



Universidad de las Fuerzas Armadas ESPE Unidad de Educación a Distancia

Integrantes:

Rubén González

José Mejía

Silvia Yunga

Tutor:

Ing. Geovanni Ninahualpa


2023

Grupo 1

NRC:10528

**Análisis forense
sistemas muertos**

1. Desarrollo en formato indicado en “NRCXXXX_P2_LAB1.PDF”

 DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN		
CARRERA EN LÍNEA: Ingeniería en Tecnologías de la Información	GUÍA No. 01	TIEMPO ESTIMADO: 2h
ASIGNATURA: Informática Forense	FECHA:	
TÍTULO: Análisis Forense de Sistemas Muertos.	DOCENTE: Ing. Geovanni Ninahualpa, Mgtr.	
OBJETIVO DE APRENDIZAJE Conocer, identificar he implementar las acciones que se deben llevar a cabo posterior a un incidente de seguridad, mediante el uso de herramientas de análisis forense y gestión de incidentes que permitan obtener evidencias que describan el cometimiento del mismo mediante un informe. DESCRIPCIÓN / CASO En la empresa "Tecnologías y Sistemas", el jefe de ventas, Andrés Simbaña informa a la administración sobre la pérdida de información referente a cartera de clientes, misma que se encontraba en el archivo nombrado "clientes2023.xlsx", de la computadora codificada "TYS005". El Sr. Simbaña informa que con fecha 05 de mayo de 2023 se percató del incidente, también indica que hasta 03 de mayo 2023 el colaborador Guillermo Morales trabajó normalmente con esta información, ya que el 04 de mayo 2023 la empresa desvinculó al Sr. Morales, por lo que se observa que posterior a su salida el archivo "clientes2023.xlsx" ya no se encontraba. Adicionalmente se han recibido llamadas telefónicas de los clientes de la empresa, señalando que de otra empresa denominada "Morales Tech", el Sr. Morlaes (antiguo colaborador), les esta ofertando productos similares a los que la empresa comercializa. Esto hace sospechar a la administración, que esta persona posee el archivo con la información de los clientes y la esta utilizando para su beneficio. La Administración levantó una denuncia de robo de información, llevando el caso a la justicia, la cual incautó y realizó el secuestro de un equipo informático de la empresa "Morales Tech", cuyo propietario es el hermano del ex colaborador y de una pendrive propiedad del ex colaborador, que adicionalmente auguraba no conocer nada del tema. Con este antecedente y dentro del marco legal vigente, se inicia la investigación y se procede al análisis de la evidencia en el pendrive del supuesto acusado. El dispositivo a indagar entregado tiene el siguiente código de seguridad: MD5: (Obtener código y registrarlo en este espacio)		

2. Descripción de generalidades de un sistema muerto

Una "generalidad de un sistema muerto" no es un término técnico o conceptual común en el lenguaje general o en campos específicos como la informática o la ingeniería. Sin embargo, puedo proporcionarte información sobre sistemas muertos en un contexto general.

Un sistema muerto generalmente se refiere a un sistema que ha dejado de funcionar, operar o mantener actividad. Puede aplicarse a diversas áreas, como la tecnología, la biología o incluso a conceptos más abstractos.

Por ejemplo, en informática, un sistema muerto podría referirse a una computadora o un programa que ha dejado de responder o funcionar correctamente. En biología, podría referirse a un organismo que ha perdido todas sus funciones vitales y ya no está vivo. En un sentido más abstracto, podría aplicarse a una organización o proyecto que ha dejado de existir o de tener actividad.

En resumen, el término "sistema muerto" hace referencia a algo que ha perdido su funcionamiento, actividad o vitalidad, y generalmente se aplica en diferentes contextos para describir situaciones en las que ya no hay vida, operatividad o funcionamiento. Si tienes un contexto específico en mente, estaré encantado de proporcionarte información más detallada.

En el contexto del caso presentado, el término "sistema" se refiere a la estructura organizativa y tecnológica utilizada por la empresa "Tecnologías y Sistemas" para gestionar y almacenar información clave, así como para facilitar la comunicación con los clientes. Esto incluye el sistema de almacenamiento de datos, la computadora identificada como "TYS005", posiblemente parte de un entorno informático más amplio, y los mecanismos de comunicación que la empresa utiliza para interactuar con sus clientes. La mención de un archivo específico, "clientes2023.xlsx", sugiere la existencia de un sistema para gestionar la cartera de clientes, mientras que las acciones legales y de investigación muestran un sistema de control y seguridad.

3. Descripción y análisis del marco legal vigente tipificado sobre este caso en el COIP

Marco legal vigente tipificado sobre este caso en el COIP

El Código Orgánico Integral Penal (COIP) es la legislación penal vigente en Ecuador desde el 10 de febrero de 2014. Este código establece los delitos y las penas que se aplican en Ecuador, así como los procedimientos para juzgar y sancionar a los infractores de la ley.

En el caso de los delitos de violencia intrafamiliar, el COIP establece una serie de penas que van desde la privación de libertad hasta la prohibición de acercarse a la víctima. La pena impuesta dependerá de la gravedad del delito y de las circunstancias de su comisión.

El código integral penal del Ecuador (COIP) en su sección tercera presenta los **DELITOS INFORMÁTICOS CONTRA LA SEGURIDAD DE LOS ACTIVOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN** los siguientes artículos sobre los delitos informáticos

- Artículo 229: revelación ilegal de bases de datos
- Artículo 230: interceptación ilegal de datos
- Artículo 232: Ataque a la integridad de sistemas informáticos

También es importante mencionar los siguientes artículos los cuales están relacionados con las ciencias forenses, ya que mencionan la parte de la cadena de custodia en cuanto a la evidencia, los que se pueden aplicar en un juicio por delito informático

- Artículo 449: atribuciones: atribuciones del personal de sistema especializado integral de la investigación, medicina legal y ciencias forenses.
- Artículo 456: Cadena de custodia
- Artículo 47: criterios de valoración
- Artículo 499: Medios de Prueba: reglas generales: El documento
- Artículo 500: contenido digital

Como se conoce el COIP regula las cuestiones penales en el país dentro de esto tenemos el tratamiento que se da a el análisis forense de sistemas muertos en el ámbito legal, es así que el análisis de los sistemas muertos se refiere a la aplicación de técnicas y procedimientos para investigar delitos relacionados con sistemas y tecnologías de la información. Esto incluye la recuperación, preservación y análisis de datos digitales almacenados en dispositivos electrónicos y sistemas informáticos, los mismo que Los procedimientos de análisis forense buscan recopilar pruebas digitales que puedan ser presentadas en un tribunal como evidencia de la comisión de un delito.

Marco legal vigente tipificado sobre este caso en el COIP

El artículo 202 del Código Orgánico Integral Penal (COIP) tipifica el delito de hackeo. El artículo establece que quien ingrese sin autorización a un sistema informático o telemático, será sancionado con prisión de seis meses a tres años.

El artículo 203 del COIP tipifica el delito de extorsión. El artículo establece que quien exija a una persona una cantidad de dinero u otra cosa de valor, mediante amenazas o violencia, será sancionado con prisión de dos a cinco años.

El artículo 204 del COIP tipifica el delito de robo de información confidencial. El artículo establece que quien sustraiga, acceda o utilice información confidencial de una persona o entidad, será sancionado con prisión de uno a tres años.

Estos son solo algunos ejemplos de delitos que pueden ser resueltos mediante la informática forense. La informática forense es una herramienta poderosa que puede ser utilizada para ayudar a la Policía Nacional y a las Fuerzas del Orden a resolver delitos y a proteger a las víctimas.

4. Recopilación de la evidencia mediante el uso del software FTK IMAGER:

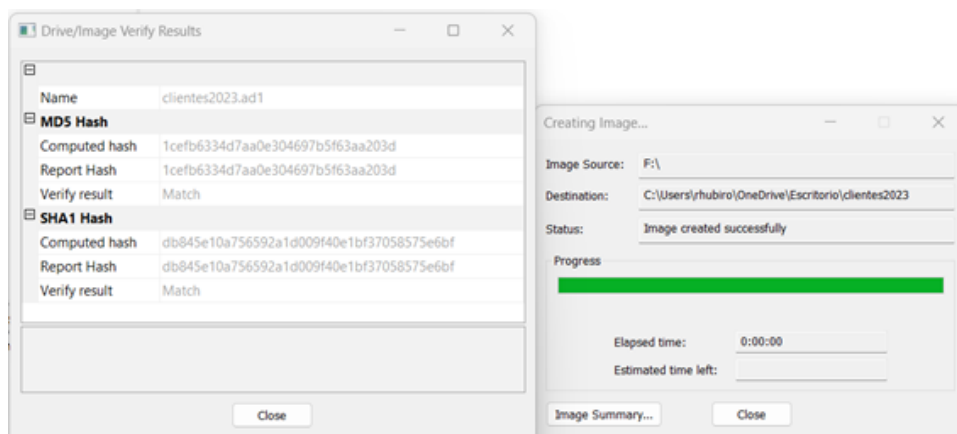
En la investigación forense digital. FTK IMAGER, una herramienta ampliamente utilizada en este ámbito permite crear una copia forense de la información almacenada en medios digitales, como discos duros o dispositivos USB, preservando la integridad de los datos originales. En el contexto de la pérdida de información en "Tecnologías y Sistemas", los investigadores podrían haber utilizado FTK Imager para realizar una copia bit a bit del archivo "clientes2023.xlsx" desde la computadora codificada "TYS005" o cualquier otro medio de almacenamiento

relevante. Esta copia forense asegura que los datos originales permanezcan intactos durante el proceso de análisis y evita cualquier alteración accidental.

Una vez creada la imagen forense del archivo con FTK IMAGER, los investigadores tendrían una réplica exacta y verificable del contenido original. Esto les permitiría llevar a cabo un análisis detallado para identificar cualquier evidencia relevante, como la fecha y hora de creación o modificación, así como cualquier actividad sospechosa relacionada con el archivo. La imagen forense también serviría como un respaldo seguro para futuras investigaciones o acciones legales. En resumen, la recuperación de la imagen del archivo utilizando FTK Imager es un paso crucial en la investigación forense digital, garantizando la preservación de la evidencia y facilitando un análisis exhaustivo de los eventos relacionados con la pérdida de información.

Para el presente laboratorio se utilizó el software de evidencia forense FTK IMAGER 4.7.1.2, tanto para la obtención de la imagen del archivo cuyos metadatos se quiere obtener como para la creación de la imagen copia para uso en el análisis forense.

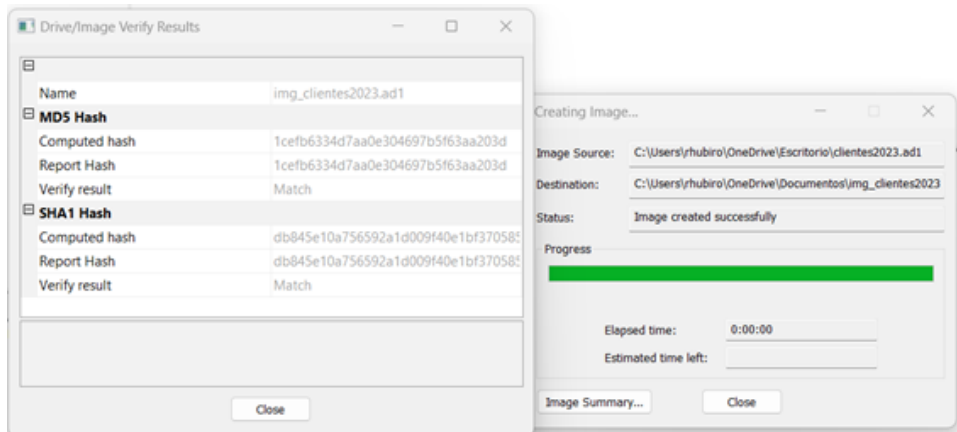
Obtención del archivo imagen con el software FTK IMAGER 4.7.1.2



MD5: 1cefb6334d7aa0e304697b5f63aa203d

SHA1: db845e10a756592a1d009f40e1bf37058575e6bf

Obtención del archivo copia del archivo imagen original.



MD5: 1cefb6334d7aa0e304697b5f63aa203d

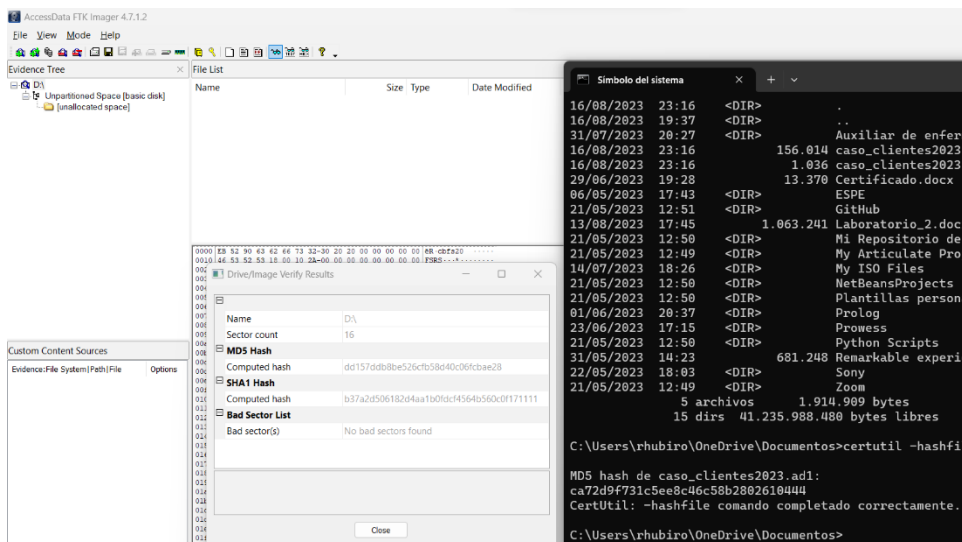
SHA1: db845e10a756592a1d009f40e1bf37058575e6bf

Como se puede ver, en ambas capturas tanto el MD5 como el SHA1 tienen los mismos valores.

5. Identificación y preservación de la evidencia mediante:

Mediante FTK Imager, la identificación y preservación de evidencia se logran al crear una imagen forense exacta de los datos relevantes. Esta herramienta asegura que los archivos y metadatos originales se mantengan intactos durante la recolección, lo que es esencial para garantizar la validez y admisibilidad de la evidencia en investigaciones legales y forenses.

Se carga la imagen desde la unidad virtual virtual D: creada por el programa de análisis forense FTK IMAGER 4.7.1.2 y se observa que no coincide el HASH, por lo que se realiza un nuevo cálculo del MD5 desde el CMD.



MD5: dd157ddb8be526cfb58d40c06fcbac28

SHA1: b37a2d506182d4aa1b0fddf4564b560c0f171111

6. Análisis de la evidencia.

El análisis de evidencia con FTK Imager implica examinar en detalle la imagen forense creada previamente. Esta herramienta proporciona capacidades de búsqueda, filtrado y visualización que permiten a los investigadores explorar los archivos y metadatos de manera exhaustiva. Se pueden utilizar palabras clave, filtros de fecha y otros criterios para localizar información relevante dentro de la imagen. Además, FTK Imager permite examinar estructuras de carpetas, ver documentos y hojas de cálculo, así como obtener vistas previas de archivos multimedia. Con estas funcionalidades, los investigadores pueden identificar patrones, anomalías y pistas que podrían ayudar a esclarecer los eventos relacionados con el caso en cuestión.

También se realiza un cálculo de MD5 desde la línea de comando del Windows y este cálculo si bien coincide con otro obtenido en línea, sin embargo, difieren del MD5 calculado al sacar la imagen original y la imagen copia para el análisis forense, como se evidencia en las capturas de pantalla a continuación:

```
C:\Users\rhubiro\OneDrive\Documentos>certutil -hashfile caso_clientes2023.ad1 MD5

MD5 hash de caso_clientes2023.ad1:
ca72d9f731c5ee8c46c58b2802610444
CertUtil: -hashfile comando completado correctamente.

C:\Users\rhubiro\OneDrive\Documentos>
```

MD5: ca72d9f731c5ee8c46c58b2802610444

MD5 Encrypt File MD5 Checksum SHA1 Encrypt File SHA1/SHA256 Checksum

Select File C:\fakepath\caso_clientes2023.ad1 MD5 Generate

File MD5 Value:

Execution process:

Generate time: 54ms
Generate success, MD5 checksum: ca72d9f731c5ee8c46c58b2802610444
Load Data: the part 1, total 1 parts
Generate start, File name: caso_clientes2023.ad1

Haciendo el cálculo de MD5, para el archivo caso_clientes2023.ad1 (copia del archivo imagen original) desde la siguiente página: <https://en.metools.info/enencrypt/dt104.html>

MD5: ca72d9f731c5ee8c46c58b2802610444

Este último valor es idéntico al obtenido mediante línea de comandos en Windows, pero, sigue siendo diferente del que tenía la imagen original y la copia para el análisis forense.