Adquisición de Análisis Forense

Nombre Creador:
Yeray Almoguera Gonzalez

Fecha de Creación:
Jueves, 24 de Octubre de 2024

Índice

Introducción

En el contexto de la presente investigación y con el objetivo de preservar evidencia digital esencial para su posterior análisis, se ha llevado a cabo un proceso de adquisición forense de información contenida en los sistemas de almacenamiento del equipo bajo estudio. Este procedimiento se realiza siguiendo los estándares y buenas prácticas establecidos para la preservación de evidencia digital, garantizando la integridad y autenticidad de los datos obtenidos.

La adquisición se ha limitado a capturar la memoria volátil y no volátil del sistema, con un enfoque específico en áreas de relevancia para la investigación, entre ellas carpetas seleccionadas del sistema de archivos y el contenido de la memoria RAM en un momento específico. Para asegurar la fiabilidad del procedimiento, se emplearon herramientas especializadas que permiten realizar capturas sin afectar la estructura original de los datos. Además, se han generado y documentado los valores hash correspondientes a cada adquisición para verificar la integridad de la información y asegurar su trazabilidad a lo largo de las fases de análisis y custodia de la evidencia.

Este informe documenta detalladamente cada fase del proceso de adquisición, describiendo las herramientas utilizadas, los métodos de captura, y los procedimientos de verificación de integridad empleados. Las secciones siguientes incluyen los detalles específicos de la recolección, los resultados del análisis de integridad, y la documentación de las rutas de evidencia, todo ello en conformidad con los requisitos técnicos y legales aplicables en el análisis forense digital.

Adquisición de memoria volátil

Introducción:

Con el fin de preservar y analizar evidencia digital relacionada con la memoria volátil del sistema, se procedió a la adquisición de la información contenida en la memoria RAM, un paso fundamental en el análisis forense debido a que esta memoria contiene datos temporales y en ejecución que pueden ser críticos en una investigación. Para dicha tarea, se utilizó la herramienta especializada Belkasoft Live RAM Capturer, seleccionada por su capacidad para realizar adquisiciones rápidas y efectivas sin necesidad de instalación en el sistema objetivo.

Descripción de la Herramienta:

Belkasoft Live RAM Capturer es una aplicación diseñada para minimizar el impacto en el sistema gracias a su tamaño reducido y a su ejecución directa desde una unidad flash USB, lo cual permite iniciar el proceso de adquisición en cuestión de segundos. A diferencia de otras herramientas que operan en modo usuario, Belkasoft Live RAM Capturer cuenta con controladores específicos para arquitecturas de 32 bits y 64 bits, permitiéndole operar a nivel de kernel con privilegios elevados. Esto garantiza un acceso profundo y directo a la memoria, optimizando la integridad de los datos capturados. Además, la compatibilidad de esta herramienta con versiones comunes de sistemas operativos Windows, junto con la posibilidad de utilizar dispositivos USB con protección contra escritura, ofrece un método confiable para preservar la memoria sin alteraciones.

Proceso de Adquisición:

Durante la operación, el contenido de la memoria RAM fue capturado en un archivo con formato .mem, el cual ha sido adjuntado junto a este informe para su posterior análisis forense. El archivo obtenido representa una imagen completa de la memoria volátil del sistema en el momento de la adquisición, asegurando que los datos críticos no se pierdan ni se alteren. El proceso de volcado de memoria fue completado en un entorno controlado, preservando la integridad del sistema y minimizando la intrusión en el mismo.

Conclusión:

La adquisición de la memoria volátil fue realizada exitosamente utilizando Belkasoft Live RAM Capturer, garantizando la preservación de la evidencia en conformidad con las mejores prácticas de ciberseguridad y análisis forense. La documentación asociada y el archivo de la imagen de memoria han sido asegurados para su análisis futuro. Este informe documenta los detalles relevantes relacionados con la adquisición de la evidencia, asegurando el cumplimiento de los estándares de integridad y trazabilidad requeridos en un proceso forense. En las tablas a continuación se detallan la información general del caso, la ruta de la evidencia, su integridad mediante el cálculo del hash, los datos relativos a las marcas temporales (Mtime) y una breve descripción del objeto de análisis. Este informe documenta la adquisición de evidencia digital de acuerdo con los estándares aceptados en el análisis forense, garantizando la fiabilidad de la evidencia para futuros procedimientos investigativos.

Información General

Campo	**Valor**
Número de caso:	241024
Investigador:	Yeray Almoguera Gonzalez
Fecha y hora de recolección:	Jueves, 24 de Octubre de 2024, 12:02:59 (UTC+1)

Ruta de la Evidencia

Campo	**Valor**
Ubicación física:	Disco duro #024
Ruta del sistema:	Memoria RAM

Hash no Alterado

Campo	**Valor**
Algoritmo utilizado:	SHA-256
Valor hash:	ddec53db9a734a01064d6ccdc9cfd5bd4fcaeb56acafa3e08e3b657621ded95f

Mtime (Tiempo de Modificación)

Campo	Valor
Fecha:	Jueves, 24 de Octubre de 2024
Hora:	12:03:59 (UTC+1)

Archivos Íntegros: Evidencias Volatiles

Adquisición de memoria no volátil

Introducción:

Con el fin de preservar y analizar evidencia digital contenida en la memoria no volátil del sistema, se procedió a la adquisición de datos en el dispositivo de almacenamiento principal. Esta adquisición es crítica en el análisis forense, ya que permite conservar información persistente que puede incluir archivos de sistema, registros de actividad, y otros datos esenciales en la investigación. Para dicha tarea, se empleó la herramienta especializada FTK Imager, seleccionada por su capacidad de realizar adquisiciones sin alterar el contenido original del dispositivo.

Descripción de la Herramienta:

FTK Imager es una aplicación diseñada para realizar capturas forenses en unidades de almacenamiento sin modificar el contenido del dispositivo original. Esta herramienta permite crear imágenes de disco de tipo E01 y RAW, garantizando que el proceso sea lo menos intrusivo posible. Además, su compatibilidad con sistemas de archivos comunes y su habilidad para calcular hash MD5 y SHA-1 durante la adquisición aseguran tanto la integridad como la autenticidad de la evidencia obtenida. Para esta adquisición, FTK Imager fue ejecutado desde un medio USB protegido contra escritura, lo cual minimiza cualquier riesgo de alteración en el sistema.

Proceso de Adquisición:

Durante la operación, se capturó una imagen completa del dispositivo de almacenamiento en un archivo de formato AD1, el cual se encuentra adjunto a este informe para su posterior análisis forense. El proceso incluyó la verificación de integridad mediante el cálculo de los hashes MD5 y SHA-1 antes y después de la adquisición, confirmando así la preservación de los datos sin alteración alguna.

Conclusión:

La adquisición de la memoria no volátil fue realizada exitosamente utilizando FTK Imager, cumpliendo con los protocolos de preservación de evidencia digital y las mejores prácticas forenses. La documentación correspondiente y el archivo de imagen del dispositivo han sido asegurados para análisis futuros. Este informe documenta los detalles relacionados con la adquisición de la evidencia digital, cumpliendo con los estándares de integridad y trazabilidad requeridos en un proceso forense. Las tablas a continuación contienen información sobre el caso, la ruta de la evidencia, los resultados de la verificación de integridad mediante los valores de hash y los detalles relativos a las marcas temporales (Mtime). Este informe asegura la fiabilidad de la evidencia para procedimientos investigativos futuros.

Información General

Campo	**Valor**
Número de caso:	241024
Investigador:	Yeray Almoguera Gonzalez
Fecha y hora de recolección:	Sábado, 26 de Octubre de 2024, 21:38:53 (UTC+1)

Ruta de la Evidencia

Campo	**Valor**
Ubicación física:	Disco duro #025
Ruta del sistema:	Disco Duro Interno, SSD M.2

Hash no Alterado

Campo	**Valor**
Algoritmo utilizado:	MD5, SHA1
Valor hash (MD5):	f949d1902925f2067e680237f3276803
Valor hash (SHA1):	ffeba2817312a6030d1dcf3d98ff687a4c8482fd

Mtime (Tiempo de Modificación)

Campo	Valor
Fecha:	Jueves, 25 de Octubre de 2024
Hora:	21:40:16 (UTC+1)

Archivos Íntegros: Evidencias No Volatiles