*“La intención de este documento es tener preguntas sobre los laboratorios (no aplica para todos) las mismas están respondidas en el correspondiente PDF de dicho Lab, la idea es que sea animen a responderla por si solos”.* Robert Encarnacion

A person in a hoodie typing on a computer

Description automatically generated

**Workshop Windows Forense HackConRD 2024**

**Por**

**RedTeamRD**

**Laboratorio 1.1: Montar imágenes de disco usando Arsenal Image Mounter**

A magnifying glass on a newspaper

Description automatically generated

Una capacidad importante en la informática forense es la capacidad de examinar la evidencia digital contenida dentro de **un formato de imagen forense.**

Arsenal Image Mounter (AIM) es una herramienta gratuita (también hay una versión comercial con características adicionales) que se puede utilizar para montar imágenes de disco forense en un sistema de examen forense. AIM puede montar imágenes de disco en formato **E01, Raw (dd), Advanced Forensic Format 4 (AFF4) y formatos de disco de máquina virtual como VMDK, VHD y OVA.**

AIM monta el contenido de las imágenes de disco como discos completos en Windows, no como comparticiones o particiones como lo hacen algunos otros productos. Las capacidades de montaje de bajo nivel de AIM **proporcionan acceso a artefactos especiales de Windows como copias de sombra de volumen y BitLocker que otros productos no tienen.**

En nuestra máquina virtual, en el Desktop tenemos “DFIR TOOLS”, dentro, tenemos una carpeta llamada “Acquisition Tools”, y entre las herramientas abrimos Arsenal Image Mounter.

**Laboratorio 1.2: Triage imaging con KAPE**



**Objetivos**

La recopilación de evidencia es posiblemente el paso más importante en el ciclo de vida de la evidencia digital. Generalmente, solo tienes una oportunidad para hacerlo bien, y los errores en la recopilación pueden destruir la evidencia.

Cuando respondes a un sistema en vivo, necesitarás actuar rápidamente para capturar la RAM, determinar si la unidad está cifrada y tomar una decisión informada sobre si crear una imagen en vivo o desconectar la energía del sistema. Retrasos o errores por parte del respondiente al incidente pueden resultar en una serie de resultados, incluida la modificación del sistema de archivos, el bloqueo de la pantalla o otros cambios significativos en el sistema.

Realizar una imagen de toda una unidad lleva horas. En investigaciones de alta prioridad, es posible que necesites que uno o más examinadores revisen los datos de una unidad de inmediato.

Realizar imágenes solo de porciones seleccionadas y artefactos de una unidad, aquellas áreas que sabemos tienen el mayor potencial para la información que estamos buscando, y luego proporcionar copias de esa imagen a varios examinadores puede marcar la diferencia en una investigación de rápida evolución. La imagen de triage puede ser seguida por una imagen completa del disco si es posible.

KAPE es una herramienta gratuita que se puede utilizar para dirigirse a archivos específicos, carpetas y artefactos forenses para crear imágenes de triaje. KAPE también puede preprocesar los datos de triaje recopilados mediante la ejecución de herramientas forenses contra los datos recopilados.

En este ejercicio, usaremos varias herramientas para practicar la recopilación de RAM, verificar signos de cifrado en un sistema en vivo y recopilar un conjunto de artefactos forenses de triaje que podamos usar rápidamente para análisis forense.

**Laboratorio 1.4 : User Account Profiling**

A person in a red hoodie sitting at a desk with computers

Description automatically generated

**Objetivos:**

El perfilado y la comprensión de las cuentas de usuario son críticos para asegurarse de no cometer errores fáciles mientras se realiza un análisis más complejo posteriormente. Con el análisis del hive del registro SAM, un analista puede documentar las cuentas de usuario locales asociadas con el sistema, buscar elementos que ayuden a responder preguntas investigativas e identificar anomalías. Podrás determinar cuándo se crearon las cuentas, cuándo iniciaron sesión por última vez e incluso si las cuentas son del nuevo tipo de cuenta "Cloud" de Microsoft

Buscamos el Hive offline en la ruta **F: \C\Windows\System32\Config\SAM**

**Nota: La unidad lógica puede variar.**

Ahora, dentro del Registry Explorer, vamos a navegar hacia **SAM\Domains\Account\Users**  y seleccionamos el Key “Users”

1. ¿Cuántas cuentas de usuario están presentes en este hive SAM?
2. ¿Cuál es el nombre de usuario para la cuenta de Fred Rocba y cuál es su valor de Id de usuario?
3. ¿De qué grupos era miembro la cuenta de Fred Rocba?
4. ¿Cuándo fue la última vez que hizo login la cuenta de fredr?
5. ¿Cuántas de las built-system accounts (RID < 1000) se han utilizado en el sistema?
6. ¿Por qué el Conteo total de inicio de sesión es igual a 0 para la cuenta de fredr?
7. ¿Cuál es el Conteo de Inicios de Sesión Inválidos para la cuenta del Administrador?
8. ¿Por qué la hora del último cambio de contraseña es anterior a la hora de creación de la cuenta de fredr?

**Extra- Checking for MS Accounts**

Los datos en bruto de las cuentas de usuario en el registro SAM se almacenan como subclaves(subkeys) bajo la clave(key) **Users.** Cada cuenta tiene una subclave (subkey) nombrada de acuerdo con la representación hexadecimal de su Identificador Relativo (RID). El valor hexadecimal para RID 1002 (fredr) es **3EA**. Haz clic en esta clave para ver los valores en bruto presentes.

**Haz clic en el valor InternetUserName y observa los datos en bruto en el panel Type Viewer. ¿**

1. ¿Qué cuenta de correo electrónico está vinculada a la cuenta fredr?
2. ¿Es la **cuenta srl-h** una Cuenta de Microsoft? En caso afirmativo, ¿qué correo electrónico está vinculado a esta cuenta?

**Laboratorio 1.5 – System Profiling**

A person sitting at a desk with computers

Description automatically generated

**Objetivos:**

Comprender el sistema que estás examinando es crucial para asegurarse de no cometer errores simples mientras realizas análisis más complejos más adelante. Saber algo tan simple como cuántas interfaces de red existen, la configuración de zona horaria e incluso el nombre del sistema son piezas de información crucial necesarias para analizar un sistema correctamente. Dedica un tiempo aquí y explora la información que se puede extraer de estas bases de datos útiles.

* Perfilar el sistema que estaremos analizando. Identifica el nombre del sistema, la última hora de actualización, la zona horaria y otra información importante del sistema.
* Perfilar las redes a las que el sistema se ha conectado. Identifica las primeras y últimas horas de conexión de las conexiones de red relevantes.

Procedemos a montar el Triage evidence en nuestra ruta

Abrimos Registry Explorer que esta en nuestro Desktop y procedemos a buscar el offline Hive en la siguiente ruta: **F:\C\Windows\System32\Config\SYSTEM**

Nota: Si en dado caso un dirty hive es detectado, le damos a “**yes**”

Click en “OK” para seleccionar transaction logs to replay, y en la misma ruta de SYSTEM, encontraremos SYSTEM.log1 y SYSTEM.log2, seleccionamos ambos y lo abrimos

A screenshot of a computer

Description automatically generated

Le damos OK y lo guardamos en el Desktop o en el disco CASES/Exercises/Registry. Registry Explorer nos pedirá si queremos actualizar el nuevo hive y le damos “OK”.

1. ¿Cuál es el CurrentControlSet? Key: **SYSTEM\Select**
2. Documenta el Nombre de la Computadora del sistema. Key: **SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName** [Hint: **Recuerda usar el ControlSet que identificamos anteriormente**]
3. ¿A qué zona horaria fue configurado por última vez el sistema? Key: **SYSTEM\CurrentControlSet\Control\TimeZoneInformation**
4. **¿Cuándo se apagó o reinició el sistema por última vez? Key**: **SYSTEM\CurrentControlSet\Control\Windows .**
5. Revisa la clave de Interfaces de red para perfilar las conexiones de red más recientes. Key: **SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces** . Observaremos que solo hay una interfaz que mantiene información interesante. Documenta el DhcpDomain para esa interfaz de red

Ahora examinaremos el offline hive SOFTWARE, lo cargamos al Registry Explorer (Si da problemas con Dirty Hive, realizamos los pasos anteriores)

Ve a **SOFTWARE\Microsoft\Windows NT\CurrentVersion** y responde las siguientes preguntas.

1. ¿Qué versión de Windows se está utilizando?
2. ¿Cuál es el ReleaseID y CurrentBuild del sistema operativo?
3. ¿Cuál es el valor InstallDate en formato de tiempo legible para humanos?
4. ¿Quién es el RegisteredOwner?

Ve a la clave **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList** y asegúrate de estar mirando la pestaña del complemento de redes conocidas **(Known networks plugin tab).**

1. ¿Qué redes inalámbricas se han registrado?
2. ¿Cuales WWAN (VPN) fueron registradas?
3. ¿Cuál de las redes identificadas fue almacenada como una red "administrada" (managed)? Las redes administradas suelen ser parte de un dominio de Windows, como una red corporativa. La clave **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures** puede ayudar a hacer esta determinación.

**Lab 1.6**

**NTUSER.DAT Analysis**

A cat looking up at the light

Description automatically generated

**Objetivos:**

El archivo hive NTUSER.DAT está lleno de artefactos extremadamente interesantes y rastreables, y **cada usuario en el sistema tiene uno.** Es importante destacar que esto significa que podemos diferenciar actividades entre cada una de las cuentas de usuario en Windows. Un análisis adecuado del hive NTUSER.DAT de cada usuario permitirá a un investigador identificar la ejecución de programas, la apertura de archivos, la apertura de carpetas y mucho más.

NTUSER.DAT puede contener una gran cantidad de información importante.

* Encuentra artefactos asociados con la Evidencia de Apertura de Archivos y Carpetas, como las claves RecentDocs, OpenSaveMru y ComDlg32.
* Aprende a identificar términos de búsqueda y rutas de archivos que el usuario escribió en el sistema a través de las claves TypedPaths y WordWheelQuery.
* Perfil de actividad de la cuenta e identifica comportamientos del usuario.

Con la evidencia montada (Triage evidence) tal cual en los otros ejercicios, procedemos a abrir el Registry Explorer y cargar el hive NTUSER.DAT : C\Users\fredr\NTUSER.DAT

**WordWheelQuery Key:**

**NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery**

Revisa las búsquedas escritas por la cuenta de Fred Rocba.

1. ¿Qué términos de búsqueda podrían ser relevantes en una investigación de robo de datos?
2. ¿Qué término de búsqueda tiene asociada una marca de tiempo? ¿A qué hora se ejecutó esa búsqueda?

**TypedPaths Key:**

**NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths**

TypedPaths identifica las ubicaciones escritas por el usuario en la barra de direcciones del Explorador de archivos de Windows. Sin embargo, parece que esta función fue utilizada solo de manera esporádica en este sistema.

1. ¿Qué tienen en común todas las entadas?
2. ¿Cuál es la entrada más reciente de TypedPaths? ¿A qué hora fue utilizada?

**RecentDocs**

**Key: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs**

Los registros de tiempo en la clave RecentDocs se identifican mediante listas MRU y las horas de escritura de las claves del registro.

**Revisa la columna Última Apertura de la Extensión e identifica el nombre de archivo relacionado con la marca de tiempo más temprana registrada el 2020-11-14.**

El Sr. Rocba se fue de vacaciones el 10 de noviembre de 2020. De los registros de tiempo disponibles en la columna Última Apertura de la Extensión,

1. ¿cuál es el último elemento abierto en ese día?
2. ¿Cuántas claves BitLocker diferentes se abrieron con esta cuenta? ¿Por qué no tenemos marcas de tiempo disponibles para cada una de estas?

**Office File MRU File MRU Key:**

**NTUSER.DAT\SOFTWARE\Microsoft\Office\16.0\Word\User MRU\ ADAL\_71509F4C9F29E24E25306165B32FE79B68FD54A88446B7C792A3A9D5AB6BB5AE\File MRU**

Los documentos de Microsoft Office rastreados por las claves File MRU tienen dos ventajas principales sobre la clave RecentDocs: información completa de la ruta y marcas de tiempo para cada entrada.

1. ¿Qué letras de unidad se utilizaron para abrir documentos de Word el 14 de noviembre de 2020?

**OpenSavePidlMRU**

Clave OpenSavePidlMRUKey:

**NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU**

La mayoría de los archivos mencionados en OpenSavePidlMRU también están presentes en RecentDocs. Sin embargo, esta es una buena fuente de datos para revisar principalmente porque proporciona información completa de la ruta, que no está disponible en RecentDocs.

Utiliza la información completa de la ruta disponible aquí para buscar archivos abiertos dentro de Google Drive. Filtra la columna Ruta Absoluta por "MyDrive".

* ¿Cuántas entradas hay para archivos abiertos o guardados en este conjunto de carpetas? ¿Ves cómo esta información puede ser más valiosa que simplemente los nombres que proporciona RecentDocs?

**Elimina el filtro en la columna Absolute Path ¿**

1. ¿Cuál es el último archivo abierto o guardado por este usuario?

Ahora intentemos relacionar la información de OpenSavePidlMRU con la información de la aplicación presente en la clave LastVisitedPidlMRU (solo dos claves arriba de la que estás viendo actualmente).

1. ¿Qué aplicación probablemente abrió o guardó el archivo My Computer\D:\ROCBA-SYSTEM\Rocba-Memory.raw?

Key: **NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU**

**Autostart "Run" Keys**

Para finalizar este ejercicio, echemos un vistazo a la infame clave "Run" del archivo NTUSER.DAT. Los elementos en esta clave se ejecutan cada vez que el usuario inicia sesión. Los elementos en esta clave se ejecutan cada vez que el usuario inicia sesión. Por esta razón, esta clave es el lugar más común para que el malware agregue una referencia a sí mismo en un intento de sobrevivir a un reinicio (comúnmente llamado un "mecanismo de persistencia"). Además de buscar malware, esta clave también indica las aplicaciones instaladas por el usuario

Ve a la pestaña Bookmarks y haz clic en el marcador Run.

**Run Key: NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**

**Lab 1.7 Application Execution Analysis**

A person working in a server room

Description automatically generated

**Objetivos:**

La ejecución de aplicaciones es una de las categorías de artefactos más importantes que utilizamos para comprender lo que sucedió en una computadora. Auditar qué aplicaciones estaban presentes y en funcionamiento puede proporcionar una gran perspectiva sobre las actividades del usuario, el tipo de datos que esperar en el sistema, y explicar anomalías que podrían ser causadas por malware o herramientas anti-forenses. Afortunadamente, esta categoría contiene una gran cantidad de artefactos diferentes que pueden demostrar la ejecución de aplicaciones. En este ejercicio exploraremos tres artefactos muy importantes: BAM, UserAssist y Prefetch.

* Exploraremos la clave del registro BAM de Windows 10.
* Decodificaremos los datos ocultos presentes en la clave UserAssist de NTUSER.DAT.
* Examinaremos la gran cantidad de información de ejecución de aplicaciones presente en los archivos de Prefetch de Windows.
* Utilizaremos los metadatos de ejecución de aplicaciones para determinar los tiempos de ejecución y el número de ejecuciones de las aplicaciones.

Al igual que ejercicios anteriores, montamos nuestra imagen (Triage Evidence) y usamos los registros clean de SYSTEM y NTUSER

**BAM!**

BAM es un acrónimo Background Activity Moderator, y la clave del registro correspondiente mantiene una lista simple de aplicaciones ejecutadas y su último tiempo de ejecución

Recuerda que la cuenta fredr tiene un RID de 1002 (según nuestro análisis previo del registro SAM). Por lo tanto, querremos investigar la siguiente clave en el registro SYSTEM:

BAM Key: **SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-528816539-567677750-276746561-1002**

Ordene el contenido de la clave por Tiempo de Ejecución y revise las aplicaciones ejecutadas el 14 de noviembre de 2020 (UTC), el día del incidente en la residencia del Sr. Rocba. Si no está acostumbrado a mirar los nombres de las aplicaciones de Windows, puede haber muchas de las que no está al tanto. Enumere algunas que podrían ser particularmente interesantes para nuestra investigación.

**UserAssist**

UserAssist ha sido durante mucho tiempo un valioso artefacto de Windows para proporcionar una profunda comprensión del uso de aplicaciones. Debido a que está presente en el hive NTUSER.DAT

Abra la siguiente clave:

**NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\ .**

Los dos GUID más comúnmente utilizados en UserAssist son:

**- CEBFF5CD-ACE2-4F4F-9178-9926F41749EA ->** Ejecución de Archivos Ejecutables

**- F4E57C4B-2036-45F0-A9AB-443BCFE33D9F** -> Ejecución de Archivos de Acceso Directo

1. Comenzemos con el GUID que comienza con F4E57 y hagamos clic en la subclave llamada "Count" para activar el complemento de Registry Explorer.

2.Ordena la salida por Nombre del Programa. ¿Qué elementos están anclados en la barra de tareas del usuario? (Pista: Busca {User Pinned}.)

Ahora pasamos al GUID de UserAssist que comienza con **CEBFF** y haz clic en su subclave llamada "Count" para activar el complemento de Registry Explorer

Ordena la salida por "Last Executed" y registra las aplicaciones interesantes que ocurrieron el 14 de noviembre de 2020

Ordena la salida por **Focus Count**. Este valor representa el número de veces que la aplicación fue la ventana principal para el usuario. Los elementos con un conteo de enfoque más alto a menudo representan aplicaciones más comúnmente utilizadas. ¿Qué aplicación de usuario tiene el conteo de enfoque más alto?

Ahora vamos a profundizar en una de las entradas. Examinemos detenidamente la entrada {Windows}\regedit.exe y responde a las siguientes preguntas:

**¿Número de ejecuciones?**

**¿Última hora de ejecución?**

**¿Cuántas veces estuvo en foco? Y ¿Cuál fue el tiempo total de enfoque?**

Ahora tenemos información muy detallada sobre la ejecución de regedit.exe. Si creemos que regedit pudo haber sido utilizado para modificar el registro, podemos utilizar esta información para ver qué se escribió "últimamente" alrededor de este período de tiempo.

Usa Ctrl-F (o Tools -> Find) para abrir el diálogo de búsqueda de Registry Explorer. Bajo Marca de tiempo de última escritura, selecciona Entre y utiliza 2020-11-14 04:39:00 y 2020-11-14 04:45:00 como el período de tiempo a buscar (la última hora de ejecución más algún tiempo de enfoque - no es una ciencia exacta, pero es un buen punto de partida). Haz clic en Buscar.

¿Has notado que la última vez que se escribió en **SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths** está dentro de esta ventana de tiempo? ¿Quizás fue manipulado de alguna manera?

Haz doble clic en el resultado de **SOFTWARE\Microsoft\Windows\CurrentVersion\Applets\Regedit.** Esto debería llevarte a esa clave en RegistryExplorer. ¿A qué ubicación del registro hace referencia el valor LastKey?

**Investigating Prefetch**

Ahora nos alejamos del registro de Windows hacia la sorprendentemente útil carpeta Prefetch. Prefetch sigue las aplicaciones ejecutadas tanto desde la interfaz gráfica como desde la línea de comandos

Win Prefetch View se abre por defecto con el Prefetch del sistema en vivo, lo cual no es interesante para nosotros (pero a veces es útil cuando se practica o se realizan pruebas). Selecciona Opciones -> Opciones avanzadas y luego navega hasta la carpeta Prefetch de nuestra imagen de triaje montada: F:\C\Windows\Prefetch. Haz clic en Aceptar

Realiza una revisión superficial de los archivos prefetch disponibles y luego encuentra BITLOCKERWIZARD.EXE-BC98F555.pf. Responde a las siguientes preguntas:

¿Número de ejecuciones?

¿Última hora de ejecución**?**

Encuentra TSTHEME.EXE-01D23267.pf en tu herramienta WinPrefetchView y perfila su ejecución. TSTHEME es una aplicación interesante ya que se ejecuta en el sistema durante las sesiones de protocolo de escritorio remoto (RDP) entrantes. Es un buen indicador de RDP entrante a una computadora.

**¿Numero de ejecuciones?**

Encuentra MSTSC.EXE-2A83B7D7.pf en tu herramienta WinPrefetchView y perfila su ejecución. MSTSC.exe se utiliza para establecer conexiones salientes de RDP desde un sistema (básicamente lo contrario de TSTHEME.exe). Perfila el uso de MSTSC.exe en este sistema:

**¿Número de ejecuciones?**

**Prefetch Parsing with PECmd**

Ahora practicaremos con la herramienta de análisis de prefetch PECmd de Eric Zimmerman. Esta es una herramienta basada en línea de comandos que permite el análisis rápido y exhaustivo de grandes cantidades de archivos Prefetch.

Abre un Símbolo del sistema de administrador encontrando el icono en el lado izquierdo de tu escritorio.

A screen shot of a computer

Description automatically generated

Revisa la salida de PECmd para SDELETE.EXE-0E837E93 y responde las siguientes preguntas.

**¿Número de ejecuciones?**

**¿Cuál es la fecha de todas las ejecuciones?**

**¿Ves alguna información en la salida que pueda indicar quién ejecutó la herramienta y para qué se usó para borrar?**

Para finalizar esta sección, ejecuta PECmd contra cada archivo Prefetch adquirido del sistema. Para ello, utilizarás la opción -d para señalar al directorio Prefetch, la opción -q para el modo silencioso (menos salida) y --csv para la ubicación de la salida en formato CSV:

pecmd.exe -d F:\C\Windows\prefetch -q --csv D:\Exercises\Prefetch



En la misma carpeta de WInPrefech Viewer (DFIR TOOLS -- > Artifact Tools) abrimos Timeline Explorer



A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Ordena la salida por la columna "Run Time" y revisa la salida de la línea de tiempo de PECmd. Este archivo tiene cada ejecución registrada por Prefetch en orden cronológico. Puede ser muy útil para ver las relaciones entre diferentes herramientas y para perfilar las acciones del usuario en un sistema. Filtra la columna "Nombre del ejecutable" para sdelete.

Enumera las ubicaciones desde las que se ejecutó sdelete:

**¿Cuál es el período de tiempo total de la actividad conocida de sdelete en este sistema?**