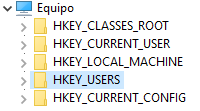
## CARPETAS PRINCIPALES



* HKCR (HKEY\_CLASES\_ROOT) :
* HKCU (HKEY\_CURRENT\_USER) : Configuraciones específicas de usuarios con sesiones iniciadas en el sistema y redirección de APIs a archivos INI virtuales en esta clave del registro HKCU.
* HKLM (HKEY\_LOCAL\_MACHINE)
* HKU (HKEY\_USER)
* HKCC (HKEY\_CURRENT\_CONFIG)
* HKEY\_PERFORMANCE\_DATA (Clave Raiz INVISIBLE para el REGEDIT)

## SUBCLAVES

* Software
* Microsoft
* Shell
* Open
* Command
* Exefile

## VALORES DENTRO DE LAS SUBCARPETAS (SON COMO ARCHIVOS)

Formados por pares NOMBRE/TIPO/DATO



## TIPOS DE VALORES

* REG\_NONE: Dato sin tipo específico
* REG\_SZ: Contiene un String o cadena de texto codificada en UTF-16
* REG\_EXPAND\_SZ: string & variables de entorno (por ejemplo: %systemroot%\drivers\etc\hosts)
* REG\_BINARY: Datos Binarios [Fileless Attacks]
* REG\_DWORD: Números positivos hasta 32bits
* REG\_LINK: Enlace a otra clave del registro [Fileless Attacks]
* REG\_MULTI\_SZ: Lista de varias cadenas (como una pequeña base de datos de texto con varias palabras)
* REG\_QWORD: Números enteros de 64bits

**No visibles para el usuario**

* REG\_RESOURCE\_LIST: Lista de recursos para dispositivos Plug&Play
* REG\_FULL\_RESOURCE\_DESCRIPTOR: descripción de recursos Plug&Play
* REG\_RESOURCE\_REQUIREMENTS\_LIST: Lista de requerimientos de recursos de Plug&Play