



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.

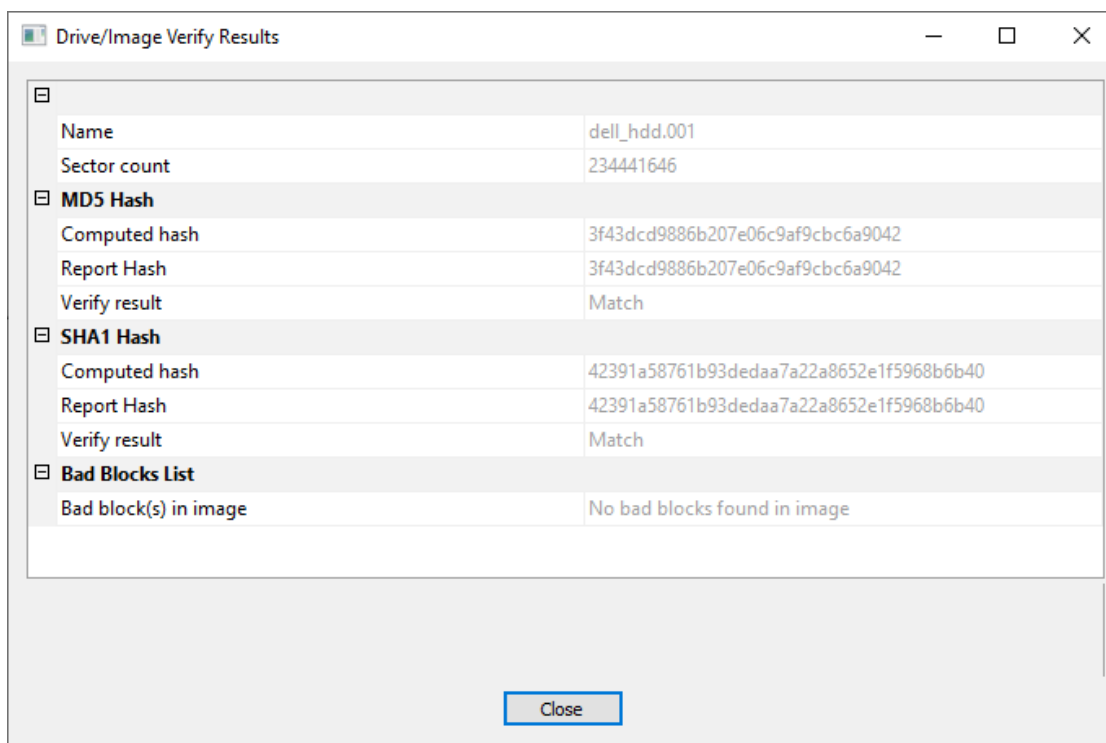
El dispositivo para analizar es un disco duro tomado de una computadora que un cliente dejo abandonada.



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

CASE001 - Autopsy 4.21.0
Case View Tools Window Help

Add Data Source
 Images/Videos
 Communications
 Geolocation
 Timeline
 Discovery
 Generate Report
 Close Case

Data Sources
 dell_hdd.001_1 Host
 File Views
 File Types
 Deleted Files
 MB File Size
 Data Artifacts
 Bluetooth Pairings (4)
 Chromium Extensions (24)
 Chromium Profiles (1)
 Communication Accounts (3)
 E-Mail Messages (2)
 Favicon (181)
 Installed Programs (219)
 Metadata (1077)
 Operating System Information (1)
 Recent Documents (328)
 Recycle Bin (30)
 Run Programs (129)
 Shell Bags (243)
 USB Device Attached (120)
 Web Accounts (7)
 Web Bookmarks (23)
 Web Cache (1547)
 Web Cookies (1288)
 Web Downloads (147)
 Web Form Autofill (102)
 Web History (2126)
 Web Search (25)
 Wireless Networks (1)
 Analysis Results
 Encryption Detected (1)
 Encryption Suspected (24)
 EXIF Metadata (267)
 Extension Mismatch Detected (322)
 Interesting Items (1)
 User Content Suspected (267)
 Web Account Type (6)
 Web Categories (11)
 OS Accounts
 Tags
 Score
 Reports

Listing
Metadata
Table Thumbnail Summary

Source Name	S	C	O	Date Created	Owner
</> EULA_esm.rtf				2006-04-21 03:07:00 CST	Christian Zastera
</> EULA_frc.rtf				2006-04-21 03:13:00 CST	Christian Zastera
</> Eula_jpn.rtf				2006-04-21 03:14:00 CST	Christian Zastera
</> Eula_kor.rtf				2006-07-07 18:39:00 CST	bwallace
Le_damos_la_bienvenida_a_PowerPoint.potx				2017-01-11 05:13:55 CST	
</> -WRC0000.tmp				2015-11-15 22:28:00 CST	
</> -WRC0002.tmp				2018-04-09 16:25:00 CST	Lab-10
</> 4491199ba02a76ceb7b43e335b7defbb8a797967				2016-03-29 14:54:42 CST	
</> 034615e72f51d70895ee08583fb2bcb5c00413fe				2016-03-17 01:36:04 CST	
</> f5919806ab247e63de2a047f370c728d9983d2bf				2016-04-25 18:55:40 CST	
</> Building Blocks.dotx				2006-10-27 16:04:00 CST	
</> Built-In Building Blocks.dotx				2009-10-29 20:40:00 CST	
</> Building Blocks.dotx				2006-10-27 16:04:00 CST	
</> Built-In Building Blocks.dotx				2009-10-29 20:40:00 CST	

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 1 of 1 Result

Type	Value
Date Modified	2017-09-19 08:07:59 CST
Program Name	Microsoft Office PowerPoint
Date Created	2017-01-11 05:13:55 CST
User ID	admin
Source File Path	/img_dell_hdd.001/vol_vol3/Users/Cris/AppData/Local/Temp/TCDD93F.tmp/Le_damos_la_bienven
Artifact ID	-9223372036854769888



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.