Práctica 3

Parte A. Adquisición de Elementos Volátiles sobre Windows 7

Máquina utilizada:

- Win7-32b-ElementosVolatiles.ova (alumno/abc123.)

1. Se sospecha que el usuario alumno ha estado realizando actividades anómalas dentro de la empresa.
   - Utilizando los comandos y herramientas aprendidos, deberás de encontrar indicios que lo demuestren.
   - Almacena los resultados anteriores en la carpeta EvidenciasDigitales_131021.zip y extrae el resumen hash del fichero *.zip* para garantizar la integridad de los datos. Como funciones de hash puedes utilizar *sha256* y *sha512*.

Se adjuntan los ficheros *`2022-02-21-08.34.54,31.zip`* que contiene toda la información extraída por comandos, y los ficheros de suma de verificación *`2022-02-21-08.34.54,31-hash.sha256`* y *`2022-02-21-08.34.54,31-hash.sha512`*.

Se han encontrado evidencias de las actividades anómalas reportadas, ya que se puede comprobar en el historial de búsqueda del navegador que ha buscado términos como 'Como crackear servidor empresa' y 'Como robar'.

2. Posteriormente utiliza *RedLine* para recolectar las principales evidencias en las cuales hemos encontrado información valiosa en el análisis anterior.
   - La herramienta está disponible para descarga en el siguiente enlace.
   - Enlace al manual de usuario.
   - Ejemplo de uso en el canal de Alonso Caballero en Youtube (a partir del min. 13). Enlace.

3. Indica para qué son útiles las funciones de hash en un análisis forense. Aplica las funciones sha256 y sha512 a los ficheros generados en el apartado 1.

Son útiles para tener una suma de verificación del fichero, que asegura la integridad de datos del mismo.