El Registro de Windows

Introducción

Al trabajar con Windows constantemente estamos realizando modificaciones en su configuración, por ejemplo cambios en su aspecto como fondo del escritorio, combinación de colores, etc.

Además también podemos configurar las aplicaciones, su aspecto, últimos programas almacenados, etc. Y queremos que toda esta información de configuración permanezca cuando reiniciamos Windows o una aplicación. La cuestión es donde se almacenan todas estas características de personalización.

Características del Registro

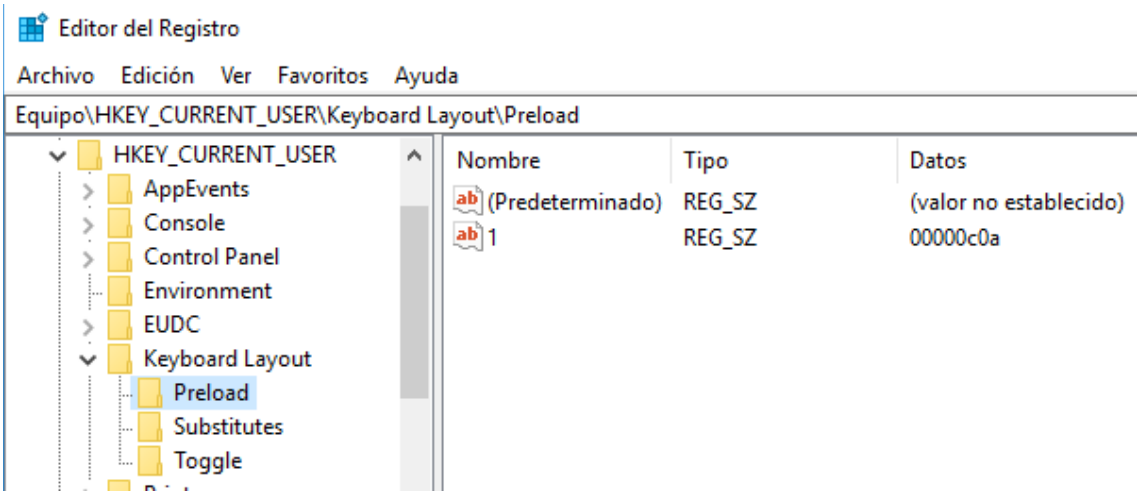
- **La información del Registro se organiza por categorías**, de forma que los parámetros que pertenecen a un usuario concreto (como fondo de escritorio) se guardan separadamente de los parámetros de otros usuarios o los propios parámetros internos del sistema. Cada parámetro se guarda como una pieza de información independiente.
- La información del Registro **se almacena en archivos binarios en disco**.
- Al igual que cualquier objeto del sistema, **cada elemento del Registro tiene un propietario**, una **ACL** y **controles de auditoria**.
- Con los permisos apropiados, los administradores o programas de una computadora pueden **conectarse, leer y modificar los registros de computadoras remotas**.

El Registro es una base de datos que contiene toda la información de configuración de Windows.
En él se incluye absolutamente todo, desde las opciones de pantalla hasta las contraseñas de usuario.

Estructura Lógica del Registro

Para examinar la información almacenada en el registro utilizamos el editor del registro **regedit**.

El Registro está organizado en una estructura jerárquica, compuesta por subárboles con sus respectivas claves, subclaves y entradas de valor.



Tipos de datos

El Editor del Registro puede soportar los siguientes tipos de datos:

Valor	**Tipo de datos**	**Descripción**
Cadena	REG_SZ	Cadena de texto Unicode de longitud fija.
Binario	REG_BINARY	Número de hasta 4 bytes de longitud.
DWord	REG_DWORD	Número de hasta 8 bytes de longitud.
QWord	REG_QWORD	Número de hasta 16 bytes de longitud.
Cadena Múltiple	REG_MULTI_SZ	Cadena de texto formada por múltiples subcadenas separadas por espacios, comas u otros caracteres especiales. Puede ser usada para presentar los valores de un cuadro de lista.
Cadena Expandible	REG_EXPAND_SZ	Cadena de datos de longitud variable. Suele contener información que pude cambiar en tiempo de ejecución., como variables de entorno.

Para borrar una entrada:

Seleccionar la entrada y pulsar **Supr** (**No existe una función Undo**, con lo que los cambios se almacenan directamente en el disco)

La información se almacena dividiéndola en cinco subárboles que se pueden observar en la fotografía obtenida con Regedit de la página anterior.

Nombre de la clave raíz	Abrev	Descripción	Enlace

HKEY_LOCAL_MACHINE	HKLM	Contiene información sobre el sistema del equipo local, incluyendo datos del **hardware**, **software** y del sistema operativo tales como el tipo de bus, la memoria del sistema, los controladores de dispositivo y datos de control de inicio. Incluyendo dispositivos que puede que no estén conectados en este momento.
		`set devmgr_show_nonpresent_devices=1`
		`start devmgmt.msc`	

HKEY_CLASSES_ROOT	HKCR	Contiene **asociaciones de archivos**. También contiene la base de datos del registro OLE, el antiguo REG.DAT de Win 3.x.	HKLM\Software\Classes
HKEY_CURRENT_USER	HKCU	Contiene el **perfil del usuario que ha iniciado la sesión** actual de modo interactivo (no remoto) e incluye las variables de entorno, la configuración del escritorio, las conexiones de red, las impresoras y las preferencias para los programas.	HKU\SID del usuario actual
HKEY_USERS	HKU	Contiene una entrada para cada usuario que haya iniciado una sesión previamente en la computadora. Se incluye información que también aparece en **HKEY_CURRENT_USER**. Los usuarios con acceso remoto al servidor no tienen perfiles en esta clave del servidor. Sus perfiles se cargan en el Registro de sus propios equipos.	
HKEY_CURRENT_CONFIG	HKCC	Contiene información para la **configuración de hardware del equipo local al iniciarse**. Esta información se usa para configurar opciones tales como los controladores de dispositivo y la resolución de pantalla que se va a utilizar.	HKLM\SYSTEM \CurrentControlSet \Hardware Profiles\ Current.

Para expandir todas las ramas bajo un nodo, tenemos que seleccionarlos y pulsar Alt + *

HKEY_CURRENT_USER

Contiene información del usuario actual que ha iniciado sesión localmente, examinemos sus principales ramas.

Subclave	**Descripción**
AppEvents	Asociaciones de Eventos/Sonidos
Console	Ajustes en la consola de comandos (alto, ancho, colores)
Control Panel	SalvaPantallas, escritorio, ajustes de teclado y ratón, accesibilidad y ajustes regionales
Environment	Variables de entorno definidas específicamente para este usuario
Keyboard Layout	Disposición del teclado
Network	Mapeado de unidades de red y ajustes
Printers	Impresoras conectadas
Software	Preferencias de software específicas de este usuario

HKEY_LOCAL_MACHINE

Subclave	**Descripción**
Hardware	Información sobre el hardware y los controladores de dispositivos.
SAM	Información sobre las cuentas de usuario y grupos locales, contraseñas.
Security	Información de seguridade
Software	Información del sistema que no es necesaria durante el arranque, aplicaciones.
System	Información necesaria para el arranque, que drivers cargar y que servicios arrancar.

Creando una copia de seguridad del Registro

Cada vez que arrancamos el ordenador, Windows automáticamente crea la información del registro basándose en el hardware y el software disponible. Después crea una copia de seguridad del registro.

NOTA: Antes de modificar el registro manualmente es aconsejable realizar una copia de seguridad, porque una vez hecho un cambio este no se puede deshacer.

La forma más fácil de realizar una copia de seguridad, es desde el propio editor de registro

Registro → Exportar archivo del registro→ Todo

Para restaurar el registro lo único que tenemos que hacer es importar el fichero que contiene la copia de seguridad.

Registro → Importar archivo del registro de configuraciones.

MODIFICAR EL REGISTRO SIN UTILIZAR EL EDITOR

Podemos emplear archivos .reg para importar información al registro. Para crearlos podemos exportar una clave desde Regedit o escribirlos directamente en texto ASCII.

- En la primera línea del fichero aparecerá la versión de REGEDIT con la que fue creado.
- La segunda línea debe estar en blanco.

Un ejemplo de fichero REG sería:

```
Windows Registry Editor Version 5.00
'Esto es un comentario
[HKEY_LOCAL_MACHINE\Sofware\MiPrograma]
[HKEY_LOCAL_MACHINE\Sofware\MiPrograma\Subclave]
```

- Si queremos cambiar el valor de las claves predeterminadas @=”Hola”
- Si queremos eliminar un valor `"Límite días"=-`

Estructura Física del Registro

El registro no está almacenado como un todo en el disco duro.

Sección del Registro	Ubicación	Archivo
HKEY_LOCAL_MACHINE\SAM	%Windir%/System32/Config	Sam
HKEY_LOCAL_MACHINE\SECURITY		Security
HKEY_LOCAL_MACHINE\SOFTWARE		Software
HKEY_LOCAL_MACHINE\SYSTEM		System
HKEY_USERS\.DEFAULT		Default
HKEY_CURENT_USER	%SystemDrive%:\Usuarios\%Username%	Ntuser.dat
HKEY_CURRENT_CONFIG	Volatil	

Modificaciones en el registro con la aparición de versiones de 64 bits de Windows.

Cuando se ejecutan programas en una versión de Windows de 64 bits, almacenan su configuración en lugares diferentes dependiendo si son de 32 o 64 bits.

- Los de 32 bits
  HKEY_LOCAL_MACHINE\Software\WOW6432node
- Los de 64 bis
  HKEY_LOCAL_MACHINE\Software

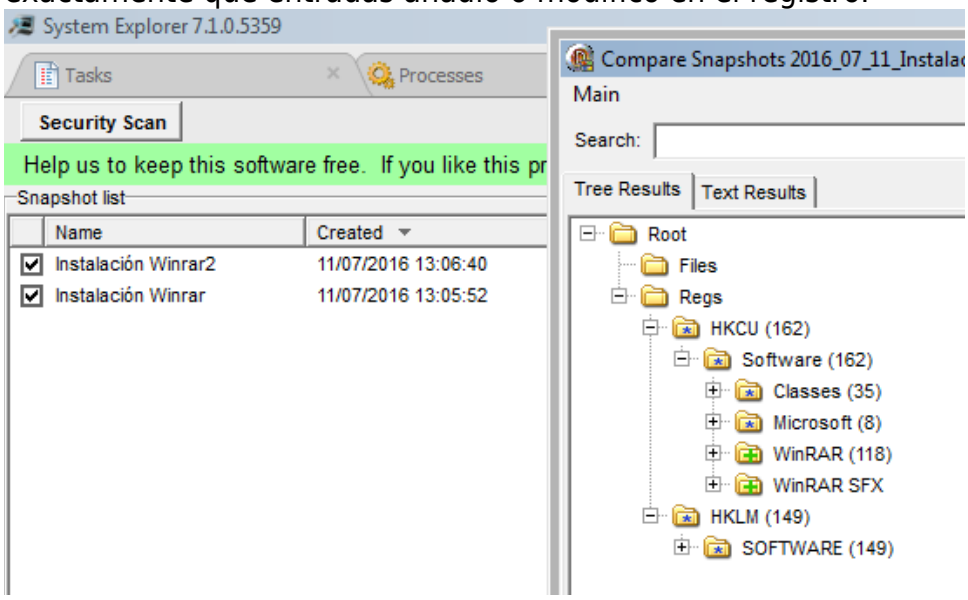
Por lo que otro posible foco de infección de nuestro sistema serían

- HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

Utilidades Para Manejar el Registro

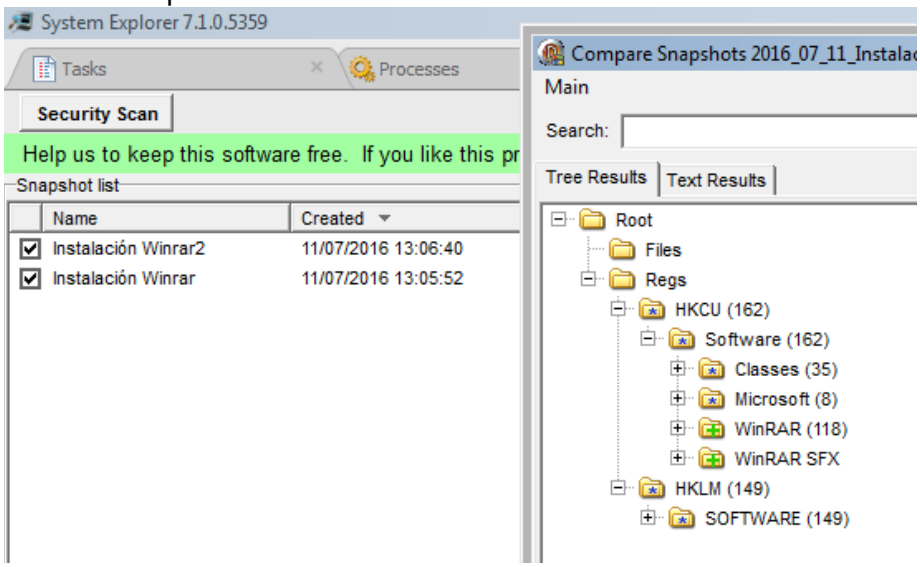
System Explorer

Este programa es muy útil ya que nos permite examinar todo lo que ocurre en nuestro sistema (procesos, conexiones de red..) para detectar posibles problemas de rendimiento, virus..
Pero lo que aquí nos interesa es que nos permite realizar instantáneas (snapshots) del registro antes y después de instalar un programa para saber exactamente que entradas añadió o modificó en el registro.



Para ello:

- Añadimos la pestaña snapshots
- Hacemos una instantánea
- Instalamos un programa
- Hacemos otra instantánea
- Comparamos

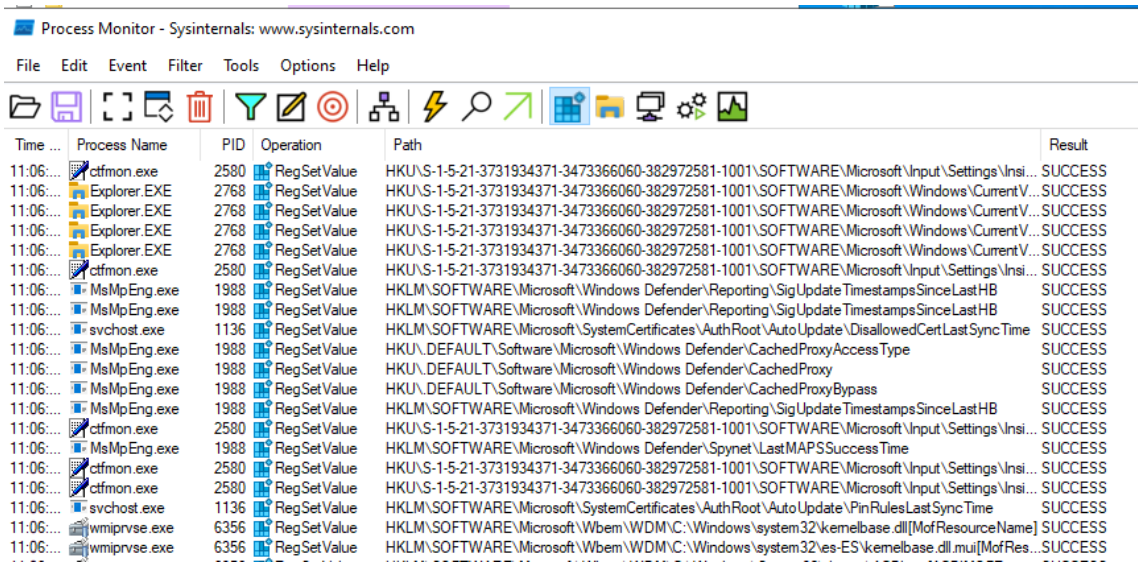


ProcessMonitor

Esta aplicación monitorizar lo que ocurre en nuestro equipo en tiempo real. No solo monitoriza los accesos al registro, sino también al sistema de archivos, y los procesos del sistema. Es una herramienta muy potente pero para utilizarla necesitamos privilegios de administrador.

Podemos emplearla para monitorizar la actividad que se produce en el registro en tiempo real. Para cada acceso a una entrada del registro. Regmon nos muestra que proceso realizó el acceso, la hora, tipo y resultado del acceso.

Esto nos permite saber en que claves almacenan las aplicaciones su información, y en caso de que una aplicación falle podemos rastrear los accesos de esa aplicación para saber si el fallo está relacionado con un acceso al registro.



Time ...	Process Name	PID	Operation	Path	Result
11:06:...	ctfmon.exe	2580	RegSetValue	HKU\S-1-5-21-3731934371-3473366060-382972581-1001\SOFTWARE\Microsoft\Input\Settings\Insi...	SUCCESS
11:06:...	Explorer.EXE	2768	RegSetValue	HKU\S-1-5-21-3731934371-3473366060-382972581-1001\SOFTWARE\Microsoft\Windows\CurrentV...	SUCCESS
11:06:...	Explorer.EXE	2768	RegSetValue	HKU\S-1-5-21-3731934371-3473366060-382972581-1001\SOFTWARE\Microsoft\Windows\CurrentV...	SUCCESS
11:06:...	Explorer.EXE	2768	RegSetValue	HKU\S-1-5-21-3731934371-3473366060-382972581-1001\SOFTWARE\Microsoft\Windows\CurrentV...	SUCCESS
11:06:...	Explorer.EXE	2768	RegSetValue	HKU\S-1-5-21-3731934371-3473366060-382972581-1001\SOFTWARE\Microsoft\Windows\CurrentV...	SUCCESS
11:06:...	ctfmon.exe	2580	RegSetValue	HKU\S-1-5-21-3731934371-3473366060-382972581-1001\SOFTWARE\Microsoft\Input\Settings\Insi...	SUCCESS
11:06:...	MsMpEng.exe	1988	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows Defender\Reporting\SigUpdateTimestampsSinceLastHB	SUCCESS
11:06:...	MsMpEng.exe	1988	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows Defender\Reporting\SigUpdateTimestampsSinceLastHB	SUCCESS
11:06:...	svchost.exe	1136	RegSetValue	HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\AutoUpdate\DisallowedCertLastSyncTime	SUCCESS
11:06:...	MsMpEng.exe	1988	RegSetValue	HKU\.DEFAULT\Software\Microsoft\Windows Defender\CachedProxyAccessType	SUCCESS
11:06:...	MsMpEng.exe	1988	RegSetValue	HKU\.DEFAULT\Software\Microsoft\Windows Defender\CachedProxy	SUCCESS
11:06:...	MsMpEng.exe	1988	RegSetValue	HKU\.DEFAULT\Software\Microsoft\Windows Defender\CachedProxyBypass	SUCCESS
11:06:...	MsMpEng.exe	1988	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows Defender\Reporting\SigUpdateTimestampsSinceLastHB	SUCCESS
11:06:...	ctfmon.exe	2580	RegSetValue	HKU\S-1-5-21-3731934371-3473366060-382972581-1001\SOFTWARE\Microsoft\Input\Settings\Insi...	SUCCESS
11:06:...	MsMpEng.exe	1988	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows Defender\Spynet\LastMAPSSuccessTime	SUCCESS
11:06:...	ctfmon.exe	2580	RegSetValue	HKU\S-1-5-21-3731934371-3473366060-382972581-1001\SOFTWARE\Microsoft\Input\Settings\Insi...	SUCCESS
11:06:...	ctfmon.exe	2580	RegSetValue	HKU\S-1-5-21-3731934371-3473366060-382972581-1001\SOFTWARE\Microsoft\Input\Settings\Insi...	SUCCESS
11:06:...	svchost.exe	1136	RegSetValue	HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\AutoUpdate\PinRulesLastSyncTime	SUCCESS
11:06:...	wmiprvse.exe	6356	RegSetValue	HKLM\SOFTWARE\Microsoft\Wbem\WDM\C:\Windows\system32\kernelbase.dll[MofResourceName]	SUCCESS
11:06:...	wmiprvse.exe	6356	RegSetValue	HKLM\SOFTWARE\Microsoft\Wbem\WDM\C:\Windows\system32\es-ES\kernelbase.dll.mui[MofRes...	SUCCESS

Manejar el Registro desde DOS

Regedit posee unos parámetros

- **Regedit /s** nombre_archivo.reg: importa el archivo reg sin pedir confirmación.
- **Regedit /e** nombre_archivo.reg: exporta la rama especificada en modo nativo; si no se especifica nada, se exporta toda la información del registro. Útil para hacer una copia de seguridad de todo el registro.
- **Regedit /a** nombre_archivo.reg, exporta la rama especificada en formato regedit4 (utilizado por Win9x).

Pero la forma mas potente es utilizar el comando reg

- **Reg query** : consulta una clave específica del registro
  - reg query clave /v variable → devuelve el valor de esa variable
  - reg query hklm\Software\Mozilla\Mozilla /v CurrentVersion → Devuelve el valor de la variable CurrentVersion dentro de esa ruta
  - reg query \\172.20.4.2\hklm\Software\Mozilla\Mozilla /v CurrentVersion → Hace lo mismo en ese equipo de red. Si tenemos los permisos adecuados

```
! REG.EXE VERSION 3.0

HKEY_LOCAL_MACHINE\Software\Mozilla\Mozilla
    CurrentVersion      REG_SZ  1.7.5
```

- **Reg export** : (idéntico al comando “regedit /e”) exporta la configuración del registro o de la ramas especificadas.
- **Reg import**: Incorpora la información incluida en un fichero.reg al registro.
- **Reg add** : agrega una clave específica al registro
- **Reg delete** : borra una clave específica del registro
- **Reg copy:** Copia todos las claves y valores de una rama a otra.
- **Reg compare**: Compara las diferencias entre claves de distintas ramas o equipos