[Curso de Informática Forense](https://platzi.com/clases/forense/)

**ArtículoReferencia del registro de Windows**

[**Juan Pablo Caro**](https://platzi.com/%40juanpcaro)

23 de Mayo de 2019

En las últimas clases aprendiste a analizar algunas ubicaciones del Registro de Windows, y a obtener información a partir de llaves usando herramientas como FRED y RegRipper. Sin embargo, el Registro de Windows es una base de datos extensa que contiene muchas ubicaciones que pueden tener información útil, y con las que deberás estar familiarizado.
A continuación, se detallan algunas de las ubicaciones comunes donde un investigador forense puede encontrar información relevante para una investigación dentro del Registro de Windows.

Archivo **NTUSER.dat**

* Historial de búsqueda
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Search\Assistant\ACMru
* Documentos recientes
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
* Documentos recientes de Office
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\10\Word\FileMRU
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\10\Excel \FileMRU
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\10\PowerPoint \FileMRU
* Comandos ejecutados por el usuario
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
* Programas ejecutados
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\CurrentVersion\Explorer\UserAssist{GUID}\Count

Archivo **SOFTWARE**

* Versión del S.O.
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
* Archivo **SYSTEM**
* CurrentControlSet
HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet00x
HKEY\_LOCAL\_MACHINE\SYSTEM\SelectCurrent

**Nota:** El Control Set es el conjunto de parámetros de una configuración del Sistema Operativo. La llave “SelectCurrent” es un apuntador a uno de los posibles ControlSet00x disponibles, y ese es el que se conoce como “CurrentControlSet”. Al hacer puntos de restauración del S.O. y guardar copias del registro, se crean nuevos Control Sets que son backups funcionales de configuraciones anteriores, pero la configuración actual del sistema siempre hace referencia al “CurrentControlSet”.

* Nombre del computador en red
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName
* Interfaces de red
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
* Zona horaria del S.O.
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation

Reportar un problema

**Análisis de procesos ejecutados**