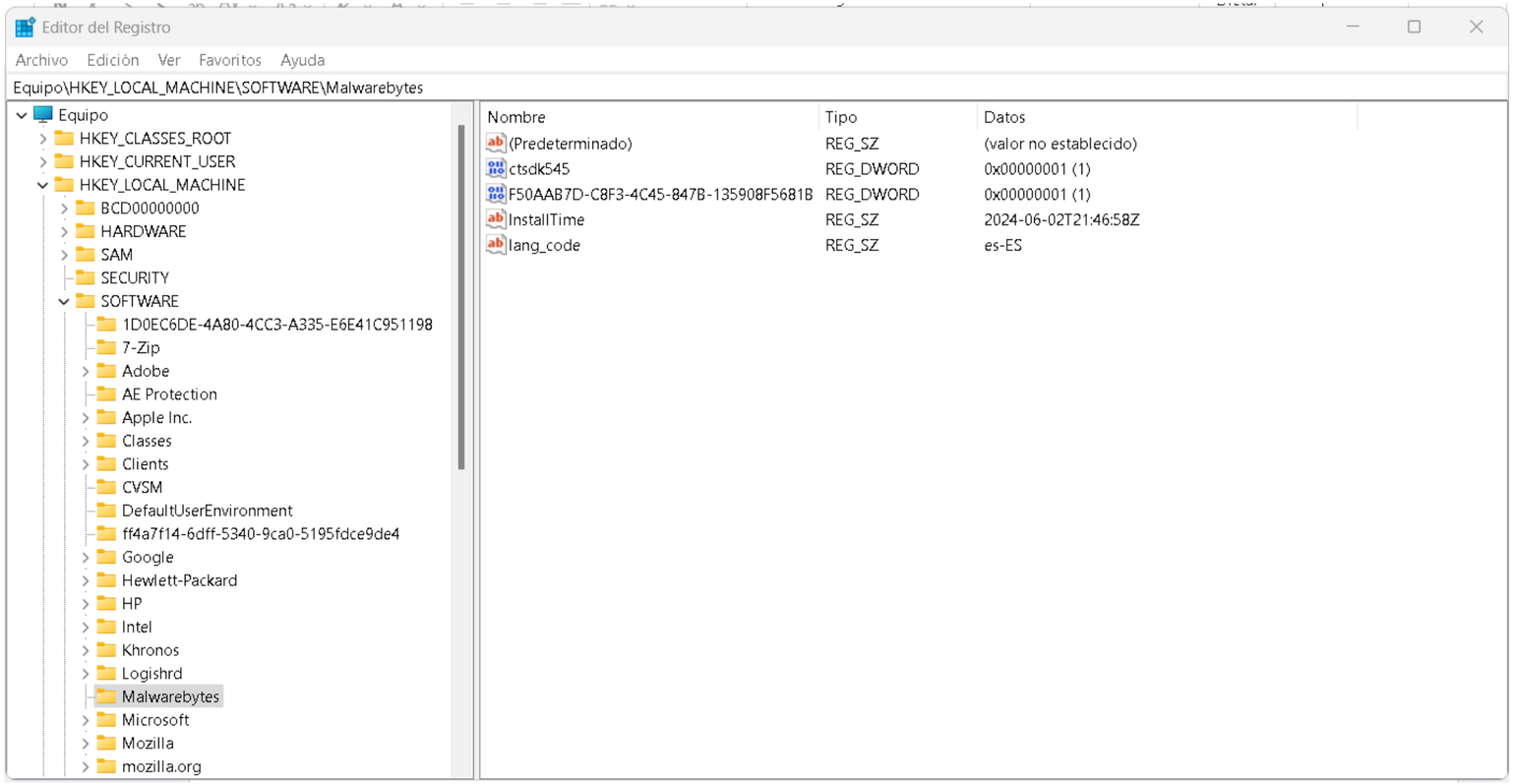
THE BRIDGE

Windows Register para forence

Registro de Windows

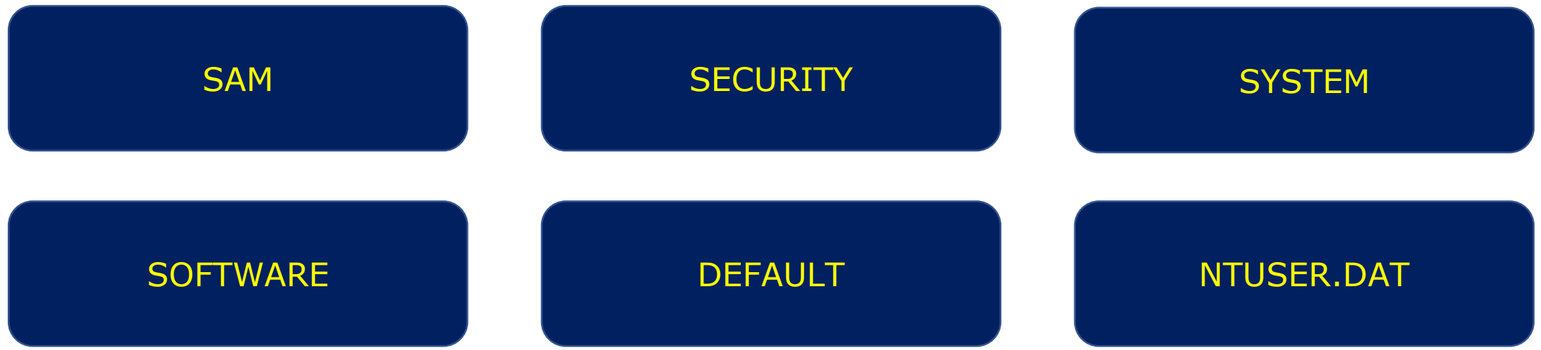
- El **Registro de Windows** es una estructura jerárquica que organiza la información en claves (similares a carpetas) y valores (similares a archivos), donde se almacenan configuraciones y opciones.
- El **Registro de Windows** es una base de datos centralizada que almacena configuraciones y opciones del sistema operativo, hardware, software y cuentas de usuario.
- Registro de Windows.



https://fwhibbit.es/registro-de-windows-prepara-la-cafetera

Hives

- Un **hive** es una porción independiente de esa base de datos del Registro que se almacena en archivos en disco.
- Cada **hive** contiene un conjunto de claves, subclaves, valores y datos que corresponden a una sección particular.
  - C:\Documents and Setting\User Profile\NTUSER.DAT o C: \Users\User Profile\NTUSER.DAT
  - C:\Windows\System32\config\DEFAULT
  - C:\Windows\System32\config\SAM
  - C:\Windows\System32\config\SECURITY
  - C:\Windows\System32\config\SOFTWARE
  - C:\Windows\System32\config\SYSTEM
- Algunos **Hive** son volátiles y no se almacenan en el disco y no todos se cargan a la vez.



https://fwhibbit.es/registro-de-windows-prepara-la-cafetera

Claves de Registro para forense - SYSTEM

- **Nombre de Sistema:**
  - HKLM\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName
- **Nombre del Sistema y Hora de apagado:**
  - HKLM\SYSTEM\ControlSet00x\Control\Windows
- **Timezone:**
  - HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation
- **Unidades USB Montadas:**
  - HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR
  - HKLM\SYSTEM\MountedDevices
- **Lista de servicios del sistema:**
  - HKLM\SYSTEM\CurrentControlSet\Services\
- **Configuraciones de red:**
  - HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\GUID

Claves de Registro para forense - SOFTWARE

- **Fecha de instalación de un Sistema:**
  - HKLM\SOFTWARE\Microsoft\Windows NT\currentversion\installdate

- **Configuración de redes inalámbricas:**
  - HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces
  - HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\GUID

- **Programas de “instalar o quitar programas”:**
  - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

- **Datos predeterminados del explorer.exe:**
  - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

- **Comandos que se ejecutan al abrir un cmd:**
  - HKLM\Software\Microsoft\Command Processor\AutoRun25

- **Perfiles de usuario:**
  - HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList

Claves de Registro para forense – NTUSER 1

- **Ficheros abiertos ejecutados recientemente:**
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU (XP)
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDIMRU (Win7)
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU (XP)
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPIDIMRU (Win7)
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

- **Documentos recientes de Office:**
  - HKCU\Software\Microsoft\Office\VERSION
  - 14: Office 2010
  - 12: Office 2007
  - 11: Office 2003
  - 10: Office XP

- **Listado de recursos de red mapeados:**
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU
-
- **Se crean entradas para las unidades de red:**
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

Claves de Registro para forense – NTUSER 2

- **Aplicaciones ejecutadas durante el inicio del sistema:**
  - HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
  - HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce ProfilePath\Start Menu\Programs\Startup\

- **URLs accedidas por el usuario:**

  - HKCU\Software\Microsoft\Internet Explorer\TypedURLs

- **Búsquedas realizadas por el usuario:**

  - HKCU\Software\Microsoft\Search Assistant\ACMru (XP)
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery (Win7)

- **Comandos ejecutados desde el menú Inicio:**
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU


THE
BRIDGE