Proyecto Final – Informática Forense

Análisis forense de un disco duro

Ronny Infante Herrera

Universidad Latinoamericana de Ciencia y Tecnología

Prof. Dennis Duran Cespedes

23 de diciembre del 2023

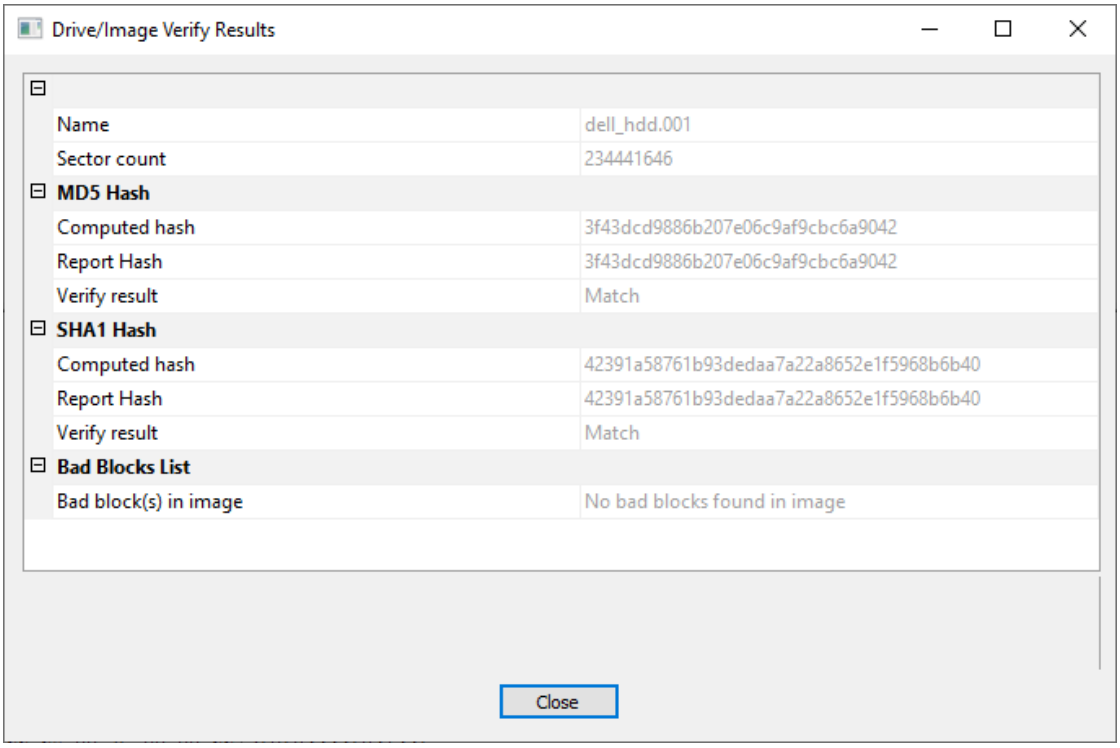
1. Dispositivo a analizar.

El dispositivo para analizar es un disco duro tomado de una computadora que un cliente dejo abandonada.

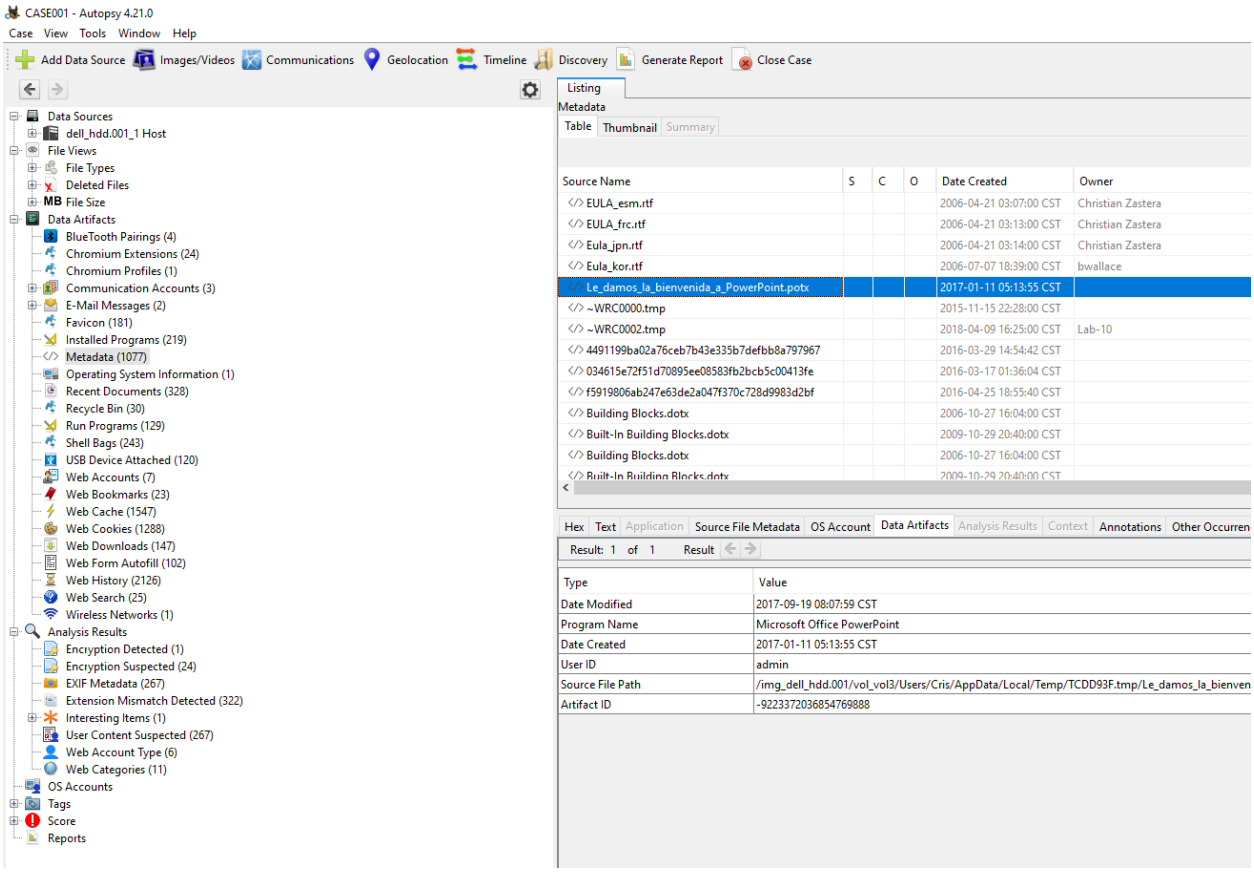
2. Herramientas utilizadas.

Las herramientas utilizadas fueron las siguientes:

Para realizar el hash inicial del disco duro, creación de la imagen del disco duro y comparación del hash de la imagen vs la del disco duro se utilizó AccessData FTK Imager



Para el análisis del disco duro y la generación del reporte se utilizó Autopsy 4.21.0



3. **Resultados.**

Informe Final de Análisis Forense

Número de Caso: CASE001
Fecha: 23/Dic/2023

Agencia Investigadora: ULACIT

Oficial Investigador: Ronny Infante Herrera

Resumen: Se ha completado el análisis forense del disco duro asociado con el Número de Caso CASE001. La investigación tuvo como objetivo evaluar el contenido digital, posibles amenazas de seguridad y actividades ilícitas asociadas con el usuario.

Hallazgos Clave:

1. **Visión General:**
    - El disco duro bajo investigación pertenecía a Cris y se utilizó en una computadora DELL.
2. **Integridad de los Datos:**
    - La integridad de los datos se confirmó mediante la verificación de hash antes y después de la creación de la imagen. No se encontraron discrepancias.
3. **Análisis del Sistema de Archivos:**
    - El análisis del sistema de archivos no reveló evidencia de manipulación, corrupción o actividades maliciosas.
    - El sistema operativo que tenía el disco instalado es: Windows 7 Professional Service Pack 1.
4. **Análisis de la Línea de Tiempo:**
    - Un análisis de la línea de tiempo de creación, modificación y acceso de archivos no mostró patrones inusuales o sospechosos.

5. **Búsquedas por Palabras Clave:**
    - Se realizaron búsquedas por palabras clave para identificar cualquier contenido indicativo de actividades ilícitas. No se encontró tal contenido.
6. **Análisis del Registro:**
    - El examen del registro de Windows no reveló entradas anormales ni signos de actividad maliciosa.
7. **Conexiones de Red:**
    - El análisis de información relacionada con la red, incluidos los registros de conexiones, no indicó ninguna actividad de red no autorizada o sospechosa.
8. **Inventario de Software:**
    - Un examen exhaustivo del software instalado no reveló aplicaciones maliciosas o no autorizadas, excepto por una utilidad utilizada para la activación ilegal de Microsoft Office.
9. **Software no Licenciado:**
    - El único hallazgo notable fue la presencia de una utilidad diseñada para la activación no autorizada de Microsoft Office.

Conclusión: Según el análisis forense realizado en el disco duro, se determina que el contenido digital es consistente con un uso normal. No se identificaron evidencias de actividades maliciosas, violaciones de seguridad o manipulación de datos, excepto por la utilidad de activación no autorizada de Office.

Recomendaciones:

1. **Educación y Conciencia:**
    - Realizar capacitación en concienciación de seguridad para empleados para enfatizar los riesgos asociados con el uso de software no autorizado.

2. **Aplicación de Políticas:**
    - Reforzar las políticas organizativas con respecto al uso y licenciamiento de software. Recordar a los empleados la importancia del cumplimiento.
3. **Monitoreo Periódico:**
    - Implementar monitoreo y auditorías periódicas de las instalaciones de software para identificar y prevenir el uso de aplicaciones no licenciadas o no autorizadas.

Conclusión: El análisis forense del disco duro concluye que no hay evidencia de conducta indebida y el sistema se considera limpio, excepto por la utilidad no autorizada de activación de Office. Las acciones recomendadas buscan mejorar la conciencia y el cumplimiento de las políticas organizativas.