**Análisis del Registro de Windows: seguimiento de cada actividad que realiza en el sistema Windows**



El propósito de este artículo es brindarle una **comprensión profunda** del **Registro de Windows** y la gran cantidad de información que contiene.

Hoy en día, para la mayoría de los administradores y analistas forenses, el registro probablemente parezca la entrada a una oscuridad.

Además de la información de configuración, el Registro de Windows contiene información sobre los archivos a los que se accedió recientemente e información considerable sobre las actividades del usuario.

La verdad es que el Registro es una verdadera mina de oro de información tanto para el administrador como para el investigador forense.

## **¿Qué es el Registro?**

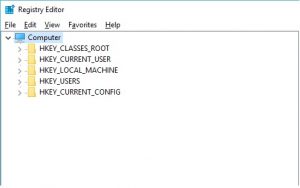
Si recuerda **DOS** y las primeras versiones de Windows (3.1, 3.11, etc.), **la información de configuración** (controladores, configuraciones) del sistema se administraba en gran medida mediante varios archivos, específicamente **autoexec.bat, config.sys, win.ini.**  (en Windows) y **system.ini** .

Varias configuraciones dentro de estos archivos determinaron qué programas se cargaron y cómo se veía el sistema y respondía a las entradas del usuario. Las versiones posteriores de Windows reemplazaron estos archivos con el Registro, una base de datos jerárquica central que mantiene los ajustes de configuración

para la aplicación, los dispositivos de hardware y los usuarios.

### **¡Cómo se ve la estructura del Registro de Windows!**

Cuando el administrador o **Forensics espera** abrir **Regedit.exe** , ve una estructura en forma de árbol con cinco carpetas raíz o "colmenas".



* **La colmena HKEY\_CLASSES\_ROOT** contiene información de configuración relacionada con qué aplicación se utiliza para abrir varios archivos en el sistema.
* **La colmena HKEY\_CURRENT\_USER es el perfil de usuario** activo y cargado para el usuario que ha iniciado sesión actualmente.
* **La colmena HKEY\_LOCAL\_MACHINE** contiene **amplia información de configuración** para el sistema, incluidas configuraciones de hardware y configuraciones de software.
* **La colmena HKEY\_USERS** contiene todos los **perfiles de usuario cargados** activamente para ese sistema.
* **La colmena HKEY\_CURRENT\_CONFIG** contiene el **perfil de hardware** que utiliza el sistema al inicio.

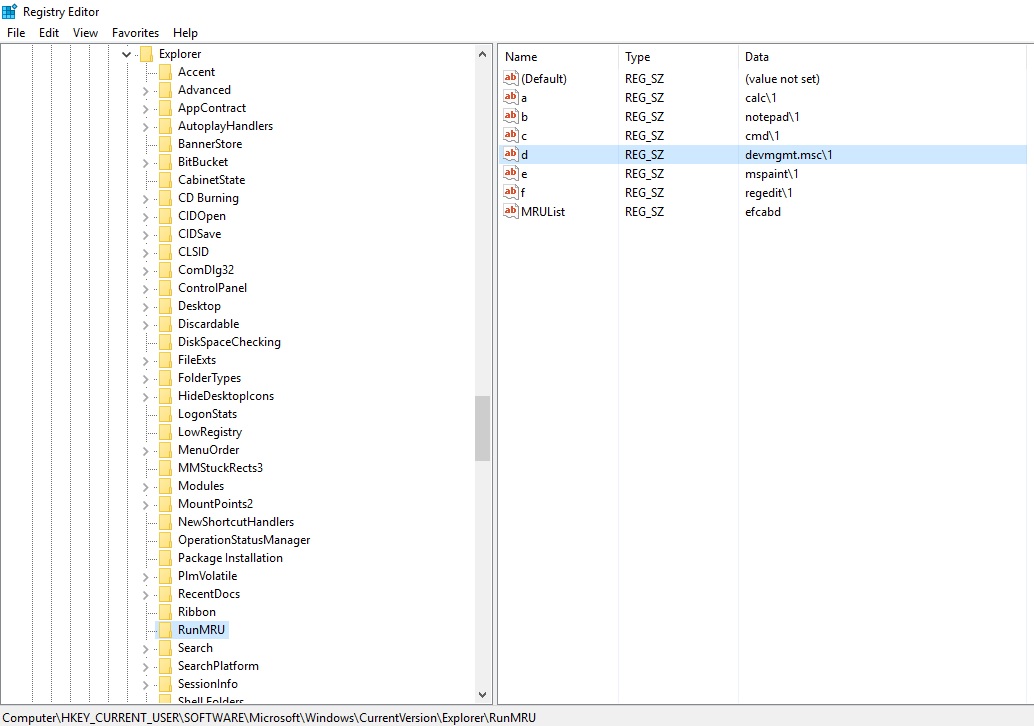
### **Examen de Registro**

#### **Listas MRU:**

MRU, en toda la lista o "usado más recientemente", contiene entradas realizadas debido a acciones específicas realizadas por el usuario. Existen numerosos MRU LIS en varias claves de registro.

El Registro mantiene estas listas de elementos en caso de que el usuario vuelva a consultarlas en el futuro. Es similar a cómo actúan el **historial y las cookies** en un navegador web.

La ubicación de esta clave es  ***HKEY\_CURRENT\_USER\software\microsoft\windows\currentversion\Explorer\RunMRU*** y contiene

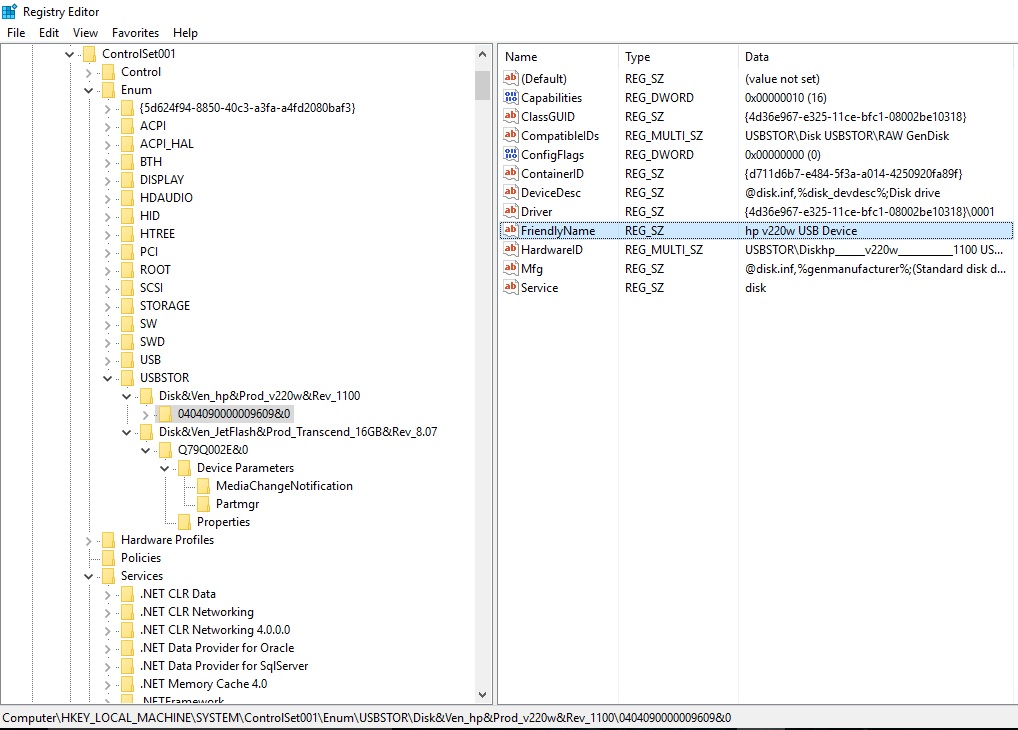
[](https://gbhackers.com/wp-content/uploads/2017/06/reg2.jpg)

Con la información proporcionada por la **clave RunMRU** , un examinador puede comprender mejor al usuario que está investigando y la aplicación que se está utilizando. En la figura anterior, puede ver que el usuario abrió **cmd, Bloc de notas, MSPaint** , etc.

## **Dispositivos USB:**

Cada vez que se conecta un dispositivo al bus serie universal (USB), se consultan los controladores y la información del dispositivo se almacena en el Registro (unidades USB).

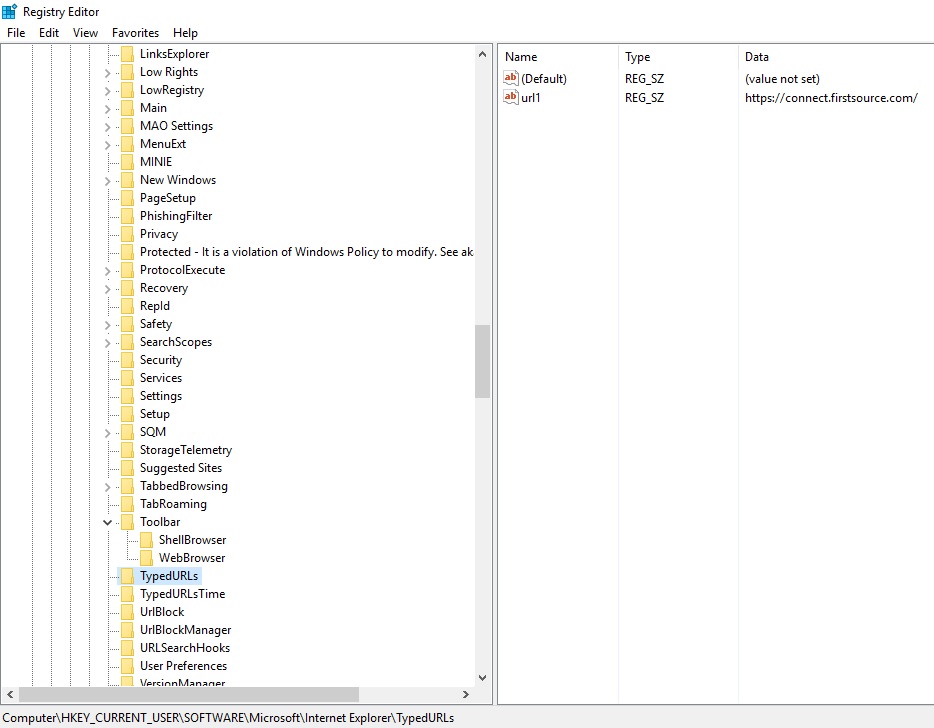
**Esta clave almacena el contenido de los valores de identificación** del producto y del dispositivo de cualquier dispositivo USB que alguna vez se haya conectado al sistema.

[**Entonces, los expertos forenses profundizarán en la ruta HKEY\_LOCAL\_MACHINE\SYSTEM\controlset001\Enum\USBSTOR.**](https://gbhackers.com/windows-registry-analysis-tracking-everything-you-do-on-the-system/)[](https://gbhackers.com/wp-content/uploads/2017/06/reg3.jpg)

## **Explorador de Internet:**

**Internet Explorer** es el navegador web nativo del sistema operativo Windows. Utiliza ampliamente el Registro en el **almacenamiento de datos, como muchas aplicaciones.**

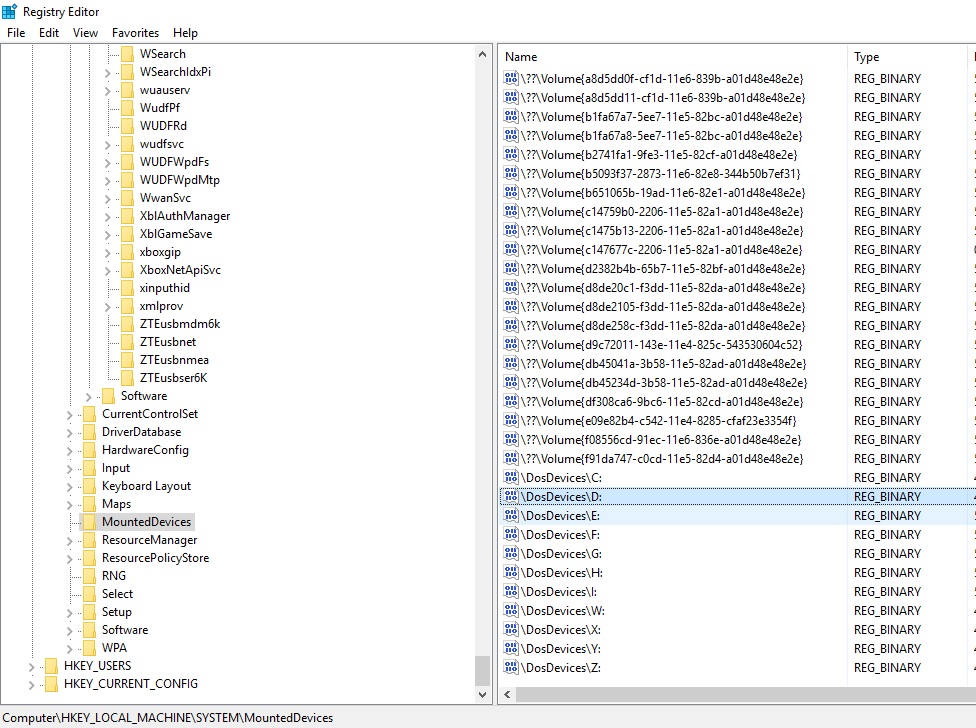
***Internet Explorer almacena sus datos en HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\TypedURLs.***

[](https://gbhackers.com/wp-content/uploads/2017/06/reg4.jpg)

## **Hardware adjunto:**

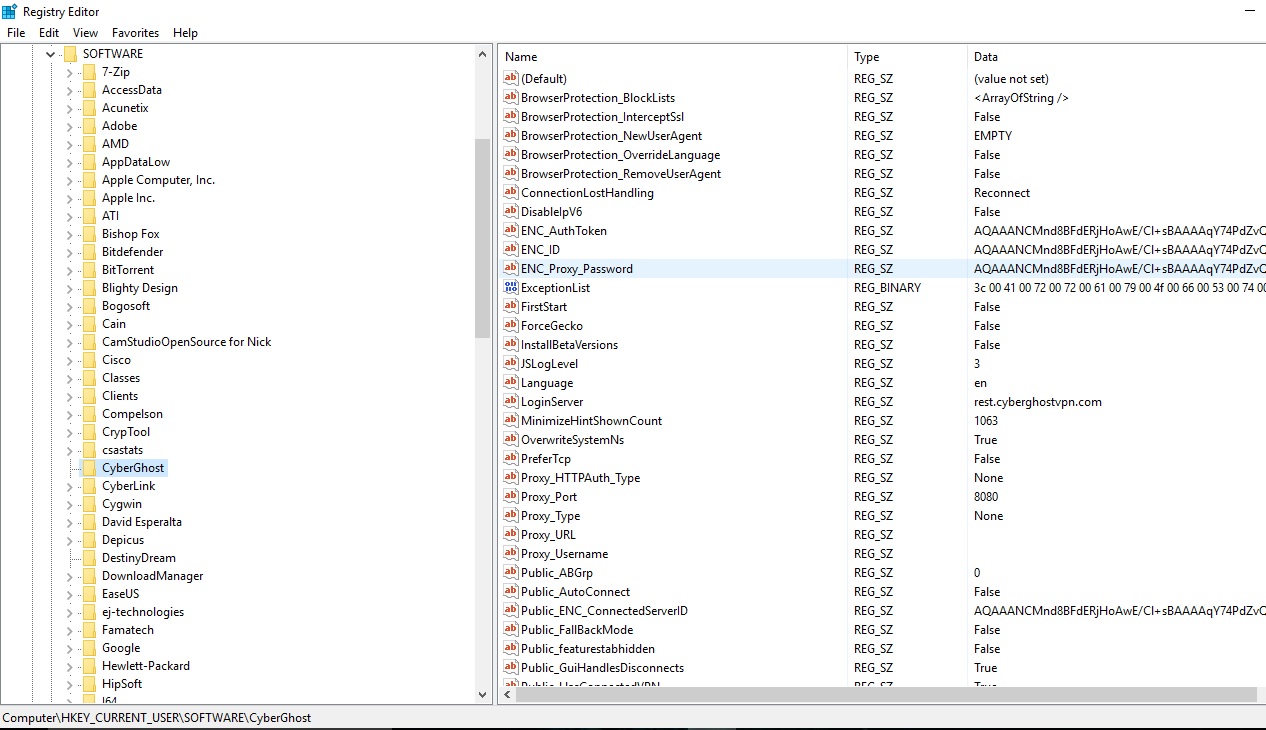
Navegando a la siguiente clave  **HKEY\_LOCAL\_MACHINE\SYSTEM** |MountedDevices. Esta información puede ser útil para un **examinador forense** ya que muestra que el **sistema operativo ha reconocido cualquier dispositivo de almacenamiento conectado.**

Si el examinador nota una discrepancia entre los **dispositivos físicamente conectados** y los reportados aquí, puede ser una indicación de que algún dispositivo fue retirado antes de que se incautaran las pruebas.

[](https://gbhackers.com/wp-content/uploads/2017/06/reg5.jpg)

## **Software malicioso:**

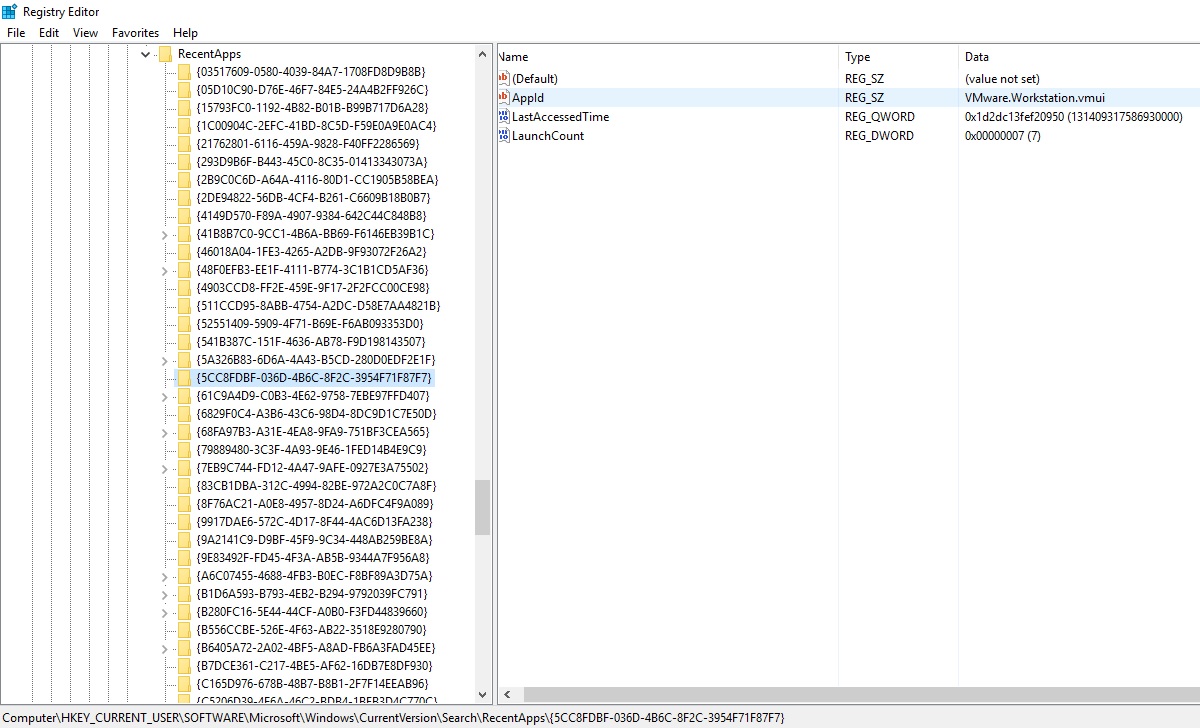
Al navegar a la siguiente clave  **HKEY\_CURRENT\_USER\Software\,**  esta información será interesante para Forensics Examiner, ya que podría ver que el hacker usó **CyberGhost Vpn** , que se usa para ser anónimo.

[](https://gbhackers.com/wp-content/uploads/2017/06/reg6.jpg)

## **Aplicaciones recientes:**

Navegar a la siguiente clave proporcionará información sobre la lista **de aplicaciones a las que se accedió por última vez HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Currentversion\Search\RecentApps.**

Este usuario tiene una amplia lista de aplicaciones, una de las cuales fue Vmworkstation encontrada.

[](https://gbhackers.com/wp-content/uploads/2017/06/reg7.jpg)

**Se puede obtener información crucial** realizando un **examen forense eficiente y eficaz.**

Para que pueda investigar y encontrar actividades maliciosas en curso en su entorno. Feliz investigando!!!!!