INSTITUTO NACIONAL DE CIBERSEGURIDAD

ANÁLISIS FORENSE DIGITAL

Unidad 4 – Artifacts Windows I
El Registro

universidad de león

MINISTERIO DE DEFENSA

SAPROMIL

MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

INDICE

1. Ficheros que dan soporte al registro.
2. Las distintas ramas del registro. Información almacenada. Herramientas.
3. Obtención de cuentas de usuario. Los ficheros SYSTEM y SAM. Herramientas.
4. Identificando la zona horaria y el horario de verano.
5. Dispositivos conectados.
6. Ficheros recientes, MRU’s.
7. Shellbags.

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

universidad de león
MINISTERIO DE DEFENSA
SAPROMIL
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

UNIDAD 4 – WINDOWS I – EL REGISTRO

1. Ficheros que dan soporte al registro

❑Importancia del forense en Windows.

- ✓ La importancia de Windows, con una cuota > 80%, es patente.
- ✓ Windows ofrece mucha asistencia al usuario y funcionalidades avanzadas. La información que da soporte a esta funcionalidades se convierte en “jugosos” artifacts para el analista forense.
- ✓ Además del SO, hay aplicaciones que también ofrecen información importante, como son los navegadores web, los sistemas de almacenamiento en cloud, las aplicaciones de email y comunicación personal, BBDD, etc…
- ✓ Por cada uno de estos apartados y herramientas concretas, podemos encontrar artifacts que nos permitan evidenciar actividad de usuario.
- ✓ Algunos los veremos y en otros casos veremos herramientas para estudiar qué información deja una determinada aplicación en el sistema.

UNIDAD 4 – WINDOWS I – EL REGISTRO

1. Ficheros que dan soporte al registro

❑El registro de Windows

- ✓ Windows, desde su versión Windows 95, guarda todos los datos de configuración de hardware, software y personalización de usuarios en una BBDD jerárquica denominada “Windows Registry”.
- ✓ En esta BBDD podemos encontrar detalles de los usuarios existentes en el sistema, las aplicaciones instaladas, con su timestamp de instalación, el hardware, los dispositivos USB conectados, la configuración de los interfaces de red, la posición de las ventanas, fecha de instalación del sistema, zona horaria, idioma, etc…
- ✓ La información se estructura en claves y/o subclaves, que toman un valor. Las claves en el más alto nivel jerárquico se denominan claves raíz:

  - ✓ HKEY_LOCAL_MACHINE (HKLM)
  - ✓ HKEY_CURRENT_USER (HKCU)
  - ✓ HKEY_USERS (HKU)
  - ✓HKEY_CLASSES_ROOT (HKCR)
  - ✓HKEY_CURRENT_CONFIG (HKCC)

UNIDAD 4 – WINDOWS I – EL REGISTRO

1. Ficheros que dan soporte al registro

❑Estructura del registro

✓ La información se almacena en los “valores”, que tienen un nombre, un tipo y datos almacenados.

Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
Nuevo valor #1	REG_DWORD	0x00000000 (0)

✓ El registro se almacena como ficheros binarios, y el programa para poder visualizar y modificar valores es `regedit.exe`.

✓ La BBDD del registro se genera durante la ejecución del SO, siendo almacenada en un conjunto de ficheros cuando este se apaga.

✓ Estos ficheros son una evidencia fundamental para el análisis forense de un dispositivo Windows. Veremos que además de la información que muestra regedit, almacena información adicional cómo el timestamp de cuándo fue modificado un determinado valor por última vez.

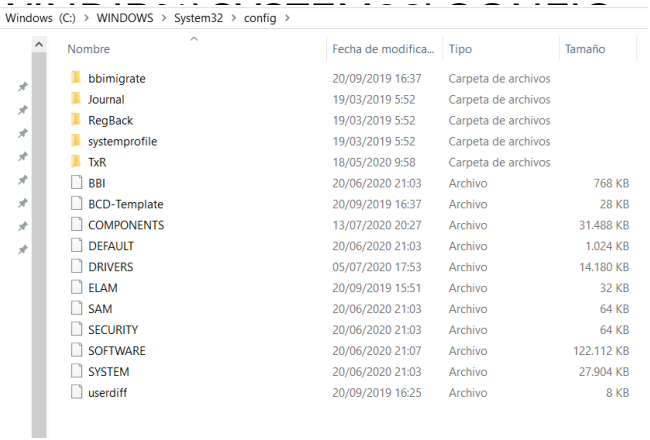
UNIDAD 4 – WINDOWS I – EL REGISTRO

1. Ficheros que dan soporte al registro

❑Ficheros de soporte del registro “Hives” de sistema

- ✓ Los ficheros dónde se almacena la información para alimentar la BBDD del registro son de dos tipos: de máquina y de usuario. En cada uno de ellos podremos encontrar actividad de uno y otro respectivamente.
- ✓ Los de máquina, se encuentran en la ruta: %

  - ✓ SAM
  - ✓ SOFTWARE
  - ✓ SYSTEM
  - ✓ SECURITY
  - ✓ DEFAULT



UNIDAD 4 – WINDOWS I – EL REGISTRO

1. Ficheros que dan soporte al registro

❑Hives de usuario

Los hives del usuario son:

- ✓ **NTUser.dat**, el principal, en la ruta \Users\"nom_usuario"\ o \Users\Default para el usuario por defecto.
- ✓ Almacena configuraciones específicas del usuario, entre ellas los asistentes para autocompletar, comandos ejecutados, unidades de red... En tiempo de ejecución se carga como la subclave HKEY_USERS\<SID_usuario> y también accesible desde HKEY_CURRENT_USER cuando el usuario ha iniciado sesión.
- ✓ **UsrClass.dat,** Ubicado en C:\Users\<nombre_usuario>\AppData\Local\Microsoft\Windows\

UNIDAD 4 – WINDOWS I – EL REGISTRO

1. Ficheros que dan soporte al registro

❑Herramientas

- ✓ Existen múltiples herramientas para análisis. Podemos distinguir entre los parser o analizadores cuya salida es en texto, muy cómodos para hacer búsquedas posteriores, y las herramientas que permiten explorar de forma interactiva el registro, a modo de visores.
- ✓ En el extremo más manual, tenemos RegRipper, https://github.com/keydet89/RegRipper2.8
- ✓ Es una herramienta escrita en perl, que dispone de múltiples plugins que extraen determinada información de los ficheros de registro.
- ✓ No realiza el análisis, pero nos permite extraer en texto información de interés del registro.
- ✓ La herramienta ejecuta conjuntos de plugins asociados a un determinado perfil. Dispone de una serie de perfiles por defecto, pudiendo crear perfiles personalizados.
- ✓ Dispone de una interface gráfica, así como de línea de comandos.

UNIDAD 4 – WINDOWS I – EL REGISTRO

1. Ficheros que dan soporte al registro

❑Valor del registro como log

- ✓ Cada clave del registro dispone de un campo de tiempo, “LastWrite”, que nos sirve de timestamp para conocer la última vez que dicha clave ha sufrido alguna modificación.
- ✓ Las aplicaciones estándar de Windows no lo presentan, por lo que tenemos que usar herramientas forenses para acceder a dicha información.

```
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time 2018-07-23 13:26:58Z
```

UNIDAD 4 – WINDOWS I – EL REGISTRO

2. Las distintas ramas del registro. Información almacenada. Herramientas.

- Correspondencia hives/ramas del registro

Sección del Registro	Archivos auxiliares
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav, Ntuser.dat, Ntuser.dat.log
HKEY_USERS\DEFAULT	Default, Default.log, Default.sav

UNIDAD 4 – WINDOWS I – EL REGISTRO

2. Las distintas ramas del registro. Información almacenada. Herramientas.

El registro es el corazón de un sistema Windows y en él reside información vital en todo análisis forense. SIEMPRE tendremos una copia del registro, bien para extraer información de ubicaciones conocidas, bien para respaldar conclusiones aún por determinar.

UNIDAD 4 – WINDOWS I – EL REGISTRO

3. Obtención de cuentas de usuario. Los ficheros SYSTEM y SAM. Herramientas.

❑SAM, Security Account Manager

- ✓ Los usuarios en Windows se almacenan en el fichero SAM, junto con su UID, y el hash NTLM de la contraseña, entre otra información de interés forense.
- ✓ En el caso de un controlador de dominio, se almacenan en %SYSTEMROOT%\NTDS\Ntds.dit
- ✓ La adquisición de los ficheros relacionados con el registro, SAM y Ntds, no puede hacerse directamente con el SO arrancado, pues los tiene bloqueados, por lo que en "live" debemos utilizar herramientas de terceros o bien las instantáneas de volumen del propio Windows.
- ✓ La adquisición partiendo de una imagen es inmediata, explorando dicha imagen con FTK Imager o con TSK.

UNIDAD 4 – WINDOWS I – EL REGISTRO

3. Obtención de cuentas de usuario. Los ficheros SYSTEM y SAM. Herramientas.

❑Adquisición live con herramientas del sistema

- ✓ Como sabemos, debemos dejar la menor huella posible en el sistema, por lo que una buena opción es utilizar las propias herramientas de este, entre las que se encuentran las instantáneas de volumen, o VSS.
- ✓ Para crear la instantánea, usamos la herramienta instantánea de volumen, de Windows Server o Recuperación de sistema de versiones de escritorio.
- ✓ Una vez creada, mediante el comando `vssadmin list shadows`, seleccionamos la que nos interesa y…
- ✓ Mediante el comando `mklink /d "punto montaje" "id. Instantánea"` la montamos en una carpeta para trabajar con ella.

UNIDAD 4 – WINDOWS I – EL REGISTRO

3. Obtención de cuentas de usuario. Los ficheros SYSTEM y SAM. Herramientas.

❑Herramientas análisis

Para el análisis y obtención de cuentas del fichero SAM podemos usar:

- ✓ Regripper, parser que nos permite volcar el contenido de los distintos hives del registro en un fichero de texto. Disponible en GitHub.
- ✓ Windows Registry Recovery, herramienta gráfica del fabricante Mitec, gratuita para uso no comercial, que nos permite explorar gráfica los hives del registro.
- ✓ RegistryExplorer de Eric Zimmerman, herramienta gráfica que nos permite ver toda la información relevante en forense sobre las cuentas de usuario.

UNIDAD 4 – WINDOWS I – EL REGISTRO

4. Identificando la zona horaria y el horario de verano.

❑Importancia de la zona horaria

- ✓ En el análisis forense es vital la correlación temporal.
- ✓ En los casos en los que sólo hay una máquina es sencillo, aunque siempre existen posibles confusiones, ya que por regla general:

> Windows registra en hora UTC y sus herramientas presentan la información en hora local

- ✓ En función de la herramienta usada, debemos tener claro en qué zona horaria presenta la información. Las herramientas de corte forense suelen incluir la prestación de definir zona horaria.
- ✓ En general, es recomendable hacer los análisis en UTC y convertir a local sólo en el informe.

UNIDAD 4 – WINDOWS I – EL REGISTRO

4. Identificando la zona horaria y el horario de verano.

❑La clave TimeZoneInformation

- ✓ La zona horaria es un dato guardado en el fichero SYSTEM, accesible en el registro en la ruta: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation
- ✓ En esta clave encontramos identificación de la zona horaria, del horario de verano y de la corrección horaria respecto a UTC.
- ✓ El valor más relevante en ActiveTimeBias, que contiene la corrección horaria total, incluyendo la zona horaria y el horario de verano.

Valor del registro	Significado
`Bias`	Desplazamiento base respecto a UTC
`StandardBias`	Cambio aplicado durante horario estándar
`DaylightBias`	Cambio aplicado durante horario de verano (DST)
`ActiveTimeBias`	Desplazamiento **actual** en minutos, dinámico

UNIDAD 4 – WINDOWS I – EL REGISTRO

5. Dispositivos conectados por USB

❑Evidenciar conexiones por USB

El uso de dispositivos externos puede ser relevante en función del caso.

Tenemos distintos artefactos de interés para investigarlos:

✓ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR

- Incluye marca, modelo, nº de serie si lo informa, de los dispositivos conectados al sistema.
- El timestamp de las claves indica el instante de la última conexión.

✓ HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices

- Indica dispositivos montados y letra de unidad.
- Permite correlacionar con la clave anterior para saber con que letra de unidad se montó.

UNIDAD 4 – WINDOWS I – EL REGISTRO

5. Dispositivos conectados por USB

❑Evidenciar conexiones por USB (II)

✓ C:\Windows\inf\setupapi.dev.log

- Son los logs de instalación, dónde quedan trazas delmomento de la instalación de los dispositivos.
- El timestamp de las claves indica el instante de primera conexión.

UNIDAD 4 – WINDOWS I – EL REGISTRO

5. Dispositivos conectados por USB

❑Evidenciar conexiones por USB. Herramientas

- ✓ Además de las propias vistas para el trabajo con el registro, contamos con la utilidad **USBDeview**, de Nirsoft. Permite correlacionar y presentar en un entorno gráfico la información sobre dispositivos USB del equipo en el que se ejecuta o bien de un conjunto de ficheros externos.

- ✓ **USB Detective**, que dispone de versión profesional y community. Correlaciona información de distintas fuentes, USBSTOR, MountedDevices, SetupAPI.dev.log, etc…

UNIDAD 4 – WINDOWS I – EL REGISTRO

6. Ficheros recientes, MRU’s.

❑Most Recent Used, MRU’s.

- ✓ Es una funcionalidad que ofrece el SO para localizar programas o documentos accedidos habitualmente.
- ✓ Existen múltiples ubicaciones donde los programas y el propio SO almacena información para agilizar el trabajo del usuario.
- ✓ La mayoría de información en relación a MRU’s se guarda en valores del registro.

Ejemplos:

```
HKCU\software\Microsoft\windows\currentversion\explorer\runmru
```

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU
```

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU
```

UNIDAD 4 – WINDOWS I – EL REGISTRO

7. ShellBags

❑Información de visualización de la ventana gráfica, ShellBag.

- ✓ Es la información que permite a Windows “recordar” la posición y preferencias de visualización de una ventana.
- ✓ Esta información se almacena, además de en el hive NTUser.dat en el otro hive de usuario que hemos nombrado con anterioridad:

  C:\Users\nacho\AppData\Local\Microsoft\Windows\UsrClass.dat

- ✓ La información en los valores de estas claves es codificada, por lo que, para analizarla, usaremos herramientas de terceros.
- ✓ Debido a los timestamp del registro, nos permite evidenciar la exploración de una ruta.

UNIDAD 4 – WINDOWS I – EL REGISTRO

7. ShellBags

❑Herramientas.

- ✓ De nuevo, podemos utilizar las herramientas generalistas para el registro, como Regripper, con los plugin adecuados.
- ✓ Adicionalmente, ShellBagsView, de Nirsoft, para analizar las del equipo local en live.
- ✓ Y ShellBags Explorer de Eric Zimmerman, una herramienta gráfica muy adecuada para este análisis. También dispone de herramienta de línea de comando, SBEcmd.
- ✓ ShellBag Parser, de TZWorks, parser que nos ofrece salida en CSV para su posterior análisis.

UNIDAD 4 – WINDOWS I – EL REGISTRO

Las herramientas ayudan a la localización de la información, pero el analista tiene que conocer los fundamentos de la herramienta para entender los resultados, así como llevar a cabo un análisis manual si es necesario. Las herramientas NO ANALIZAN.

FIN UNIDAD

Unidad 4
ARTIFACTS WINDOWS I
EL REGISTRO

INSTITUTO NACIONAL DE CIBERSEGURIDAD

universidad de león

MINISTERIO DE DEFENSA

SAPROMIL

MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES