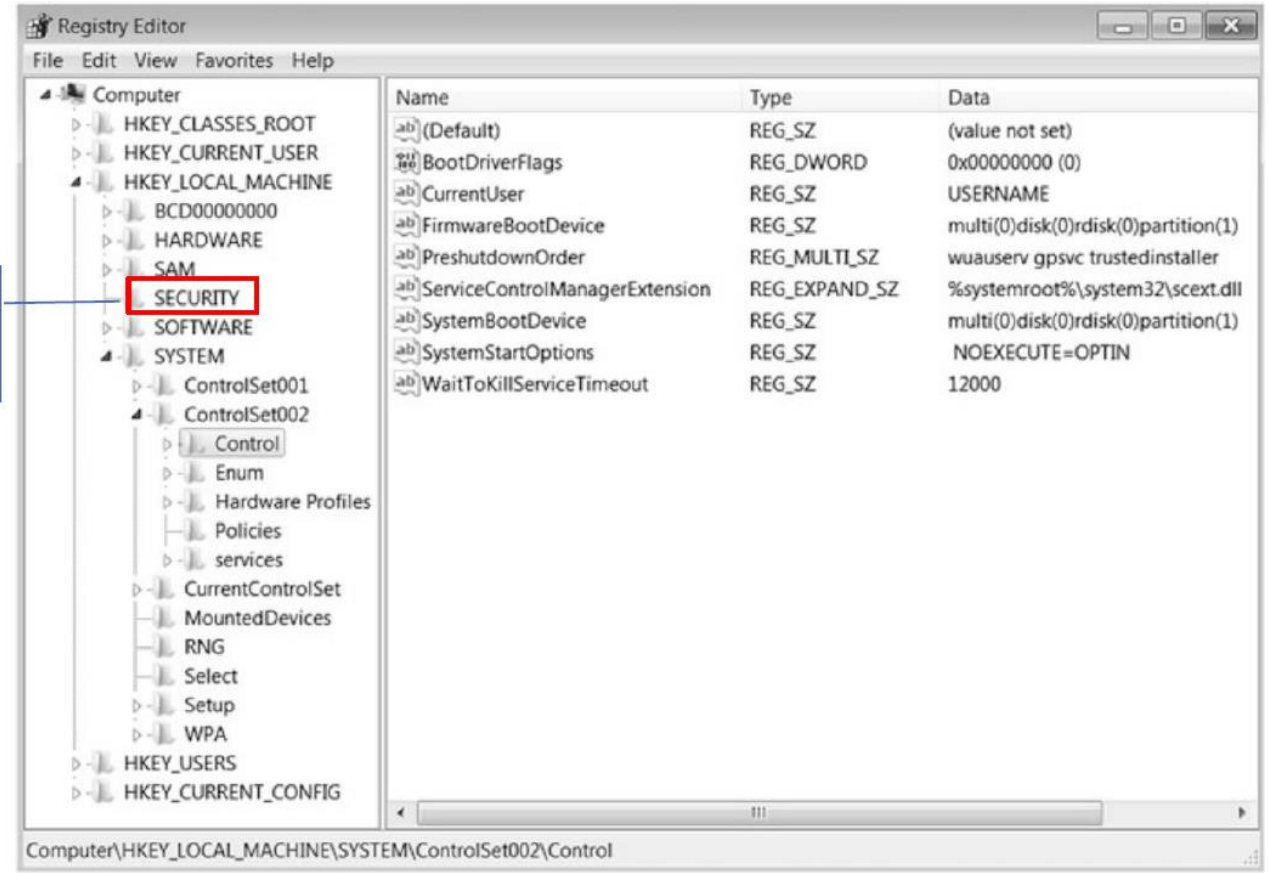
- SAM: Security Account Manager
  - The SAM file is a root key of the HKEY_LOCAL_MACHINE hive
  - C:\Windows\System32\config\SAM
  - Control panel: User accounts or manage: Local users and groups: Users



System Files: Security

- Security file overview
  - Security Hive file the overall security policies of the system, including access permissions and system audit configurations.
  - The security file is a root key of the HKEY_LOCAL_MACHINE hive
  - C:\Windows\System32\config\security

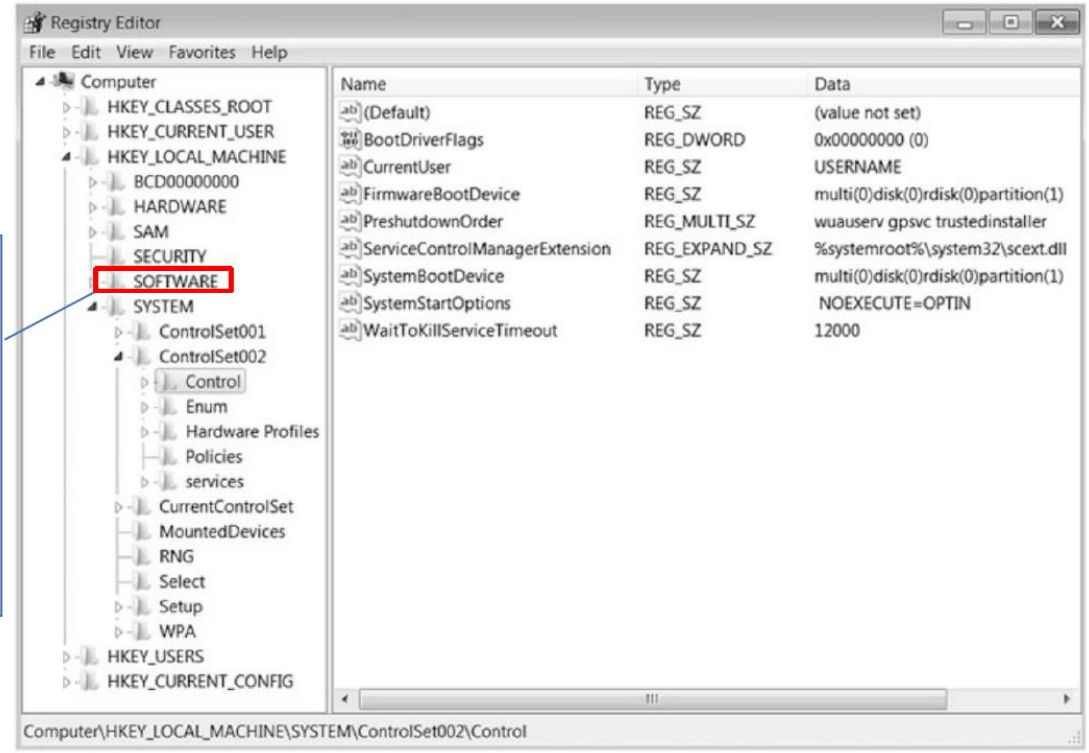
Mainly stores security policy.



System Files: Software

- Software file overview
  - Software Hive file consists, all the information regarding the software installed in this system.
  - The software file is a root key of the HKEY_LOCAL_MACHINE hive
  - C:\Windows\System32\config\software

Contains information related to applications. This includes data stored by Windows and data stored by other applications.



System Files: Software

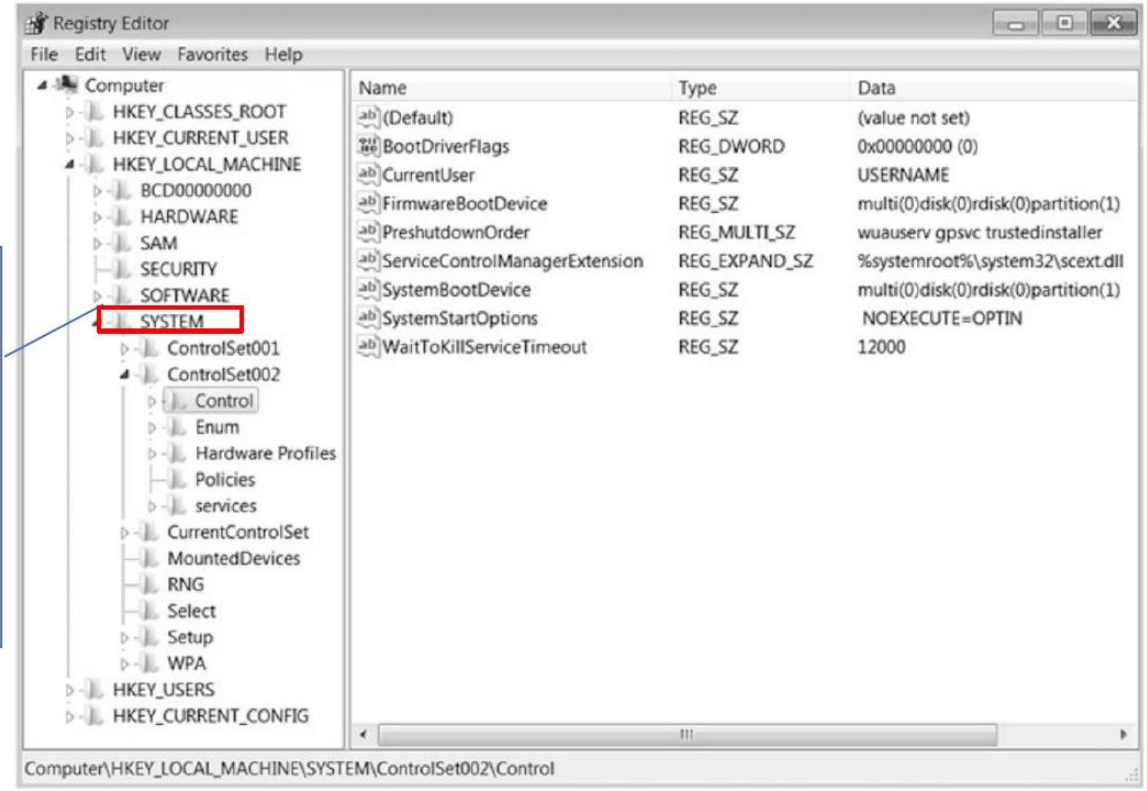
- Software file overview

1. Installed programs and applications
2. Operating system type and install date and time
3. Wireless network information
4. File association
5. Logon information
6. Attached devices

System Files: System

- System file overview
  - System Hive file consists, configuration information about the hardware and system settings necessary for Windows to start and operate.
  - The software file is a root key of the HKEY_LOCAL_MACHINE hive
  - C:\Windows\System32\config\system

Contains information about the Windows system setup



System Files: System

- System file overview

1. Computer name
2. Last shutdown time
3. Crash dump settings and location
4. Services set to run
5. Clear page file at shutdown
6. Last access file time settings

System: Memory Management

- Subkey name: Memory Management
- Location: ControlSet001\Control\Session Manager\Memory Management
- Value name: ClearPageFileAtShutdown

- Data 0 = Page file is not being cleared at shutdown

- Data 1 = Page file is being cleared at shutdown

System: Crash dump setting

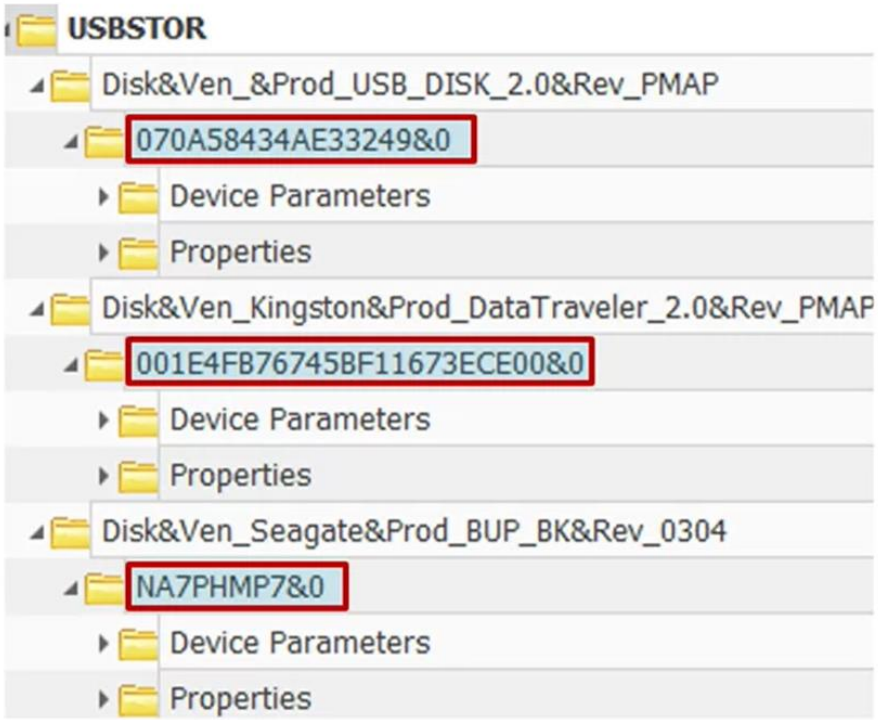
Crash dump setting

- Subkey name: CrashControl
- Location: ControlSet001\Control\CrashControl
- Value name: Dumpfile
- Value name: Minidumpdir

When a critical error occurs (such as Blue Screen of Death (BSoD)), the system creates memory dump files (also known as "crash dumps"). These files contain **a copy of the system memory at the moment of the crash**, which can help to diagnose and determine the reason for the problem

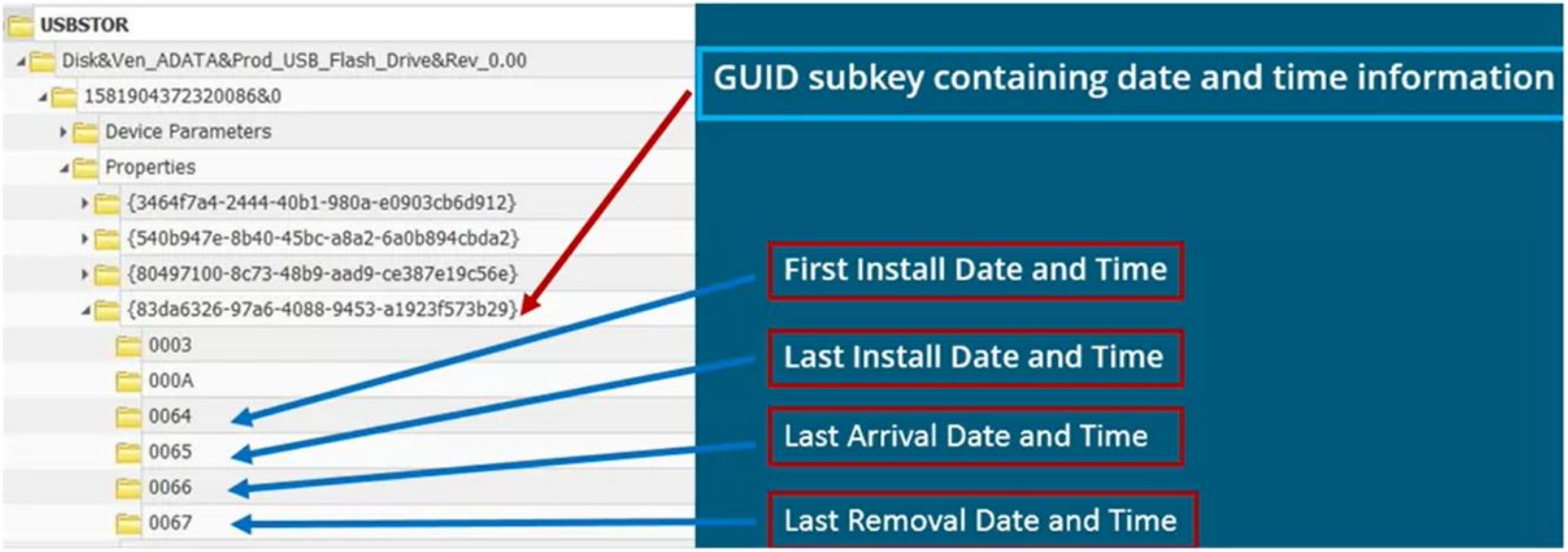
System: USB-connected devices

- USB device forensics
  - Subkey name: USBSTOR
  - Device serial numbers



System: USB-connected devices

- USB device – installation, connection and disconnection times



The SAM and Security hives

- **A live system** refers to a computer that is currently running and actively operating. When a system is "live," it means the operating system is loaded, users can interact with it, and programs and services are running.

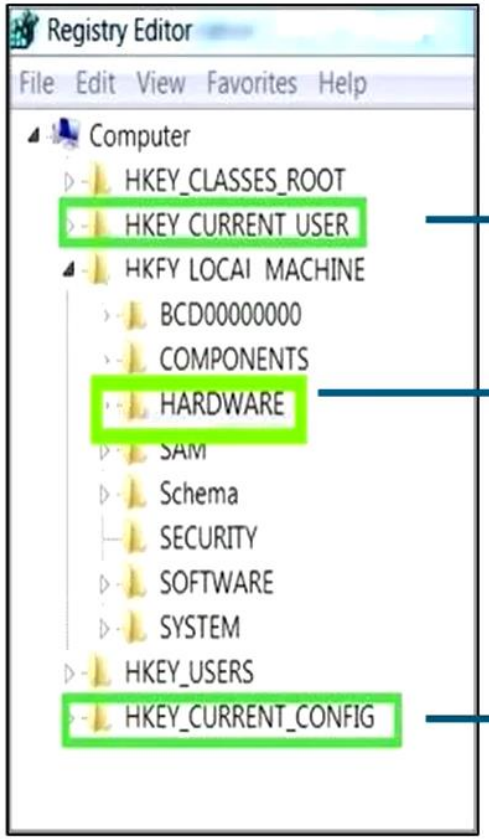
- In the context of digital forensics, examining certain files or data on a live system can be challenging because the operating system protects important files (like the SAM and SECURITY hives) from being accessed directly to prevent tampering or unauthorized access.

- The SAM hive contains usernames and password hashes (encrypted representations of passwords) for all user accounts on the system. If someone could access this data easily, they might attempt to crack the hashes to retrieve plain-text passwords, potentially gaining unauthorized access to user accounts. By protecting SAM, Windows helps safeguard user data and privacy.

- The Syskey in Security hive is essential for encrypting password hashes. If someone could alter these settings, they could potentially disable security monitoring or tamper with password protection.

Live Registry

- **Disable access to Sam and security subkeys**

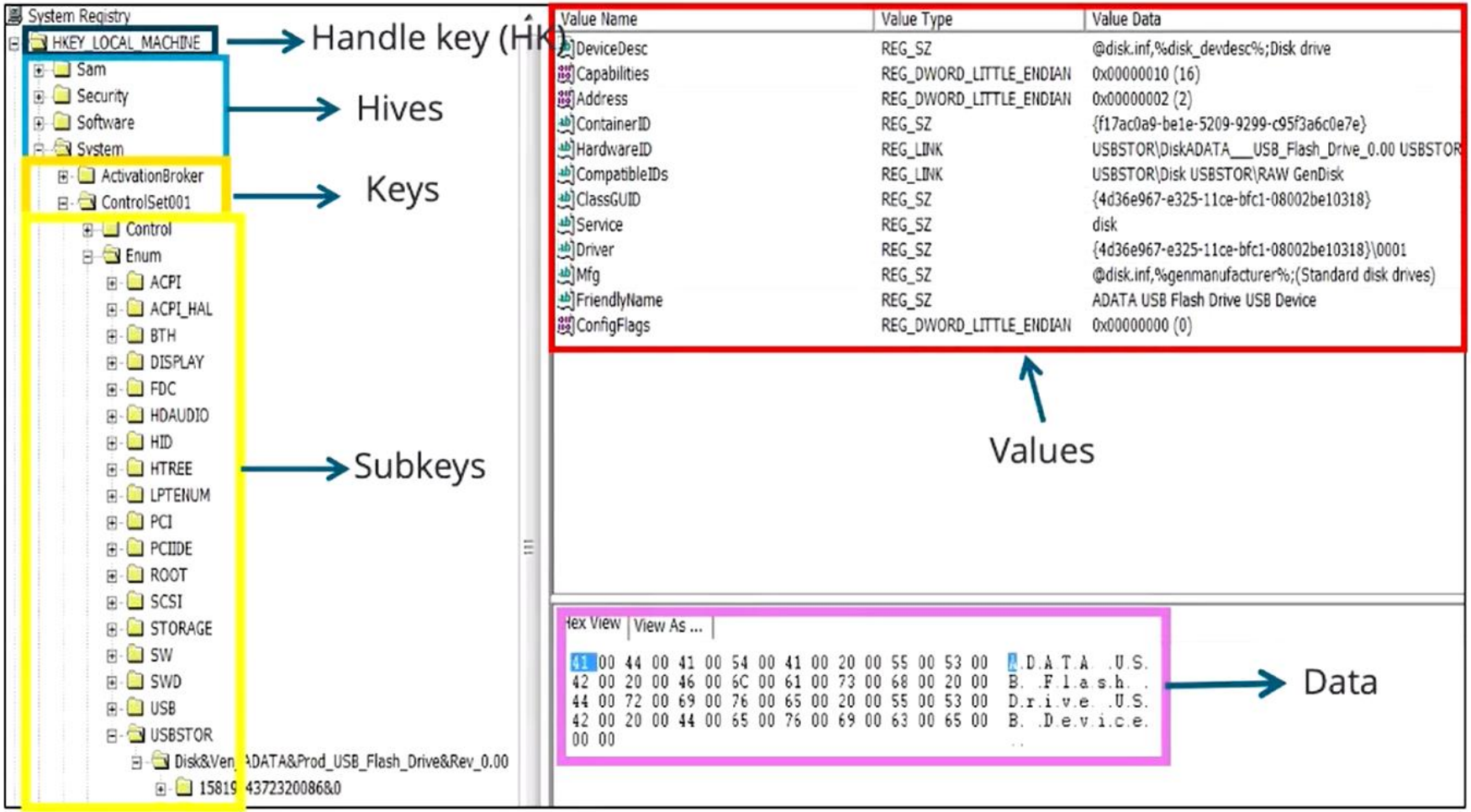


Only found on live system — currently logged-on user

Only found on live system — BIOS and current hardware configuration

Only found on live system — current system configuration

Non-Live Registry, as seen using registry browser



Registry Hive Files

- We will need to use specialized tools to view the registry files (FTK manager).
- The Hive files that make up the Windows registry can be divided into two types of classes:

1. **System files:** The system files will dictate system-wide settings.
   - SAM
   - System
   - Security
   - Software

2. **User files:** The user files are going to be specific to that individual user.
   - NT User.dat
   - User Class.dat

User Files: NT User

- NT User file is a root key of the HKEY_CURRENT_USER hive.

- This file stores personalized settings and preferences for each user, like desktop background, browser settings, and application configurations. Every time a user logs into their account, Windows reads this file to apply their unique settings. It's like a "profile" file that keeps track of a user's individual preferences.

  - Recent docs subkey
  - Typed URLs subkey
  - User assist
  - Run and run once
  - Word wheel query

User Files: NT User

- **Recent docs**
  - Documents **already accessed by a specific user**.
  - Also includes the **recent documents** by file extension
  - File path: Software\Microsoft\Windows\CurrentVersion\Explorer\Recent Docs

- **UserAssist Key**
  - Maintains a list of items such as **programs**, **shortcuts, and control panel applets** that a user has **accessed**. Making **these programs accessible to the user from the start menu.**
  - It's very helpful in building your **timeline** when you're seeing what **applications** were being used **at what time.**
  - File path: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

User Files: NT User

❑ Run and Run Once

- User-specific programs that are set to **run at startup with no interaction form the user** other than logging into Windows

- **The run key is persistent** and that may be one of the reasons that **malware** gets installed there. Even if you shut your computer down and restart it, that run key is going to be triggered and whatever values are under that run key will be executed.

- **The run once key is not persistent**. It should do what exactly what it says run once and then the value should be deleted.

- File path: Software\Microsoft\Windows\CurrentVersion\Run

User Files: NT User

- **Typed URLs**
  - Tracks **URLs typed into the Internet Explorer address bar**
  - This becomes populated when a user types or uses the **autocomplete function** to type a URL (web address) into the Internet Explorer address bar
  - File path: Software\Microsoft\Internet Explorer\TypedURLs

- **Word Wheel Query**
  - Searches conducted by the user from the **start menu and Windows Explorer**
  - Contains an Most Recently Used (**MRU)** order
  - Key **last access date**
  - **Search terms typed by the user**
  - Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

User Files: User Class.dat

- User Class file is a root key of the HKEY_CURRENT_USER hive.

- This file contains additional information specific to each user, particularly related to the layout and interactions within the Windows environment, like certain app and menu settings.

- It helps Windows remember details like the size and position of open windows for each user.

  - The size, position, and arrangement of open windows.
  - How files and folders are displayed in Explorer.
  - The appearance of the taskbar, Start menu, and other user interface elements.
  - Window state (minimized, maximized) for different apps.
  - Recent files opened within an app.
  - User preferences specific to each application, such as view options in a file manager.

Thank You ☺