El registro de Windows

Breve introducción al registro de Windows

El registro de Windows no es mas que una base de datos jerárquica donde se almacenan todos los detalles relativos a la configuración del sistema operativo. Está compuesto por los siguientes elementos:

- Subárboles:
  Raices o divisiones principales de que se compone estructuralmente el registro.

- Claves:
  Principales contenedores ubicados dentro de cada subárbol. Pueden contener subclaves o entradas.

- Entradas:
  Datos reales cuyo valor afecta al sistema. Si abrimos el editor del registro se corresponderían con los elementos que aparecen en el panel derecho.

Físicamente el registro se guarda en ficheros separados, almacenando cada uno de ellos una sección en particular. A su vez cada uno de estos ficheros tendría su .log equivalente, los cuales actúan como ficheros de transacciones.

Cuando se modifica alguna de las secciones que componen el registro de Windows los cambios se escribirían en primer lugar como registros en el archivo .log actualizándose después el fichero correspondiente a la sección en particular desde los datos escritos en el disco.

Los ficheros y sus secciones equivalentes serían los siguientes:

Nombre de la clave	Ruta absoluta del fichero
HKEY_LOCAL_MACHINE\SAM	%SystemRoot%\system32\config\SAM
HKEY_LOCAL_MACHINE\Security	%SystemRoot%\system32\config\Security
HKEY_LOCAL_MACHINE\Software	%SystemRoot%\system32\config\Software
HKEY_LOCAL_MACHINE\System	%SystemRoot%\system32\config\System
HKEY_USERS\[User SID]	%SystemDrive%\Documents and Settings\ [username]\NTUser.dat
HKEY_USERS\Default	%SystemRoot%\system32\config\default

Las entradas definidas anteriormente, y las cuales aparecerían en el panel derecho del editor del registro, estan formadas por 2 elementos:

- Nombre del valor

- Tipo de dato del valor:
  El cual puede ser uno de los siguientes, mencionándose a continuación únicamente los más comunes:

    - REG_DWORD
      Una doble palabra (2 palabras de 16 bits = 32 bits = 4 bytes). Las entradas se visualizan

en formato hexadecimal. Utilizado para la mayoría de información sobre controladores de dispositivos y servicios.

- REG_BINARY
  Entradas con datos binarios sin formato. Se utiliza principalmente para almacenar información de componentes de hardware.

- REG_SZ
  Cadenas de texto de longitud fija. La mayor parte de entradas se corresponden a datos booleanos o tienen valores de cadena de texto corto. La notacion sz (String/Zero) es debido a que las entradas se terminan con un byte cero al final. Regedit ocultaría el 0 de la terminación de los datos.

- REG_MULTI_SZ
  Cadena múltiple Utilizado para almacenar listas o valores múltiples. Los valores están separadas por comas o espacios y la entrada está terminada por dos caracteres nulos (ocultados por Regedit).

- REG_EXPAND_SZ
  Cadena de datos de longitud variable. Este tipo de datos incluye variables que se resuelven cuando un programa o servicio utiliza los datos.

- REG_FULL_RESOURCE_DESCRIPTOR
  Utilizada para almacenar una lista de recursos para componentes de hardware, por loq estaría compuesto por series de matrices anidadas.

- REG_LINK
  Contiene un vínculo simbólico entre los datos y un valor del registro determinado.

HKEY_CLASSES_ROOT

Se trata de una subclave de HKEY_LOCAL_MACHINE\Software. En este subárbol existen dos tipos de datos:

- Información de asociación de archivos.
- Datos de configuración para objetos COM.

Esta sección es en realidad un alias y deriva sus datos desde dos orígenes:

HKEY_LOCAL_MACHINE\Software\Classes
HKEY_LOCAL_MACHINE\Software\Classes

De esta forma se permite el registro de clases por usuario. Esta funcionalidad implica que los equipos con usuarios múltiples pueden poseer diferente información para las clases registradas cuando un usuario específico instala el software.

HKEY_CURRENT_USER

Contiene la información de configuración para el usuario que tiene iniciada una sesión actualmente en el sistema. Contiene valores que afectan al sistema operativo, las aplicaciones y las directivas. Dichos valores estan contenidos en el archivo NTUser.dat almacenado en %SystemDrive %\Documents and Settings\[username].

HKEY_LOCAL_MACHINE

Contiene información acerca del equipo, su hardware, los controladores de dispositivos y las opciones de configuración (tanto de seguridad como del software instalado) que afectan a todos los usuarios del sistema.

Contiene a su vez las siguientes secciones:

- HKLM\Hardware
  Ntdetect.com crea el contenido durante el inicio del sistema, manteniendose dicha información en la memoria RAM.

- HKLM\SAM
  Datos utilizados por el administrador de cuentas de seguridad no accesibles mediante el editor del registro. Se trata de un repositorio de datos de usuarios y grupos, incluyendo los permisos de acceso para las carpetas, archivos y perifericos.

- HKLM\Security
  Relacionado con los temas de seguridad y que contiene datos que dependen del tipo de red (modo nativo u modo híbrido).

- HKLM\Software
  Opciones de configuración relativas al software instalado y del sistema operativo.

- HKLM\System
  Datos que controlan el proceso de inicio de sesión del sistema operativo, servicios del kernel, etc.

HKEY_USERS

Contiene todos los perfiles de usuario que han iniciado sesión en algún momento en el equipo. Cada subclave de perfil se identifica con un ID de seguridad.

HKEY_CURRENT_CONFIG

Contiene información acerca del perfil de hardware utilizado por el equipo durante el inicio del sistema. Es un alias de HKLM\System\CurrentControlSet\Hardware\Profiles\Current.

Análisis del registro de Windows

Presentación de las herramientas

A lo largo de toda esta sección vamos a utilizar de forma intensiva 2 utilidades gráficas que nos permitirán abrir e interpretar los ficheros que componen las diferentes secciones del registro. Ambas son gratuitas y pertenecen a MiTeC. Son las siguientes:

- Windows Registry Recovery[1]
- Windows Registry File Viewer[2]

1 http://www.snapfiles.com/get/rfv.html
2 http://www.mitec.cz/wrr.html

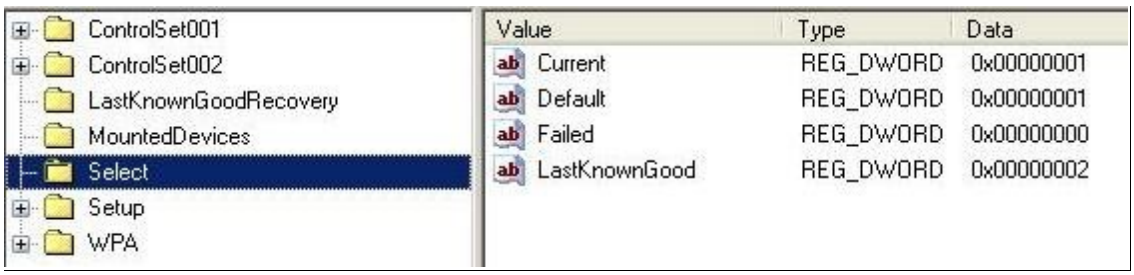
Las dos nos permitirán analizar el registro con una interfaz similar a la aplicación Regedit incluida de serie con todos los sistemas Windows, pero además, y de forma automatizada, interpretarán los datos en crudo de determinadas claves para facilitarnos la obtención de información.

Para todos aquellos casos en los que no se defina un procedimiento especial para la interpretación de la información utilizaremos la herramienta "Registry File Viewer". El proceso será similar en todos los casos y consistirá en abrir el fichero correspondiente a la sección concreta del registro que estemos tratando y navegar hasta la clave mencionada para ver la información adecuada.

Nota acerca de CurrentControlSet

Cuando realizamos un análisis offline del registro, y concretamente de la sección contenida en el fichero system, observaremos que pueden llegar a existir hasta 4 entradas diferentes con la siguiente nomenclatura: ControlSet00x. Lo normal será encontrarnos únicamente dos entradas, donde x sería sustituido por números enteros consecutivos (1 y 2 habitualmente).

De las dos entradas solo una será la utilizada por el sistema operativo para obtener los valores de configuración para el arranque, es decir, como la entrada CurrentControlSet. Para determinar cual de ellas es la utilizada accederemos a los valores almacenados en HKLM\System\Select:



Los valores Current y Default se corresponden con el valor en hexadecimal del ControlSet utilizado (1 para nuestro ejemplo) y el valor de LastKnownGood se correspondería con el ControlSet cargado cuando el sistema no es capaz de iniciarse correctamente y nos aparece la opción de "Iniciar el sistema utilizando la última configuración buena conocida" (2 en nuestro ejemplo).

Obteniendo información general del sistema

<u>Sección system</u>

1. Nombre de máquina:
   HKLM\System\CurrentControlSet\Control\ComputerName\ComputerName

2. Fecha de último apagado del sistema:
   HKLM\System\CurrentControlSet\Control\Windows\ShutdownTime

   Para interpretar la información binaria almacenada en esta entrada utilizaremos la aplicación Decode Date[3] tal y como se muestra en la siguiente captura.

3. Información de la zona horaria:
   HKLM\System\CurrentControlSet\Control\TimeZoneInformation\ActiveTimeBias

   Valor indicado en minutos que contiene la configuración de la zona horaria del sistema. Podremos utilizar dicho valor para normalizar los registros de tiempo obtenidos de otras fuentes en formato UTC/GMT.

4. Servicios instalados en el sistema
   HKLM\System\CurrentControlSet\Services

   Si el valor de la entrada Start está establecido a 0x0000002 el servicio se iniciará de forma automática con el arranque del sistema.

   Para obtener el listado de forma sencilla utilizaremos la aplicación “Windows Registry Recovery”. Abriremos el fichero system contenido en la imagen del sistema y pulsaremos sobre el botón “Services and Drivers” del apartado “Explorer Tasks”.

5. Configuración TCP/IP:
   HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces

   Para obtener los datos de forma sencilla utilizaremos la aplicación “Windows Registry Recovery”. Abriremos el fichero system contenido en la imagen del sistema y pulsaremos sobre el botón “Network Configuration” del apartado “Explorer Tasks”.

Sección software

1. Dueño del software:
   HKLM\Software\Microsoft\Windows NT\CurrentVersion\RegisteredOwner

2. Organización:
   HKLM\Software\Microsoft\Windows NT\CurrentVersion\RegisteredOrganization

3. Sistema operativo:
   HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProductName

3 http://www.digital-detective.co.uk/freetools/decode.asp

4. Version:
   HKLM\Software\Microsoft\Windows NT\CurrentVersion\CurrentBuildNumber

5. Service Pack instalado:
   HKLM\Software\Microsoft\Windows NT\CurrentVersion\CSDVersion

6. Fecha de instalación del sistema:
   HKLM\Software\Microsoft\Windows NT\CurrentVersion\InstallDate

7. ID de producto:
   HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProductId

8. Software instalado en el sistema:
   HKLM\Software

9. Parches instalados en el sistema:
   HKLM\Software\Microsoft\Updates\Windows Server 2003\SP2

Para obtener de forma simple todos los datos anteriores utilizaremos la aplicación "Windows Registry Recovery". Abriremos el fichero software contenido en la imagen del sistema y pulsaremos sobre el botón "Windows Installation" del apartado "Explorer Tasks". Como resultado obtendremos toda la información anterior de forma visual en las pestañas "General", "Installed Software" y "Hot Fixes".

Listando aplicaciones que se inician de forma automática

Las siguientes son las ubicaciones más comunes para la instalación de virus, troyanos y demás tipos de malware. Para más información consultar el documento Registry Reference (nota al pié con el enlace) de Harlan Carvey.

HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler

Dispositivos USB extraibles

Al conectar un dispositivo USB al sistema (p.e. un pendrive) se almacena en el registro su huella digital. Cuando el administrador Plug-and-Play carga el driver adecuado (registrado en el fichero setupapi.log) y el dispositivo ha sido identificado se genera una entrada conocida como "Device Class ID" en:

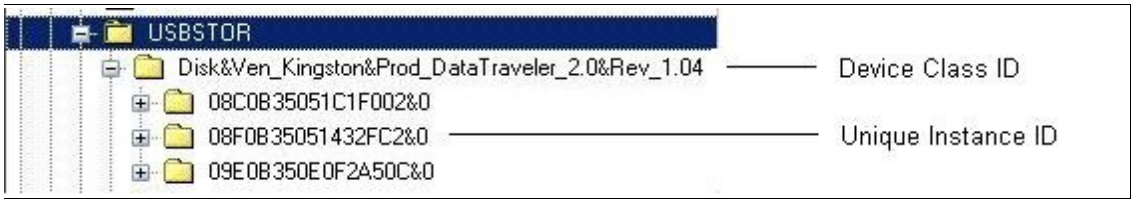
HKLM\System\CurrentControlSet\Enum\USBSTOR

con un formato similar al siguiente:

Disk&Ven_xxx&Prod_xxx&Rev_xxx

donde xxx sería rellenado por PnP en función de las características del dispositivo.

Una vez creado el “Device Class ID” se agregará una entrada unívoca, “Unique Instance ID”, para cada dispositivo similar basándose en el valor iSerialNumber integrado en el propio hardware.



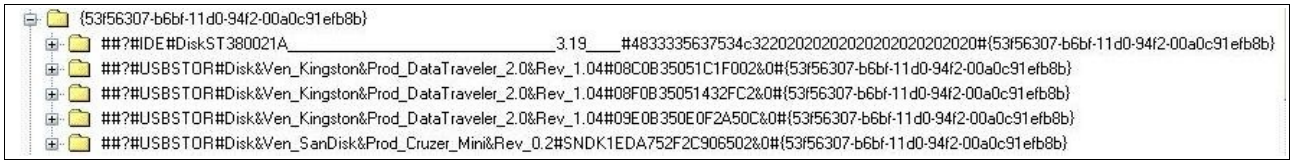
En el caso de que el dispositivo no incluya un valor de iSerialNumber este le será asignado de forma automática por Windows de forma que sea único.

Un valor interesante que podemos encontrar dentro de cada entrada “Unique Instance ID” sería el de “ParentIdPrefix, el cual nos permitirá determinar la fecha en que se conectó por última vez el dispositivo USB concreto al sistema. Para correlacionar dicho valor desplegaremos la clave:

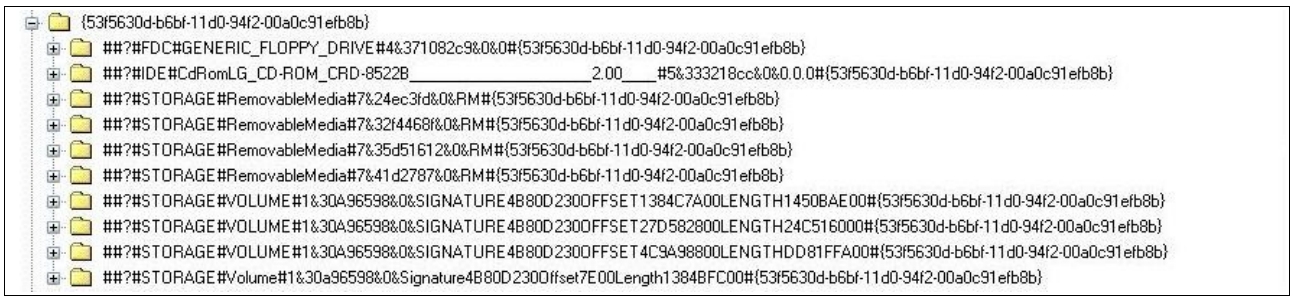
HKLM\System\CurrentControlSet\Control\DeviceClasses

En su interior apreciaremos la existencia de las siguientes subclaves:

{53f56307-b6bf-11d0-94f2-00a0c91efb8b} → GUID del interfaz de disco
Contenida en ella encontraremos entradas para cada dispositivo conectado. Para identificarlo usaremos el valor de “Unique Instance ID” asociado a cada dispositivo e indicado entre paréntesis.

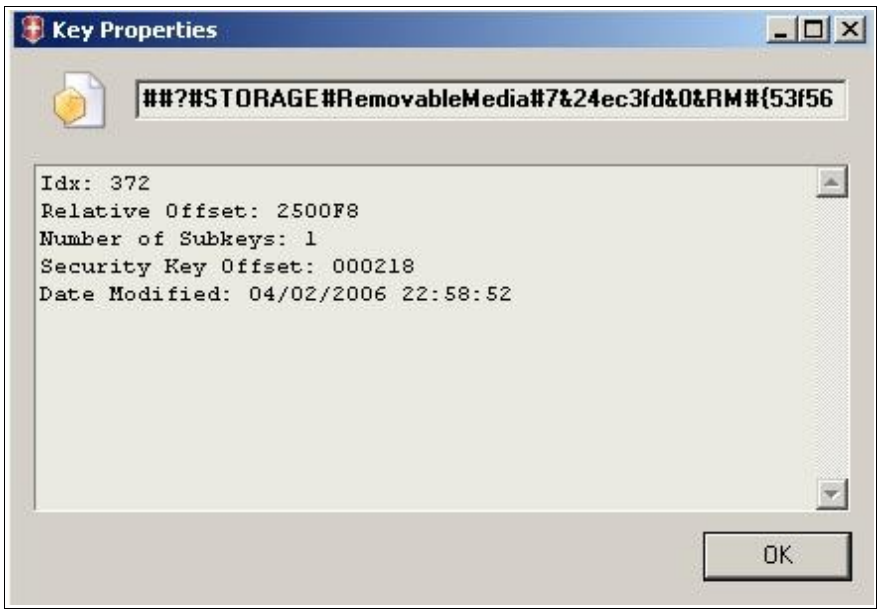


{53f5630d-b6bf-11d0-94f2-00a0c91efb8b} → GUID del interfaz de volumen
Contenida en ella encontraremos entradas para cada dispositivo conectado. Para identificarlo usaremos el valor de “ParentIdPrefix” asociado a cada dispositivo.



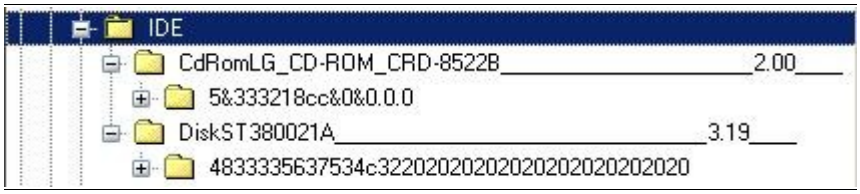
La fecha de última modificación para las entradas correspondientes a cada dispositivo nos permitirán obtener la fecha de la última ocasión en que el dispositivo USB fué conectado al sistema.

Para obtener el valor de fecha ejecutaremos la herramienta “Windows Registry Recovery” y abriremos el fichero system contenido en la imagen del sistema. Una vez abierto pulsaremos el botón “Raw Data” del apartado “Explorer Tasks” y navegaremos hasta la clave adecuada. Una vez seleccionada pulsaremos con el botón derecho del ratón → “Properties...”.

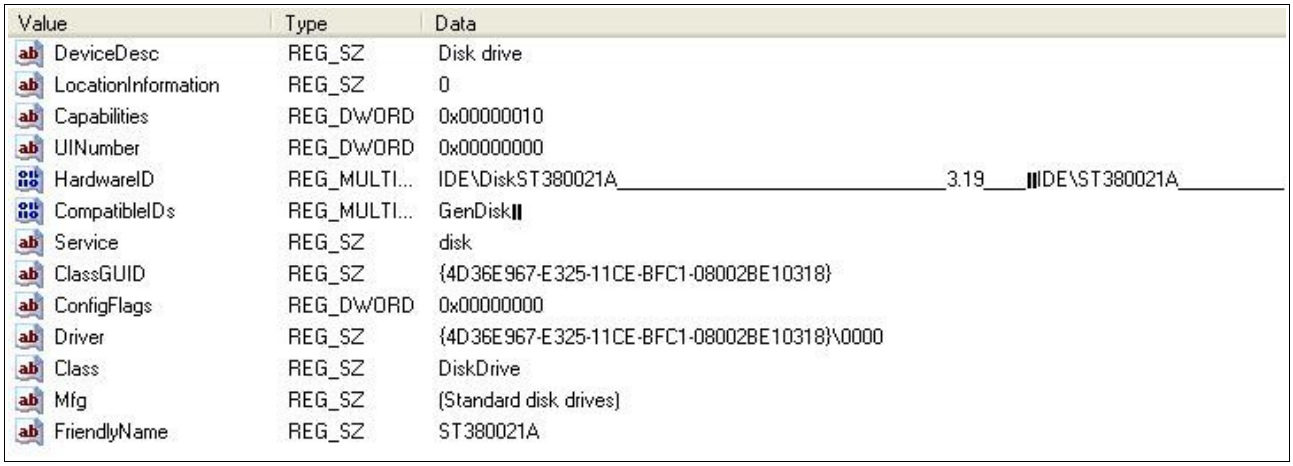


Dispositivos IDE conectados al sistema

La clave del registro HKLM\system\CurrentControlSet\Enum\IDE contiene a su vez diferentes subclaves que se corresponden con los dispositivos IDE que existen en el sistema analizado, cada una con su "Unique Instance ID" correspondiente.



A su vez cada subclave tiene asociada una entrada de nombre UINumber cuyo valor, si es distinto de 0, nos permitirá saber si el sistema Windows se instaló en una máquina junto con otros sistemas operativos.



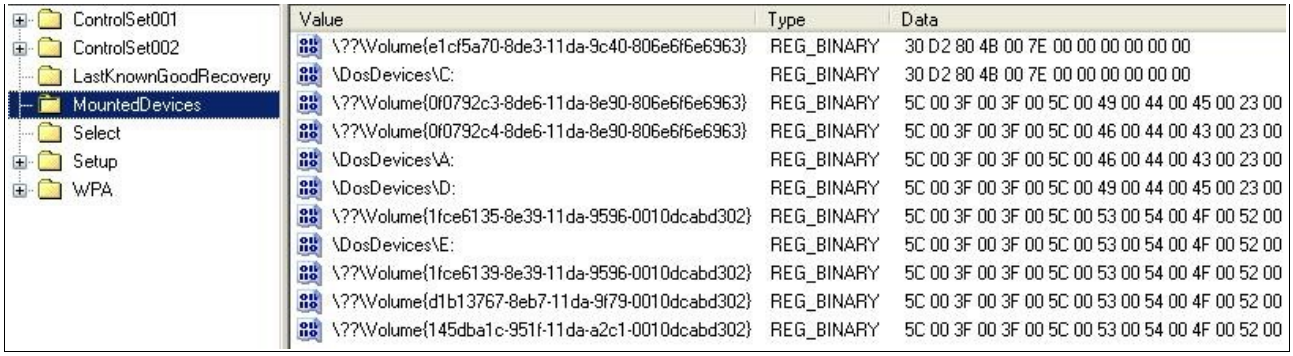
Value	Type	Data
DeviceDesc	REG_SZ	Disk drive
LocationInformation	REG_SZ	0
Capabilities	REG_DWORD	0x00000010
UINumber	REG_DWORD	0x00000000
HardwareID	REG_MULTI...	IDE\DiskST380021A_____3.19____IDE\ST380021A_____
CompatibleIDs	REG_MULTI...	GenDisk
Service	REG_SZ	disk
ClassGUID	REG_SZ	{4D36E967-E325-11CE-BFC1-08002BE10318}
ConfigFlags	REG_DWORD	0x00000000
Driver	REG_SZ	{4D36E967-E325-11CE-BFC1-08002BE10318}\0000
Class	REG_SZ	DiskDrive
Mfg	REG_SZ	(Standard disk drives)
FriendlyName	REG_SZ	ST380021A

Dispositivos montados en el sistema

La información relativa a los diferentes dispositivos y volúmenes montados en el sistema de

ficheros NTFS podremos encontrarla en la siguiente clave del registro:

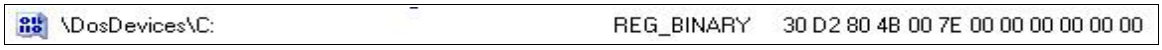
HKLM\system\MountedDevices



Cada una de las entradas incluidas en esta clave y con formato \DosDevices\X: se corresponderá con un dispositivo instalado en el sistema y deberemos sustituir X: por el nombre de la unidad que utiliza el sistema para acceder a él.

Unidades de disco y particiones

Aquellas entradas cuyos datos ocupen únicamente 12 bytes (3 DWORDS) se corresponderán con dispositivos o unidades de disco:

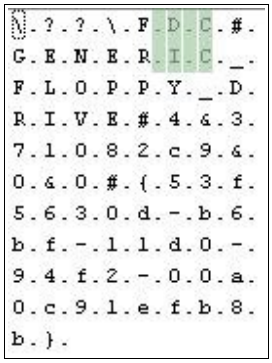


- El primer DWORD (30 D2 80 4B) se corresponde con la firma digital del disco duro, por lo que si encontraramos otra entrada cuyo primer DWORD fuera similar se trataría de una nueva partición del mismo disco duro.

- El segundo y tercer DWORD (00 7E 00 00 00 00 00 00) se corresponden con el offset en que comienza la partición. En nuestro caso 0x7E00 sería igual a 32.256 en decimal. Sabiendo que cada sector tiene un tamaño de 512 bytes la partición C: comenzaría en el sector 63.

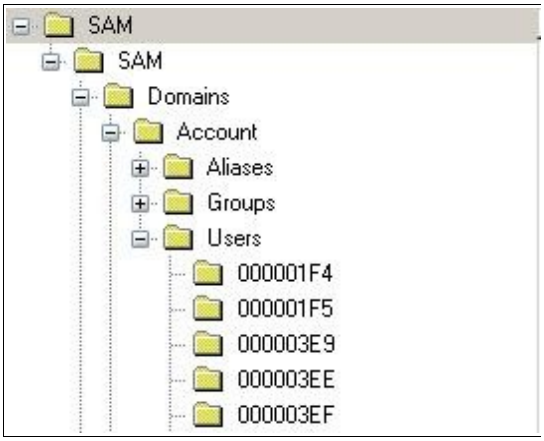
Otros dispositivos

Si analizamos los valores para las entradas \DosDevices\A: y \DosDevices\D: obtendremos información sobre el tipo de dispositivos de que se tratan.



Dispositivos USB extraibles

Utilizando el ParentIdPrefix asignado a cada dispositivo USB en la clave USBSTOR podemos identificar el dispositivo concreto que se conectó por última vez al sistema. Para ello analizaremos el valor REG_BINARY correspondiente a la entrada \DosDevice\E: de nuestro ejemplo.



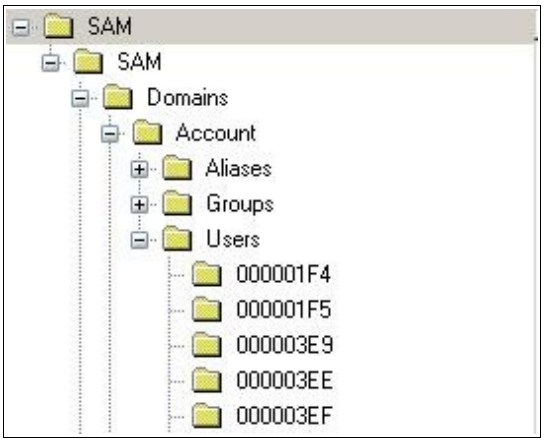
Obteniendo información de los usuarios y grupos del sistema

Usuarios

La información relativa a los diferentes usuarios que existen en el sistema Windows podemos hallarla en la siguiente clave del registro:

HKLM\SAM\Domains\Account\Users

Allí podremos encontrar diversas subclaves cuyo nombre consiste en un valor hexadecimal que, trasladado a su correspondiente valor en decimal, identifica el RID (enlace al documento de las contraseñas en windows) de los diferentes usuarios del sistema.



Para nuestro ejemplo el valor 1F4 hexadecimal se correspondería con el 500 en decimal (usuario Administrador), el valor 1F5 hex sería igual al 501 dec (usuario Invitado), etc.

La entrada de nombre F que existe en la clave correspondiente al RID del usuario contiene la siguiente información:

- La fecha de último inicio de sesión.
- La fecha en que se cambió la contraseña por última vez o la fecha de creación para la cuenta si la contraseña no ha sido cambiada o reseteada desde entonces.
- La fecha de expiración para la cuenta.
- La fecha del último inicio de sesión fallido.

Por otra parte, la entrada de nombre V nos proporcionaría los siguientes datos relativos a la cuenta de usuario:

- Nombre completo del usuario al que pertenece la cuenta.
- Comentario.
- Ruta del script de logon.
- Hashes de la contraseña.

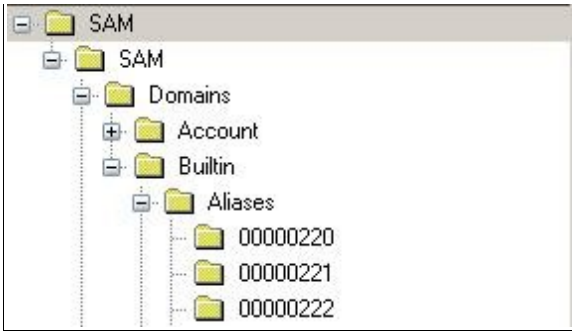
Para obtener de forma simple todos los datos anteriores utilizaremos la aplicación "Windows Registry Recovery". Abriremos el fichero SAM contenido en la imagen del sistema y pulsaremos sobre el botón "SAM" del apartado "Explorer Tasks". Como resultado obtendremos toda la información anterior de forma visual en las pestañas "General" y "Groups and Users".

El único dato que no nos mostrará el proceso anterior serán los hashes de las contraseñas de los usuarios. Para obtener dichos valores utilizaremos la información complementaria obtenida mediante la aplicación "Registry File Viewer". Abriremos el fichero SAM con dicha aplicación y en este caso accederemos al menú "Tools" → "Spy & Analyze" → "SAM". Se generará un panel inferior de Resultados donde obtendremos para cada entrada correspondiente a los diferentes usuarios los hashes de las contraseñas almacenadas en el registro, además de la mayor parte de información mostrada de forma gráfica en la aplicación "Windows Registry Recovery".

Grupos

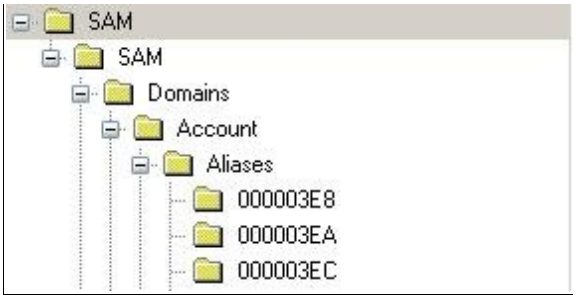
La información relativa a los diferentes grupos preincorporados que existen en el sistema Windows podremos hallarla en la siguiente clave del registro:

HKLM\SAM\Domains\Builtin\Aliases



Por otra parte, la información relativa a los nuevos grupos creados en el sistema Windows la encontraremos en:

HKLM\SAM\Domains\Account\Aliases



En ambos casos, y al igual que sucedía para las cuentas de usuarios, dentro de ambas claves encontraremos diferentes subclaves cuyo nombre consiste en un valor hexadecimal que, trasladado a su correspondiente valor en decimal, identifica el RID (enlace al documento de las contraseñas en windows) de los diferentes grupos del sistema.

La entrada de nombre C que existe en la clave correspondiente al RID del grupo contiene la siguiente información:

- Nombre del grupo
- Descripción
- Lista de usuarios que pertenecen a dicho grupo

Para obtener de forma simple la lista de todos los grupos definidos en el sistema utilizaremos la aplicación “Windows Registry Recovery”. Abriremos el fichero SAM contenido en la imagen del sistema y pulsaremos sobre el botón “SAM” del apartado “Explorer Tasks”, hallando la informacuón deseada en la pestaña “Groups and Users”.

El proceso de obtención de la lista de usuarios pertenecientes a cada grupo resultará algo más “trabajoso”, pero no imposible, gracias al trabajo de Andreas Schuster (incluir al pie enlace al documento de su blog).

En primer lugar instalaremos el editor hexadecimal 010[4], una herramienta comercial pero que será totalmente funcional durante un periodo de prueba de 30 días. Una vez instalado descargaremos las plantillas para dicho editor creadas por Andreas Schuster[5], las cuales extraeremos en la carpeta “Templates” del directorio de instalación de 010 (C:\Archivos de programa\010Editor, por defecto).

A continuación utilizaremos la aplicación “Registry File Viewer” para abrir el fichero SAM contenido en la imagen del sistema. Una vez abierto nos desplazaremos hasta la siguiente clave:

SAM\ Domains\Builtin\Aliases\00000220

Haciendo doble click con el ratón sobre la entrada C accederemos a la ventana de vista de datos donde deberemos pulsar sobre el botón “Save data...” y elegir un nombre y una ubicación para el fichero conteniendo el volcado hexadecimal con los datos correspondientes a dicha entrada.

Seguidamente abriremos el fichero anterior con el editor 010 y seleccionaremos el menú “Templates” → “Open Template...”. Elegiremos la plantilla “SAM_Group_c.bt” y pulsaremos el botón Abrir. Desplegaremos nuevamente el menú “Templates” seleccionando la opción “Run Template”. Como resultado obtendremos un nuevo panel con la información que buscábamos .

4 http://www.sweetscape.com/010editor/
5 http://computer.forensikblog.de/files/010_templates/SAM_Group_c.zip

Template Results - SAM_Group_c.bt

Name	Value	Start	Size	Color
uint32 GroupID	544	0h	4h	Fg: Bg:
uint32 OfsSD	0	4h	4h	Fg: Bg:
uint32 LenSD	152	8h	4h	Fg: Bg:
uint32 OfsName	152	10h	4h	Fg: Bg:
uint32 LenName	28	14h	4h	Fg: Bg:
uint32 OfsDesc	180	1Ch	4h	Fg: Bg:
uint32 LenDesc	150	20h	4h	Fg: Bg:
uint32 OfsMember	332	28h	4h	Fg: Bg:
uint32 LenMember	140	2Ch	4h	Fg: Bg:
uint32 CntMember	5	30h	4h	Fg: Bg:
struct SD_t SD		34h	98h	Fg: Bg:
struct strName16 Name	Administrators	CCh	1Ch	Fg: Bg:
struct strDesc16 Desc	Administrators have complete and unrestricted access to th	E8h	96h	Fg: Bg:
struct SID_t Member[0]	S-1-5-21-2780117151-1340924567-2512508698-500	180h	1Ch	Fg: Bg:
struct SID_t Member[1]	S-1-5-21-2780117151-1340924567-2512508698-1006	19Ch	1Ch	Fg: Bg:
struct SID_t Member[2]	S-1-5-21-2780117151-1340924567-2512508698-1007	1B8h	1Ch	Fg: Bg:
struct SID_t Member[3]	S-1-5-21-2780117151-1340924567-2512508698-1012	1D4h	1Ch	Fg: Bg:
struct SID_t Member[4]	S-1-5-21-2780117151-1340924567-2512508698-1024	1F0h	1Ch	Fg: Bg:

Deberemos repetir el proceso para cada uno de los grupos definidos en el sistema y del que deseemos obtener la lista de usuarios que lo componen.

Información sobre la actividad de los usuarios: UserAssist

La clave UserAssit contiene valiosa información que nos ayudará a desvelar gran parte de las acciones realizadas por un usuario en el sistema. Dicha clave es particular para cada cuenta por lo que para encontrar la información allí almacenada deberemos abrir el fichero NTUSER.DAT de cada usuario en particular y navegar hasta la siguiente ubicación:

Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

En su interior encontraremos dos subclaves Count diferentes contenidas cada una de ellas a su vez en dos valores numéricos para diferentes GUID:

- {5E6AB780-7743-11CF-A12B-00AA004AE837}
  Apunta a la barra de herramientas de Internet Explorer (Internet Toolbar), localizada en %SystemRoot%\system32\browseui.dll

- {75048700-EF1F-11D0-9888-006097DEACF9 }
  Apunta a Active Desktop, ubicado en %SystemRoot%\system32\SHELL32.DLL

Dentro de cada una de las subclaves encontraremos muchas entradas, todas ellas cifradas utilizando el algoritmo Rot-13. Al descifrar los nombres de cada uno de los valores encontraremos etiquetas como las siguientes:

- UEME_RUNPATH
  Ruta absoluta a un ejecutable del sistemas lanzado mediante el Explorador de Windows o a través del menú Inicio → Ejecutar.

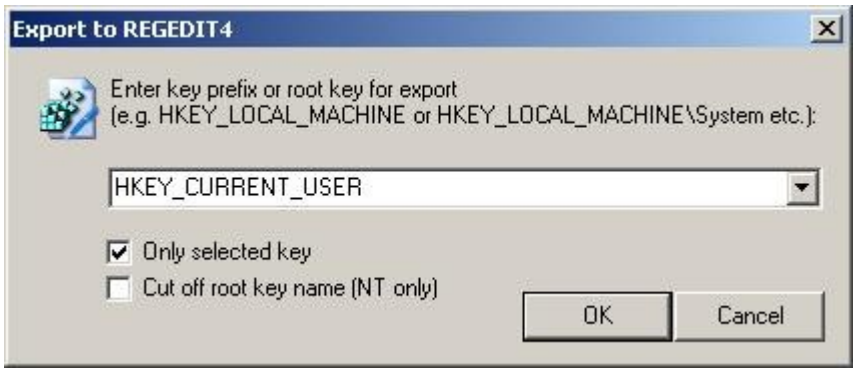
- UEME_RUNCPL
  Implica la ejecución de uno de los applets contenidos en el Panel de Control.

- UEME_RUNPIDL
  Correspondiente a un PIDL o puntero a un elemento de una lista de Ids, y que se utiliza como referencia a un objeto, habitualmente un fichero .lnk lanzado a través del menú Inicio → Documentos.

La fecha asociada a cada entrada nos indicaría la fecha de último acceso al ejecutable, applet del Panel de Control o acceso directo referenciado.

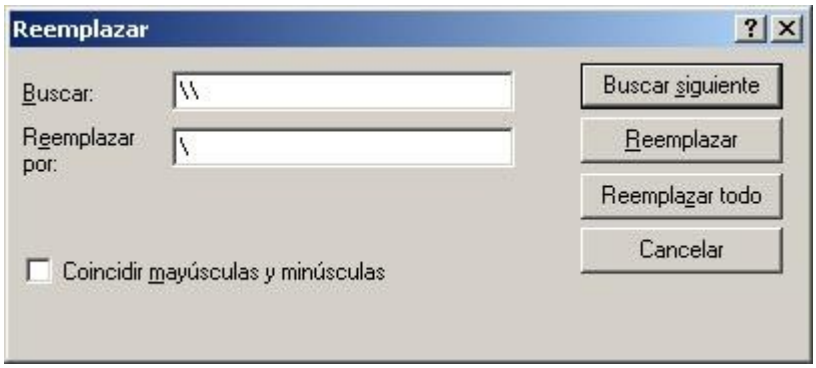
Para obtener de forma simple los datos asociados a estas entradas vamos a utilizar en primer lugar la aplicación "Windows Registry Recovery" para exportar el contenido en formato REGEDIT4 y en segundo lugar la aplicación UserAssist (enlace a la aplicación) desarrollada por Didier Stevens. Para que esta última funcione será preciso tener instalado el runtime .NET Framework 2.0 de Microsoft (enlace a la aplicación).

Comenzaremos abriendo el fichero NTUSER.DAT del usuario Administrador contenido en el directorio Documents and Settings\Administrator de la imagen del sistema comprometido. Una vez hecho esto pulsaremos sobre el botón "Raw Data" del apartado "Explorer Tasks" y accederemos a la clave UserAssist. Una vez allí desplegaremos el menú "File" seleccionando la opción "Export to REGEDIT4 format...". Como resultado obtendremos una nueva ventana la cual dejaremos como sigue:



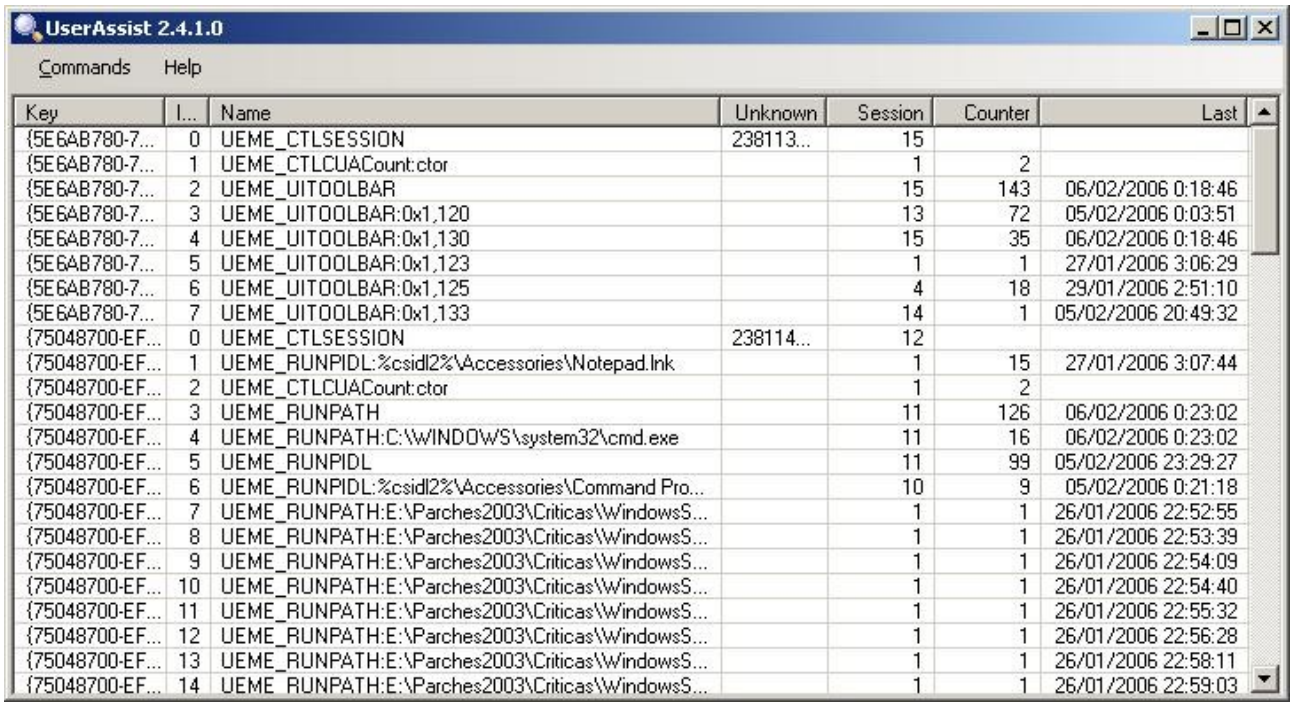
A continuación pulsaremos sobre el botón "OK" y guardaremos el fichero. Navegaremos hasta el fichero recién generado y seleccionándolo haremos click sobre el con el botón derecho del ratón → "Editar". Una vez abierto (por defecto utilizará la aplicación Notepad) desplegaremos el menú "Edición" → "Reemplazar...". En el cuadro de diálogo incluiremos los siguientes datos, pulsando seguidamente sobre el botón "Reemplazar todo":

A continuación completaremos nuevamente el cuadro de diálogo incluyendo en esta ocasión los siguientes datos tras lo que deberemos pulsar nuevamente el botón “Reemplazar todo”:



Cuando terminemos con las sustituciones anteriores cerraremos el cuadro de diálogo y la aplicación Notepad guardando el fichero cuando se nos solicite confirmación.

Ahora abriremos la aplicación UserAssist[6] y mediante el menú “Commands” → “Load from REG file” seleccionaremos el fichero obtenido en el paso anterior y obteniendo como resultado los datos almacenados en la clave UserAssist del usuario Administrator.



Key	I...	Name	Unknown	Session	Counter	Last
{5E6AB780-7...	0	UEME_CTLSESSION	238113...	15		
{5E6AB780-7...	1	UEME_CTLCUACount:ctor		1	2	
{5E6AB780-7...	2	UEME_UITOOLBAR		15	143	06/02/2006 0:18:46
{5E6AB780-7...	3	UEME_UITOOLBAR:0x1,120		13	72	05/02/2006 0:03:51
{5E6AB780-7...	4	UEME_UITOOLBAR:0x1,130		15	35	06/02/2006 0:18:46
{5E6AB780-7...	5	UEME_UITOOLBAR:0x1,123		1	1	27/01/2006 3:06:29
{5E6AB780-7...	6	UEME_UITOOLBAR:0x1,125		4	18	29/01/2006 2:51:10
{5E6AB780-7...	7	UEME_UITOOLBAR:0x1,133		14	1	05/02/2006 20:49:32
{75048700-EF...	0	UEME_CTLSESSION	238114...	12		
{75048700-EF...	1	UEME_RUNPIDL:%csidl2%\Accessories\Notepad.lnk		1	15	27/01/2006 3:07:44
{75048700-EF...	2	UEME_CTLCUACount:ctor		1	2	
{75048700-EF...	3	UEME_RUNPATH		11	126	06/02/2006 0:23:02
{75048700-EF...	4	UEME_RUNPATH:C:\WINDOWS\system32\cmd.exe		11	16	06/02/2006 0:23:02
{75048700-EF...	5	UEME_RUNPIDL		11	99	05/02/2006 23:29:27
{75048700-EF...	6	UEME_RUNPIDL:%csidl2%\Accessories\Command Pro...		10	9	05/02/2006 0:21:18
{75048700-EF...	7	UEME_RUNPATH:E:\Parches2003\Criticas\WindowsS...		1	1	26/01/2006 22:52:55
{75048700-EF...	8	UEME_RUNPATH:E:\Parches2003\Criticas\WindowsS...		1	1	26/01/2006 22:53:39
{75048700-EF...	9	UEME_RUNPATH:E:\Parches2003\Criticas\WindowsS...		1	1	26/01/2006 22:54:09
{75048700-EF...	10	UEME_RUNPATH:E:\Parches2003\Criticas\WindowsS...		1	1	26/01/2006 22:54:40
{75048700-EF...	11	UEME_RUNPATH:E:\Parches2003\Criticas\WindowsS...		1	1	26/01/2006 22:55:32
{75048700-EF...	12	UEME_RUNPATH:E:\Parches2003\Criticas\WindowsS...		1	1	26/01/2006 22:56:28
{75048700-EF...	13	UEME_RUNPATH:E:\Parches2003\Criticas\WindowsS...		1	1	26/01/2006 22:58:11
{75048700-EF...	14	UEME_RUNPATH:E:\Parches2003\Criticas\WindowsS...		1	1	26/01/2006 22:59:03

Obvia decir que deberemos repetir el proceso para cada uno de los usuarios que hayan iniciado alguna vez sesión en el sistema, es decir, aquellos que dispongan de una carpeta con su perfil en el directorio Documents and Settings de la imagen del sistema comprometido.

Si hacemos click con el botón derecho del ratón sobre cualquier de las entradas mostradas por el programa y seleccionamos la opción “Explain” obtendremos información ampliada.

6 http://blog.didierstevens.com/programs/userassist/

Información sobre la actividad de los usuarios: listas MRU

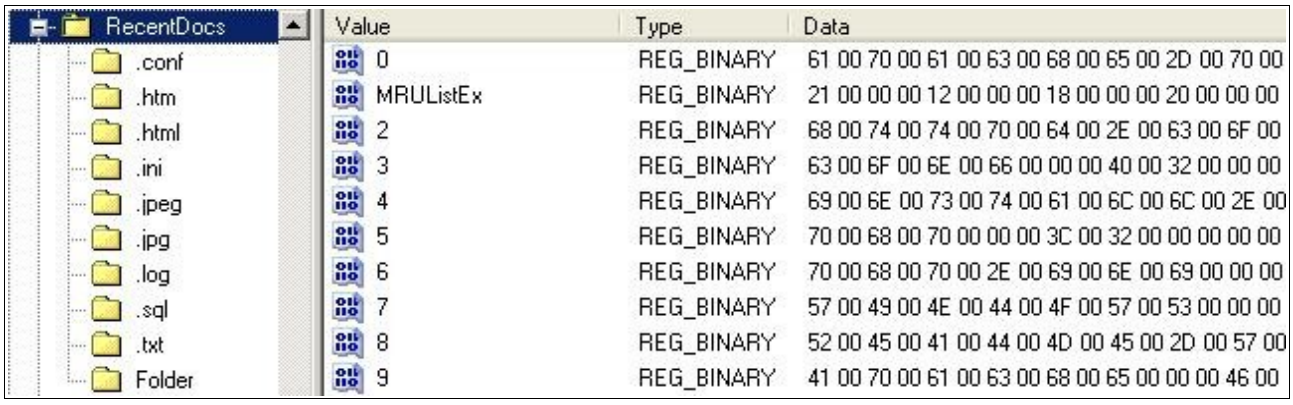
Las listas MRU (Most Recently Used) contienen entradas para un determinado número de ficheros accedidos por el usuario y organizadas por orden cronológico inverso, es decir, el primero de la lista coincidirá con el último fichero abierto.

Esta lista de ficheros aparecería habitualmente al desplegar el menú Archivo de la mayoría de aplicaciones que pueden ejecutarse en Windows.

Dado que dichas listas serán diferentes en función del usuario deberemos utilizar la porción del registro almacenada en el fichero NTUSER.DAT para cada cuenta en particular.

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

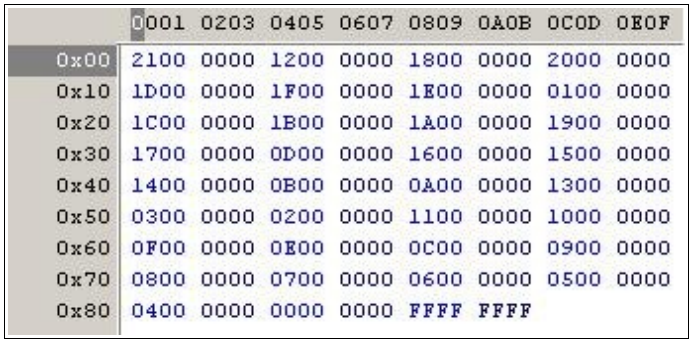
Almacena la lista de ficheros que podremos encontrar en el menú Inicio → Documentos. En esta clave podremos encontrar diferentes subclaves cuyo nombre coincidirá con una extensión por cada tipo de fichero abierto.



También encontraremos las siguientes entradas:

- Valores cuyo nombre es un número y que se corresponderán con los diferentes ficheros abiertos. La información está almacenada en forma de cadenas de texto con formato UNICODE.

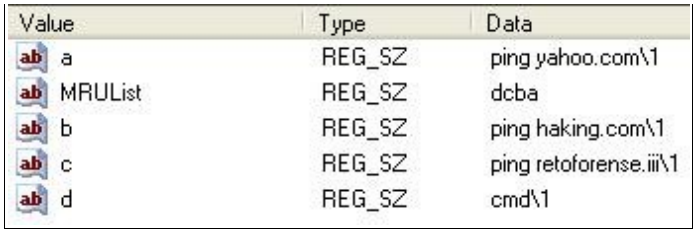
- MRUListEx
  Indica el orden en que fueron abiertos los ficheros anteriores, codificados como DWORDS y apareciendo el primero de ellos el último fichero abierto.



	0001	0203	0405	0607	0809	0A0B	0C0D	0E0F
0x00	2100	0000	1200	0000	1800	0000	2000	0000
0x10	1D00	0000	1F00	0000	1E00	0000	0100	0000
0x20	1C00	0000	1B00	0000	1A00	0000	1900	0000
0x30	1700	0000	0D00	0000	1600	0000	1500	0000
0x40	1400	0000	0B00	0000	0A00	0000	1300	0000
0x50	0300	0000	0200	0000	1100	0000	1000	0000
0x60	0F00	0000	0E00	0000	0C00	0000	0900	0000
0x70	0800	0000	0700	0000	0600	0000	0500	0000
0x80	0400	0000	0000	0000	FFFF	FFFF		

\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

Contiene todos los valores ejecutados mediante el menú Inicio → Ejecutar. Los valores aparecen especificados como texto en claro, y el nombre del valor es indicado mediante una letra del abecedario. Para saber el orden inverso (el primero será el último) en que dichos comandos fueron ejecutados deberemos analizar el valor de la entrada MRUList.



Value	Type	Data
a	REG_SZ	ping yahoo.com\1
MRUList	REG_SZ	dcba
b	REG_SZ	ping haking.com\1
c	REG_SZ	ping retoforense.iii\1
d	REG_SZ	cmd\1

\Software\Microsoft\Internet Explorer\TypedURLs

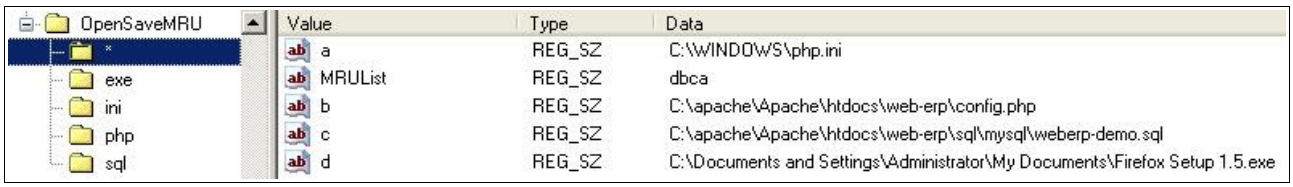
Contiene la lista de las páginas visitadas por el usuario mediante la introducción manual de la URL en la barra Dirección del navegador Internet Explorer. Esta información puede combinarse con la almacenada en la caché para diferenciar las páginas visitadas mediante un enlace de aquellas indicadas explícitamente.

Value	Type	Data
url1	REG_SZ	http://messenger.msn.com/xp/downloadx.aspx
url2	REG_SZ	Local Disk (C:)
url3	REG_SZ	http://www.google.com/
url4	REG_SZ	http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome

\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU

Contiene la lista de los ficheros abiertos mediante ventanas de diálogo “Abrir” y “Guardar como”. Los valores aparecen especificados como texto en claro agrupados en diferentes subclaves cuyo nombre coincide con la extensión del fichero abierto.

La subclave más interesante sería la que aparece nombrada con un asterisco (*) dado que contiene el total de la lista. Dentro de ella el nombre del valor es indicado mediante una letra del abecedario. Para saber el orden inverso (el primero será el último) en que dichos ficheros fueron abiertos o guardados deberemos analizar el valor de la entrada MRUList.

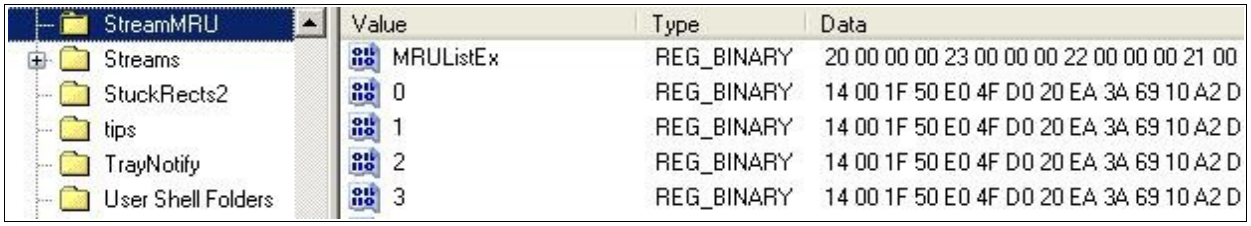


\Software\Microsoft\Windows\CurrentVersion\Explorer\StreamMRU

Mantiene una lista con los nombres de las ventanas para las diferentes aplicaciones que fueron ejecutadas por el usuario. También encontraremos las siguientes entradas:

- Valores cuyo nombre es un número y que se corresponderán con los nombres que aparecieron en las ventanas abiertas. La información está almacenada en forma de cadenas de texto con formato UNICODE.

- MRUListEx
  Indica el orden en que fueron abiertas las ventanas, codificadas como DWORDS y apareciendo la primera de ellas la última de la lista de ventanas abiertas.



\Software\Microsoft\Media Player\Player\RecentURLList

Mantiene una lista con los nombres y la ruta absoluta de los ficheros abiertos por el usuario utilizando para ello la aplicación Windows Media Player.

\Software\Microsoft\Search Assistant\ACMru

Cuando el usuario accede al asistente de búsqueda de Windows (menú Inicio → Buscar) los términos empleados en las opciones de búsqueda se almacenan en la clave anterior. Esta clave a su vez contiene, habitualmente, una combinación de cuatro subclaves:

- 5001
  Lista MRU del contenido del cuadro de texto que aparece en el diálogo “Buscar en Internet”.

- 5603
  Lista MRU del contenido del cuadro de texto “Todo o parte del nombre de archivo” que aparece en el diálogo de búsqueda de “Archivos o carpetas”.

- 5604
  Lista MRU del contenido del cuadro de texto “Una palabra o frase en el archivo” que aparece en el diálogo de búsqueda de “Archivos o carpetas”

- 5647
  Lista MRU del contenido del cuadro de texto que aparece en el diálogo de búsqueda de “Equipos o personas”.