INSTITUTO NACIONAL DE CIBERSEGURIDAD

ANÁLISIS FORENSE DIGITAL

Unidad 5 – Artifacts Windows II
El registro de Eventos y otros artifacts

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

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 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

1. Ficheros y estructura de los registros de Eventos.

❑Concepto de log

- ✓ Los logs son los registros de la actividad de un sistema.
- ✓ Actualmente cualquier dispositivo o aplicación que se precie es capaz de escribir logs sobre su actividad.
- ✓ Son una fuente fundamental en las investigaciones forenses.
- ✓ Registran, como mínimo, datos del suceso y timestamp.
- ✓ Windows los denomina “eventos” y el programa para visualizarlo Visor de Eventos, al que podemos acceder ejecutando `eventvwr.msc`.
- ✓ Generan una cantidad ingente de información, por lo que las herramientas para búsqueda, filtrado y ordenación son necesarias.
- ✓ Habitualmente son registros en formato texto, aunque Windows usa un formato propietario.

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

1. Ficheros y estructura de los registros de Eventos.

❑Registros de eventos en Windows

Windows 10 dispone de mas de 300 registros de eventos, aunque hay 5 principales, denominados registros de Windows:

- ✓ Aplicación, dónde se registran los sucesos como actualizaciones, crashes, inicios o cambios de aplicaciones.
- ✓ Seguridad, dónde se registran los resultados del servicio de auditoría, inicios y cierres de sesión, acceso a objetos, elevación de privilegios y cambios de políticas.
- ✓ Instalación, aquí se registran todas las actualizaciones del SSOO
- ✓ Sistema, dónde se deja constancia del arranque y parada de los servicios del SO, así como de los errores.
- ✓ Eventos reenviados, cuándo un equipo actúa como concentrador de eventos, aquí veremos los logs de otras máquinas.

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

1. Ficheros y estructura de los registros de Eventos.

❑Registros de eventos en Windows (ii)

✓ Los eventos en Windows, en general, tienen la siguiente información:

- ✓ Nivel, que puede ser crítico, información, advertencia, detallado o error.
- ✓ Fecha y hora
- ✓ Id del evento, un valor numérico asignado a un tipo de evento en concreto.
- ✓ Equipo y usuario, si procede.

Nombre de registro:	Sistema		
Origen:	DistributedCOM	Registrado:	16/07/2020 7:43:28
Id. del	10016	Categoría de tarea:	Ninguno
Nivel:	Advertencia	Palabras clave:	Clásico
Usuario:	KALOGEROX\nacho	Equipo:	KALOGEROX
Código de operación:	Información		
Más información:	Ayuda Registro de eventos		

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

1. Ficheros y estructura de los registros de Eventos.

❑Ubicación de los ficheros de registro

- ✓ Los registros de eventos son artefactos fundamentales en cualquier investigación forense dónde haya un sistema Windows implicado y, por lo tanto, deberemos copiarlos para su investigación.
- ✓ La ruta, en sistemas Vista en adelante es %WINDIR%\System32\winevt\logs.
- ✓ Los ficheros de eventos tienen la extensión evtx (evt en sistemas anteriores a W7)
- ✓ Dado que son muchos los registros, es una buena práctica ordenarlos por tamaño, pudiendo ver cuales de ellos contienen más información.

Registro	Contenido
System.evtx	Logs del sistema
Security.evtx	Resultados del servicio de auditoría. Esencial para forense.
Application.evtx	Logs de aplicaciones

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

1. Ficheros y estructura de los registros de Eventos.

❑Estructura de los eventos

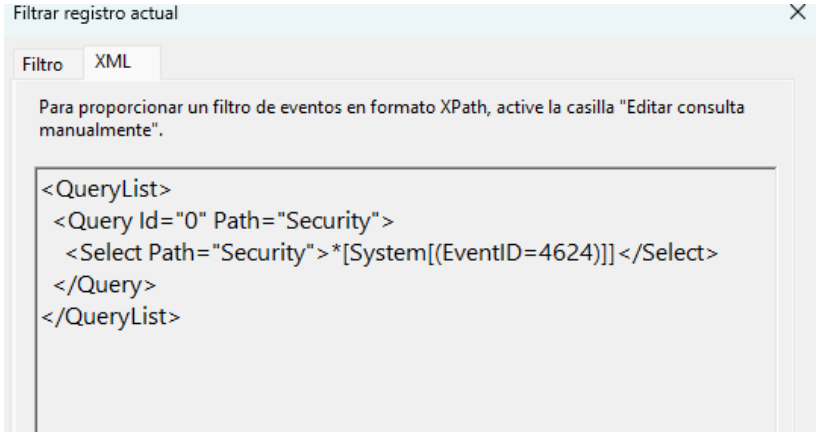
- ✓ Los ficheros .evtx son binarios, aunque tienen una parte como xml, con etiquetas.
- ✓ Guardan los registros en “chunks” de 64 Kb
- ✓ Por defecto son circulares y una vez alcanzado su tamaño máximo, sobreescriben los eventos más antiguos.
- ✓ Internamente, cada evento está en XML estructurado con:
  - <System>: metadatos como ID, tiempo, origen.
  - <EventData>: detalles del evento (usuario, ruta, etc.).

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

2. Filtrado avanzado de eventos. Herramientas.

❑Filtros en el Visor de Eventos

✓ El propio Visor de Eventos de Windows provee de una herramienta de filtrado potente, pudiendo consultar la sintaxis de los filtros para personalizarla:



✓ Permite filtrar por los campos más habituales, de forma gráfica, y además permite realizar consultas xpath para un filtrado personalizado.

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

2. Filtrado avanzado de eventos. Herramientas.

❑Herramientas

Aunque el propio visor de Windows permite abrir evtx externos, es habitual herramientas enfocadas al forense, que permiten:

- ✓ Introducir corrección horaria configurable.
- ✓ Hacer búsquedas en distintos ficheros evtx.
- ✓ Abrir múltiples ficheros y realizar búsquedas y filtrados de forma más eficiente.

Algunas herramientas son:

- ✓ Event Log Explorer, herramienta gráfica, muy útil e intuitiva. Gratuita para uso no comercial.
- ✓ Nirsoft FullEventLogView, también es gráfica y ligera, siendo una opción válida.

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

3. Eventos y tipos de inicio de sesión en Windows.

❑Eventos de inicio de sesión

- ✓ En Windows es habitual la búsqueda de eventos por ID de evento.
- ✓ Microsoft no ha mantenido una denominación de ID de eventos continua a lo largo del tiempo. Sólo podemos encontrar cierta continuidad desde los SSOO W2K8 en adelante.

Event ID	Descripción
4624	An account was successfully loged on
4625	An account failed to log on
4648	A logon was attempted using explicit credentials
4675	SSID were filtered

Eventos importantes de inicio de sesión

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

3. Eventos y tipos de inicio de sesión en Windows.

❑Tipos de inicio de sesión

- ✓ El mismo evento de inicio de sesión puede ser de un tipo u otro, aportando información interesante sobre la ubicación del usuario.
- ✓ Los de mayor interés por estar asociados a un usuario, son el 2, interactivo delante del Pc o con herramienta de gestión remota, y el 10, de escritorio remoto. El 3 se produce al acceder a un recurso compartido.

Tipo de inicio de sesión	Título de inicio de sesión
2	Interactiva
3	Red
4	Proceso Batch
5	Servicio
7	Desbloquear
8	NetworkCleartext
9	NewCredentials
10	RemoteInteractive (Escritorio Remoto o Terminal Services)
11	CachedInteractive (Sin comprobar con el AD)

Eventos y tipos de inicio de sesión en Windows.

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

4. Otros artefactos de Interés

❑UserAssist

- ✓ Windows registra los programas abiertos por un usuario, el número de ejecuciones y desde dónde se ha ejecutado, guardando esta información en el registro, en el hive NTUser.dat.
- ✓ UserAssist provee de información interesante para el análisis forense, ya que al tratarse de un valor del registro también tenemos el timestamp de la última modificación.
- ✓ La ruta dentro del registro es:

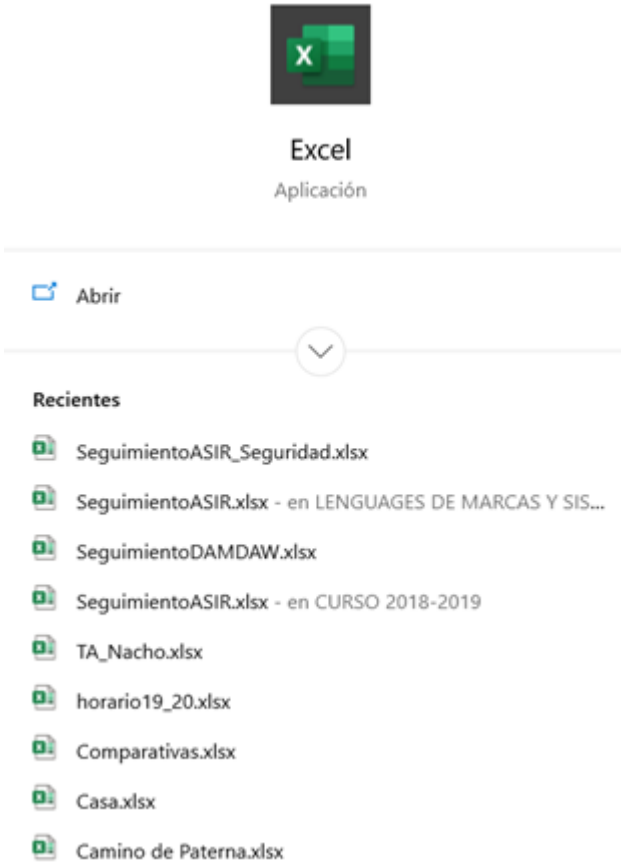
`Equipo\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist`

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

4. Otros artefactos de Interés

❑Jump List

- ✓ Funcionalidad que nos permite acceder fácilmente a los últimos documentos, conexiones o ubicaciones abiertas.
- ✓ Dispone de dos vertientes, una en la que guarda los “links” a cada uno de estos elementos, en la carpeta “recent”, ubicada en %AppData%\Roaming\Microsoft\Windows\Recent
- ✓ Una segunda en la que guarda un stream por cada aplicación, dónde va guardando los ficheros, conexiones o ubicaciones que desde esta se abren.
- ✓ Esta última a su vez, tiene dos stream, la adición automática por parte del SSOO y los ficheros que puede “anclar” el usuario, denominadas automatic o custom destinations respectivamente.

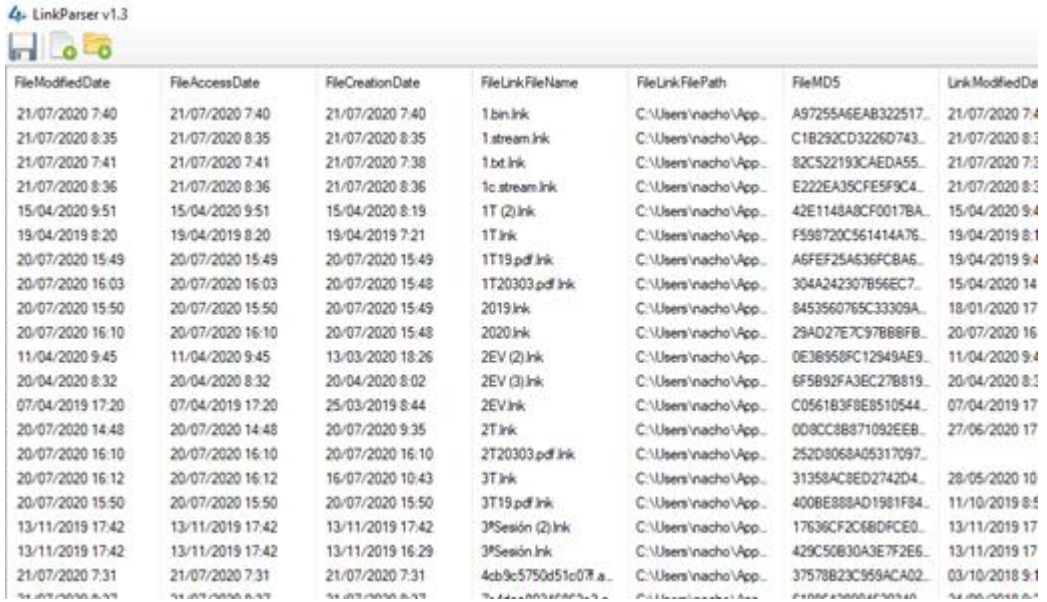


UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

4. Otros artefactos de Interés

❑Jump List (ii)

- ✓ El formato de Microsoft de los ficheros .lnk deja información interesante adicional a la ruta del fichero, como:
  - ✓ Fecha de creación (1er acceso)
  - ✓ Fecha de acceso (última ejecución)
  - ✓ Nº Serie y nombre del volumen donde se encuentra el destino.
  - ✓ Tipo de medio (Fixed o removable)



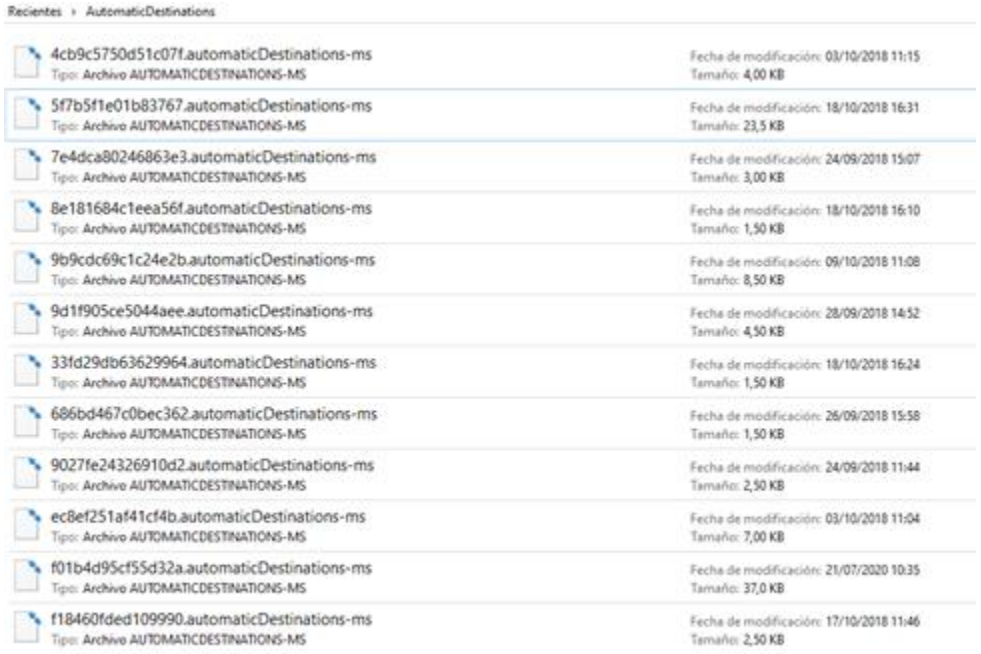
FileModifiedDate	FileAccessDate	FileCreationDate	FileLink.FileName	FileLink.FilePath	FileMD5	LinkModifiedDa
21/07/2020 7:40	21/07/2020 7:40	21/07/2020 7:40	1.bin.lnk	C:\Users\nacho\App...	A97255A6EAB322517...	21/07/2020 7:4
21/07/2020 8:35	21/07/2020 8:35	21/07/2020 8:35	1.stream.lnk	C:\Users\nacho\App...	C1B292CD3226D743...	21/07/2020 8:3
21/07/2020 7:41	21/07/2020 7:41	21/07/2020 7:38	1.txt.lnk	C:\Users\nacho\App...	82C522193CAEDA55...	21/07/2020 7:3
21/07/2020 8:36	21/07/2020 8:36	21/07/2020 8:36	1c.stream.lnk	C:\Users\nacho\App...	E222EA35CFE5F9C4...	21/07/2020 8:3
15/04/2020 9:51	15/04/2020 9:51	15/04/2020 8:19	1T (2).lnk	C:\Users\nacho\App...	42E1148A8CF0017BA...	15/04/2020 9:4
19/04/2019 8:20	19/04/2019 8:20	19/04/2019 7:21	1T.lnk	C:\Users\nacho\App...	F598720C561414A76...	19/04/2019 8:1
20/07/2020 15:49	20/07/2020 15:49	20/07/2020 15:49	1T19.pdf.lnk	C:\Users\nacho\App...	A6FEF25A636FCBA6...	19/04/2019 9:4
20/07/2020 16:03	20/07/2020 16:03	20/07/2020 15:48	1T20303.pdf.lnk	C:\Users\nacho\App...	304A242307B56EC7...	15/04/2020 14
20/07/2020 15:50	20/07/2020 15:50	20/07/2020 15:49	2019.lnk	C:\Users\nacho\App...	8453560765C33309A...	18/01/2020 17
20/07/2020 16:10	20/07/2020 16:10	20/07/2020 15:48	2020.lnk	C:\Users\nacho\App...	29AD27E7C97B8BFB...	20/07/2020 16
11/04/2020 9:45	11/04/2020 9:45	13/03/2020 18:26	2EV (2).lnk	C:\Users\nacho\App...	0E3B958FC12949AE9...	11/04/2020 9:4
20/04/2020 8:32	20/04/2020 8:32	20/04/2020 8:02	2EV (3).lnk	C:\Users\nacho\App...	6F5B92FA3EC27B819...	20/04/2020 8:3
07/04/2019 17:20	07/04/2019 17:20	25/03/2019 8:44	2EV.lnk	C:\Users\nacho\App...	C0561B3F8E8510544...	07/04/2019 17
20/07/2020 14:48	20/07/2020 14:48	20/07/2020 9:35	2T.lnk	C:\Users\nacho\App...	0D8CC8B871092EEB...	27/06/2020 17
20/07/2020 16:10	20/07/2020 16:10	20/07/2020 16:10	2T20303.pdf.lnk	C:\Users\nacho\App...	252D8068A05317097...	
20/07/2020 16:12	20/07/2020 16:12	16/07/2020 10:43	3T.lnk	C:\Users\nacho\App...	31358AC8ED2742D4...	28/05/2020 10
20/07/2020 15:50	20/07/2020 15:50	20/07/2020 15:50	3T19.pdf.lnk	C:\Users\nacho\App...	400BE888AD1981F84...	11/10/2019 8:5
13/11/2019 17:42	13/11/2019 17:42	13/11/2019 17:42	3ªSesión (2).lnk	C:\Users\nacho\App...	17636CF2C6BDFCE0...	13/11/2019 17
13/11/2019 17:42	13/11/2019 17:42	13/11/2019 16:29	3ªSesión.lnk	C:\Users\nacho\App...	429C50B30A3E7F2E6...	13/11/2019 17
21/07/2020 7:31	21/07/2020 7:31	21/07/2020 7:31	4cb9c5750d51c07ff.a...	C:\Users\nacho\App...	37578B23C959ACA02...	03/10/2018 9:1

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

4. Otros artefactos de Interés

❑Jump List (iii)

- ✓ El formato en el que se guardan los “stream” de las jump list se denomina Structured Storage, basado en el estándar OLE.
  - ✓ Un stream por aplicación.
  - ✓ Los primeros caracteres de cada fichero de stream identifican la aplicación a la que corresponde, el applicationID.
  - ✓ En ese stream están todos los accesos a documentos, conexiones o carpetas, sería como una carpeta “recent” de la aplicación.



UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

4. Otros artefactos de Interés

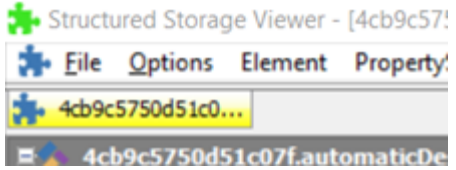
❑Herramientas para el análisis de Jump List

✓ Para el análisis de los ficheros .lnk podemos usar Link Parser, de 4Discovery.

https://4discovery.com/our-tools/link-parser/

✓ Para el análisis de los ficheros de stream de automatic destinations, disponemos de MiTec Structured Storage Viewer, que permite ver el contenido de estas listas y exportarlo en modo de ficheros .lnk, que pueden ser a su vez analizados por Link Parser.

https://www.mitec.cz/ssv.html



UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

4. Otros artefactos de Interés

❑Nirsoft

- ✓ Se trata de una colección de utilidades desarrolladas y compartidas de forma totalmente altruista por Nir Sofer.
- ✓ En general, son herramientas de un propósito muy específico, ligeras y portables, muchas de ellas están pensadas para uso forense, permitiendo analizar evidencias tomadas de otras máquinas.
- ✓ Se pueden descargar herramientas en modo “stand alone” o mediante un gestor que permite acceder por familias, el NirLauncher. Incluso el mismo gestor permite unificar otro tipo de suites de herramientas como Sysinternals:

https://launcher.nirsoft.net/downloads/index.html

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

4. Otros artefactos de Interés

❑Nirsoft (ii)

Entre las aproximadamente 200 utilidades, las siguientes nos valen para analizar los artifacts mencionados.

- ✓ UserAssistView
- ✓ ShellBagsView
- ✓ LatActivityView
- ✓ USBDeView
- ✓ RecentFilesView (MRU's)

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

5. Ubicaciones jugosas del sistema de ficheros.

❑Rutas de interés en Windows

- ✓ Adicionalmente a todas las rutas nombradas, es de especial interés las rutas del perfil de usuario %userprofile%\Appdata.
- ✓ Aquí encontraremos tres carpetas, local, local low y roaming dónde muchas aplicaciones nos dejarán sus datos específicos relativos al usuario, como son cookies, BBDD sqlite con formularios, contraseñas de sitios web, BBDD de correo electrónico, logs de sincronización de herramientas de almacenamiento cloud, etc...
- ✓ No podemos saber a priori qué aplicaciones tiene el usuario y cuáles nos van a ofrecer información, por lo tanto deberemos pensar en recopilar todo lo que podamos de esta ruta.
- ✓ En particular es de interés la ruta: C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt, por encontrarse el historial de comandos de Powershell.

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

6. Prefecth. Mecanismo y análisis.

❑Windows Prefetch

- ✓ El “prefetching” es una funcionalidad de Windows utilizada para acelerar la carga tanto del SO como de las aplicaciones.
- ✓ Para ello, registra durante los 10 primeros segundos tras la ejecución de una aplicación las librerías que esta necesita. Además, registra el número de veces que se ejecuta la aplicación, con el fin de anticipar la carga de estas librerías y agilizar la carga de la aplicación.
- ✓ A efectos forenses, este artifact nos permite evidenciar la ejecución de un programa, el número de veces ejecutado y la fecha de la última ejecución.
- ✓ Existen dos tipos de servicio, prefetch se boot y prefetch de aplicación.
- ✓ Por defecto, el de aplicación sólo está habilitado en los SSOO cliente.
- ✓ La ruta a los ficheros de prefetch se encuentra en %Windir%\Prefetch

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

6. Prefecth. Mecanismo y análisis.

❑Windows Prefetch (ii)

- ✓ Los archivos de Prefetch tienen la extensión .pf y se generan de forma individual, uno por cada aplicación ejecutada.
- ✓ Dado que se trata de ficheros binarios, usaremos una aplicación de terceros para su análisis.
- ✓ Nirsoft WinPrefetchView es una herramienta sencilla, de la suite de Nirsoft, que nos permite extraer esta información de los ficheros .pf.

https://www.nirsoft.net/utils/win_prefetch_view.html

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

7. Navegadores

❑Actividad de navegación

✓El análisis de la actividad de navegación por Internet es básico, y ofrece información como:

- ✓ Sitios WEB visitados
- ✓ Ficheros descargados
- ✓ Cookies de sesión
- ✓ Passwords almacenadas
- ✓ Formularios completados
- ✓ Navegación por el sistema de ficheros local (Edge en Windows)
- ✓ Correlación de la navegación con la actividad del sistema de ficheros

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

7. Navegadores

❑El formato SQLite.

- ✓ Los navegadores manejan cada vez más información, que han pasado de almacenar en ficheros planos a modelos de BBDD.
- ✓ Un formato habitual de BBDD para navegadores es Sqlite.
- ✓ Sqlite no necesita de un servidor, sino que ofrece mediante una librería las funciones necesarias para la gestión de la BBDD contenida en un único fichero, de extensión `.sqlite`.

http://www.sqlite.org/

- ✓ Hay varios programas y complementos que nos permiten explorar el contenido de estos ficheros, p.e. DB Browser for SQLite, SQLite Manager.

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

7. Navegadores

❑Artifacts de principales navegadores

- ✓ Todos los navegadores nos ofrecen, cómo mínimo, los siguientes Artifacts:
  - ✓ Historial de navegación: relación de sitios visitados con timestamp.
  - ✓ Cache: contenido descargado almacenado para su reutilización
  - ✓ Cookies: ficheros que guardan datos de la sesión del usuario, como preferencias o identificadores de sesión.
- ✓ Adicionalmente, nos pueden ofrecer:
  - ✓ Formularios completados, con los datos tecleados.
  - ✓ Passwords de sitios web almacenadas.
  - ✓ Relación de ficheros descargados.

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

7. Navegadores

❑Artifacts de Mozilla Firefox

- ✓ Firefox genera un perfil por usuario y genera un directorio por perfil, en el que almacena todos los datos.
- ✓ La ruta de este directorio es:
  - ✓ %USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\
- ✓ Los ficheros que encontramos de interés son:
  - ✓ cache2
  - ✓ cookies.sqlite
  - ✓ **places.sqlite.**
  - ✓ downloads.sqlite: Historial de descargas.
  - ✓ formhistory.sqlite: Contiene los formularios memorizados pior la función “autocompletar”.
  - ✓ permissions.sqlite: Contiene los sitios a los que se le permitió abrir pop-ups.
  - ✓ search.sqlite: Historial del motor de búsqueda que se encuentra en la parte derecha de la barra de herramientas.
  - ✓ webappsstore.sqlite: Almacena las sesiones.
  - ✓ signons.sqlite: Contraseñas almacenadas.

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

7. Navegadores

❑Artifacts de Google Chrome

- ✓ Chrome dispone de un directorio con los datos de usuario y guarda por defecto en la carpeta default de este directorio.
- ✓ La ruta de este directorio es:
  - ✓ %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\
- ✓ Los ficheros que encontramos de interés son, en formato SQLite:
  - ✓ history
  - ✓ cookies
  - ✓ login.data: Password almacenadas
  - ✓ cache

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

7. Navegadores

❑Artifacts de Internet Explorer 11 y EDGE

- ✓ Microsoft ha dado muchas vueltas con sus navegadores y esto afecta a la diversidad de artifacts.
- ✓ Básicamente, distinguimos las versiones de Internet Explorer, que acaba con la 11 y MS Edge.
- ✓ Microsoft Edge es el sucesor, basado en tecnología MS hasta enero de 2020, en el que se ha lanzado un nuevo EDGE basado en Chromium, por lo que el análisis se hará, a partir de esta fecha, de forma similar a Chrome.
- ✓ MS ha usado como sistema BBDD ESE, Extensible Storage Engine, en vez de SQLite hasta Enero de 2020.

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

7. Navegadores

❑Artifacts de Internet Explorer 11 y EDGE (ii)

- ✓ Hasta Windows 7, los datos de navegación se guardan en un fichero de datos llamado index.dat ubicado en %USERPROFILE%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5

- ✓ A partir de Windows 8, estos datos se guardan en una BBDD ESE llamada WebCacheV01.dat, en la ruta %USERPROFILE%\AppData\Local\Microsoft\Windows\Webcache

Otras ubicaciones de interés son:

- ✓ %USERPROFILE%\AppData\Local\Microsoft\Windows\History, donde encontramos el historial de ficheros descargados/abiertos.
- ✓ Como vemos, la actividad registrada no es específica de la navegación Internet, sino que enontraremos registros de actividad de l apropia interface de Windows, ya que el navegador forma parte del SSOO.

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

7. Navegadores

❑Herramientas de análisis

La suite de Nirsoft incluye varias herramientas para el análisis de estos artifacts:

- ✓EseDatabaseView, para ver el contenidos de ficheros de Microsoft ESE.
- ✓Visores de Cache para IE, Chrome y Firefox.
- ✓Browsing History View, una herramienta excepcional para analizar el historial de todos los navegadores de forma centralziada, con filtros de fecha muy finos.
- ✓WebBrowserPassView, herramienta para visualizar las credenciales guardadas de los navegadores mayoritarios. No está incluida en NirLauncher.

https://www.nirsoft.net/utils/web_browser_password.html

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

8. Obtención de información en live. Process Monitor y process Explorer.

❑Adquisición en live

- ✓ Es la situación más común en DFIR, siempre que los datos volátiles tengan algún interés.
- ✓ Vista la cantidad de artefactos, es recomendable utilizar uan herramienta que permita automatizar el proceso.
- ✓ Ádemás es deseable que la herramienta calcule hashes de los ficheros capturados y sea muy “verbose” en cuanto a la escritura de comandos y/o acciones ejecutados y salida de estos.
- ✓ Por ello, usamos la herramienta gratuita de Securizame Wintriage, que reúne todas estas características:

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

8. Obtención de información en live. Process Monitor y process Explorer.

Process Explorer

❑Análisis en live

- ✓ En DFIR es frecuente tener que analizar una máquina en vivo.
- ✓ Las herramientas deben ser precisas y portables para dejar las menores alteraciones posibles.
- ✓ Sysinternals nos ofrece dos pequeñas joyas en este aspecto:

- ✓ Process Explorer, permite volcar la memoria del proceso, ver las dll's que carga, las dependencias.
- ✓ Process Monitor, permite ver la actividad de los procesos en la máquina. Operaciones de r/w a disco, red, registro, etc…

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

9. Análisis de memoria RAM en Windows. Volatility.

❑Análisis de RAM

En la memoria se encuentra toda la información de la ejecución del SSOO:

- ✓ Fichero $MFT
- ✓ Ficheros abiertos
- ✓ Sesiones iniciadas
- ✓ Conexiones de red
- ✓ Hashes y tickets de autenticación
- ✓ Contenido de la pantalla
- ✓ Contenido de cada uno de los programas en ejecución
- ✓ Etc…

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

9. Análisis de memoria RAM en Windows. Volatility.

❑Análisis de RAM - Dificultades

- ✓ Cada vez son más aleatorias las posiciones en las que se guarda una determinada información en memoria, por lo que, aunque sabemos que la información está, es difícil localizarla.
- ✓ Existen distintas herramientas para el análisis de volcados de memoria, pero el proyecto opensource que predomina es Volatility Framework.
- ✓ La adquisición de memoria es sencilla, utilizando un programa como Ramcapturer, del fabricante Belkasoft.

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

9. Análisis de memoria RAM en Windows. Volatility.

❑Volatility

- ✓ Se trata de un framework opensource para el análisis de memoria RAM, que permite el desarrollo de plugins, que permiten extraer una información concreta de la memoria.
- ✓ Consta del propio framework, perfiles de memoria que le indican el "cómo" encontrar las cosas en el fichero de volcado y de "plugins" que realizan una acción sobre el fichero de memoria.
- ✓ El formato de los comandos es:

```
volatility --profile "nombre_perfil_volcado" –f "fichero_volcado" plugin
```

- ✓ Como plugins de especial interés:
  - ✓ imageinfo: Si no conocemos el sistema origen, nos indica posibles perfiles candidatos.
  - ✓ pslist: nos muestra la lista de procesos en el momento de la adquisición.
  - ✓ pssccan:
  - ✓ netscan: similar a un netstat.
  - ✓ -h: muestra la ayuda y la lista de plugins disponibles.
  - ✓ --info: igual que -h pero, además, muestra los perfiles disponibles.

https://www.volatilityfoundation.org/

UNIDAD 5 – WINDOWS II – EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

9. Análisis de memoria RAM en Windows. Volatility.

❑Otras herramientas

- ✓ Para el trabajo con memoria de los procesos, podemos “bucear” en la memoria de uno en concreto mediante otros programas, como “strings”, que nos permite buscar cadenas de texto en un volcado de memoria.
- ✓ Strings está disponible en Linux y en Windows a través de Sysinternals.
- ✓ Adicionalmente, podemos realizar búsqueda de ficheros mediante el proceso de carving visto con anterioridad.
- ✓ Para la obtención de un volcado de memoria de una sola aplicación, podemos usar el process monitor nombrado con anterioridad.

FIN UNIDAD

Unidad 5
ARTIFACTS WINDOWS II
EL REGISTRO DE EVENTOS Y OTROS ARTIFACTS

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