IPSA Scientia

Revista Científica Multidisciplinaria
ISSN: 2711-4406 | e-ISSN:2744-8355
Octubre-Diciembre 2023, Vol. 8, Nro. 4, pp. 37-52

Artículo de Investigación

Implementación de la metodología para el análisis forense de imágenes de unidades de almacenamiento

Implementation of the methodology for forensic analysis of storage unit images

ROJAS-ROSADO, Junior[1]
Universidad Técnica de Esmeraldas "Luis Vargas Torres", Esmeraldas, Ecuador

PATIÑO-ROSADO, Susana[2]
Universidad Técnica de Esmeraldas "Luis Vargas Torres", Esmeraldas, Ecuador

SACÓN KLINGER, Héctor[3]
Universidad Técnica de Esmeraldas "Luis Vargas Torres", Esmeraldas, Ecuador

Autor corresponsal: *susana.patino.rosado@utelvt.edu.ec*

Recibido: 11-02-2023**;** ***Aceptado:*** 27-12-2023**;** ***En línea:*** 31-12-2023

DOI: https://doi.org/10.62580/ipsc.2023.8.6

Cómo citar este artículo:
Rojas-Rosado, J., Patiño-Rosado, S. & Sacón-Klinger, H. (2023). Implementación de la metodología para el análisis forense de imágenes de unidades de almacenamiento. *IPSA Scientia, revista científica multidisciplinaria, 8*(4), 37-52. https://doi.org/10.62580/ipsc.2023.8.6

Resumen **–** El objetivo principal de este artículo es presentar una metodología propuesta para llevar a cabo investigaciones forenses informáticas de manera estructurada y efectiva. La metodología se divide en cuatro fases principales: identificación, conservación, análisis y presentación de la evidencia digital. Se enfoca la fase de identificación en asegurar la escena del incidente y organizar los objetos encontrados, incluyendo pruebas físicas y lógicas; durante la fase de conservación se garantiza que la evidencia digital se mantenga en su estado original utilizando técnicas como la copia bit a bit y la adquisición de datos en tiempo real para preservar la información de manera efectiva; la fase de análisis se lleva a cabo en un laboratorio forense y utiliza herramientas específicas para investigar la evidencia digital; y finalmente, la fase de presentación de informes se divide en un informe técnico y un informe ejecutivo, que describen los métodos utilizados, los resultados obtenidos y las conclusiones. Para garantizar la eficacia y precisión de la metodología propuesta, esta fue evaluada por tres expertos en Seguridad Informática de la Universidad de la Rioja mediante un cuestionario de juicio de expertos y posteriormente se implementó en un caso hipotético. Entre las conclusiones se destaca la importancia de contar con una metodología sólida en un mundo donde la información digital es crucial y ofrece una guía valiosa para profesionales de la ciberseguridad y la informática forense.

Palabras clave: metodología, forense, informática, figuras, peritaje.

Abstract **–** The main objective of this article is to present a proposed methodology for conducting computer forensic investigations in a structured and effective manner. The methodology is divided into four main phases: identification, preservation, analysis and presentation of digital evidence. The identification phase focuses on securing the incident

[1] Rol: *conceptualización, investigación, análisis formal, metodología.*
[2] Rol: *conceptualización, análisis formal, metodología.*
[3] Rol: *investigación, validación, supervisión.*

scene and organizing the objects found, including physical and logical evidence; during the preservation phase, it ensures that the digital evidence is maintained in its original state using techniques such as bit-by-bit copying and real-time data acquisition to effectively preserve the information; the analysis phase is carried out in a forensic laboratory and uses specific tools to investigate the digital evidence; and finally, the reporting phase is divided into a technical report and an executive report, which describe the methods used, the results obtained and the conclusions. To ensure the effectiveness and accuracy of the proposed methodology, it was evaluated by three Computer Security experts from the University of La Rioja through an expert judgment questionnaire and subsequently implemented in a hypothetical case. Among the conclusions, it highlights the importance of having a solid methodology in a world where digital information is crucial and offers valuable guidance to cybersecurity and IT professionals for the development and implementation of the methodology.

Keywords: methodology, forensic, IT, diagrams, expertise.

Introducción

Los equipos tecnológicos hoy en día ocupan una postura fundamental en las ocupaciones cotidianas como por ejemplo la comunicación entre usuarios de algún servicio, almacenamiento masivo de información, automatización de procesos que a lo largo de años se realizaban manualmente y conllevaban tiempo y más grandes costos de recursos económicos y humanos; por eso se debería ser bastante cuidadoso en la implementación y difusión de contenido en formato digital debido a que su desempeño inadecuado llevaría a que personas de mala conducta logren poseerla y cometer delitos.

Según Kessler et al. (2020), el auge de la tecnología y la digitalización ha llevado a un aumento significativo de los delitos informáticos en todo el mundo. Es por eso que es fundamental contar con peritos capacitados en informática forense para investigar y recopilar evidencia digital en casos criminales. Además, la falta de capacitación y conocimientos adecuados en el campo de la informática forense puede llevar a una mala gestión de la evidencia digital, lo que puede comprometer su integridad y su capacidad para ser utilizada en un proceso judicial (Quick & Choo, 2018). Por lo tanto, es crucial contar con una metodología efectiva para el análisis forense de imágenes de unidades de almacenamiento, que garantice la preservación y la validez de la evidencia digital.

En este entorno, la Fiscalía General del Estado Ecuatoriano requiere de un conjunto de expertos capacitados en diferentes profesiones para el desarrollo de los informes, denominados como peritos, los mismos que forman parte de la organización y en diversos casos, una vez que no se cuenta con los especialistas, se acude a los individuos con personalidad jurídica (asociaciones o colegios de profesionales) o naturales que estén debidamente registrados y calificados en la función judicial. En Ecuador, los delitos informáticos son realizados por una persona o grupo de ellos que se caracterizan por tener conductas maliciosas teniendo como fin atentar contra bienes ajenos e irrumpir en la privacidad de los individuos para sacar beneficio de las vulnerabilidades y de carencias de controles en los diferentes servicios o medios digitales.

El Código Orgánico Integral Penal del Ecuador (COIP) en el párrafo tercero referente a la pericia, detalla en su artículo 511 el perfil que debería tener el perito y establece que debe estar acreditado por el Consejo de la Judicatura. Menciona que en la situación de no existir una persona acreditada

es preciso que quien realice el proceso pueda tenga el razonamiento, la experticia o un título que lo acredite. Si el perito es acreditado los informes serían tomados como prueba en alusión a testimonios. Asimismo, en el artículo 456 del COIP sobre pruebas, indica que los elementos físicos o con contenido digital materia de prueba deberán aplicárseles la cadena de custodia para garantizar su autenticidad, asegurando su identidad y estado original (Rosero, 2019).

Actualmente, diversos estudios han comparado las diferentes normas y metodologías de análisis forense informático utilizadas en la examinación de datos en medios digitales (Hidalgo et al., 2018; Loarte Cajamarca & Grijalva Lima, 2018; Pineda, 2016; Santos & Florez, 2012). Estos estudios proporcionan un punto de partida para la metodología propuesta, que aborda los procesos de indagación a lo largo de cada etapa del desarrollo, y cubre todas las metas mediante la correcta utilización de herramientas informáticas.

Por lo tanto, en los procesos investigativos en el ámbito de la informática forense si no se tiene la experticia suficiente podrían provocar que las evidencias digitales pierdan validez. Por ello debe existir una metodología que guíe de principio a fin las etapas para la ejecución de un estudio forense para dispositivos de almacenamiento de contenido digital, bajo este trabajo se justifica su desarrollo (Tugnarelli et al., 2017).

Acerca de las metodologías existentes, un estudio realizado por Hidalgo et al. (2018), realizó una comparación de las metodologías y normas de análisis forense informático en la ciencia forense digital , cuyos resultados revelaron que el 60% de los especialistas prefieren la metodología UNE 71506:2013 por su proceso integrado y sistemático de cuatro etapas, mientras que el 30% opta por el NIST (National Institute of Standards and Technology) con un proceso de cuatro etapas, y el 10% restante se inclina por el Integrated Digital Investigation Process que consta de tres etapas. Estas metodologías ofrecen eficiencia, confiabilidad y seguridad en los procesos investigativos, lo que contribuye a la veracidad de los resultados en el peritaje informático.

Otra investigación realizada por Pinto (2014), propone una metodología de análisis forense enfocada en incidentes de dispositivos móviles, donde destaca su creciente importancia en la vida cotidiana y su rol en diferentes escenarios delictivos, se resalta la diversidad de usos y la urgencia de contar con estándares que garanticen la integridad de las evidencias digitales recuperadas. La propuesta ofrece un proceso detallado compuesto por 31 pasos ordenados, donde cada etapa define claramente los objetivos, indicaciones y productos a entregar, distinguiéndose de otros enfoques que no especifican acciones detalladas por etapa.

La investigación reveló que muchas herramientas de análisis forense no abarcan íntegramente el proceso para dispositivos móviles, lo que subraya la imperante necesidad de que las universidades desarrollen y perfeccionen estas herramientas, posicionándose como centros pioneros de investigación y soporte en este campo. Es esencial establecer acuerdos de investigación que involucren a la academia, entidades gubernamentales y organismos nacionales e internacionales.

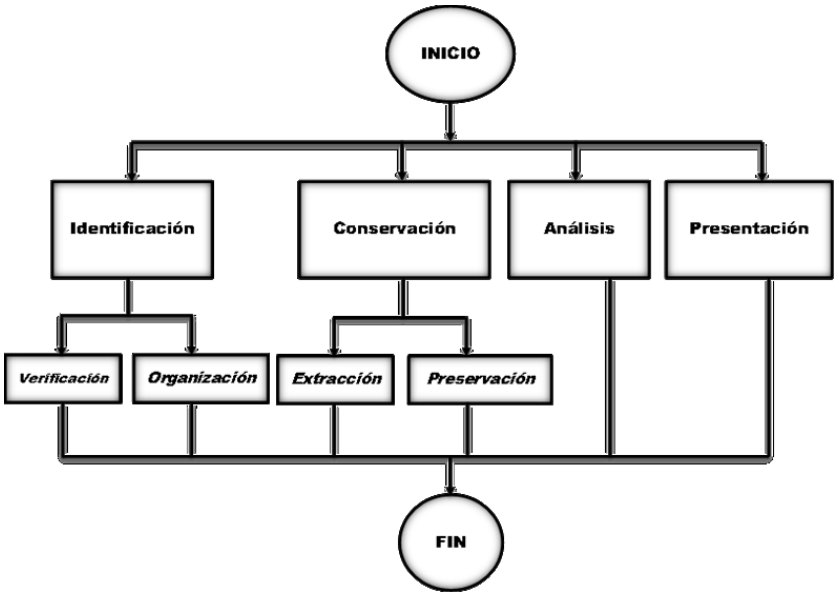
Estas colaboraciones deben enfocarse tanto en el ámbito técnico como legal, proporcionando formación y capacitación en análisis forense de dispositivos móviles para estudiantes de pregrado, posgrado y profesionales en peritaje digital. Independientemente de la metodología empleada en

la investigación forense, es primordial que cada acción esté rigurosamente validada, documentada, justificada y en consonancia con la normativa legal vigente.

Materiales y Métodos

La investigación es del tipo aplicada bajo un diseño no experimental de campo, su enfoque se dirige a la implementación de la metodología propuesta, la cual plantea la posibilidad de estructurar mediante diagramas de flujo un estudio forense informático que consiga complementar los procesos de identificación, conservación y análisis que garanticen la confiabilidad de las potenciales pruebas digitales. A continuación, en la figura 1 se presenta el diagrama general de las etapas que la comprenden.

Figura 1. Fases de ña metodología propuesta de análisis forense informático



Fuente: propia

1. Fase de identificación

Se apoya en afirmar la escena y ordenar los objetos hallados en el sitio, reconociendo al principio que las pruebas observadas tienen la posibilidad de manifestarse en forma física por medio de los dispositivos tangibles y de manera lógica por medio de los datos, y que además tienen la posibilidad de estar dependiendo funcionalmente en aquel instante de otros recursos como energía eléctrica o conexión a una red de datos.

1.1. Verificación de la escena

La cadena de custodia es un proceso crítico en la investigación de una conducta punible, y su importancia radica en la necesidad de garantizar la integridad y autenticidad de la evidencia durante todo el proceso de investigación. Como señalan Reyes et al. (2016), la cadena de custodia implica la aplicación de una serie de normas y procedimientos tendientes a proteger y preservar la evidencia, desde el momento en que se recoge hasta su presentación en un juicio.

La cadena de custodia debe asegurar que la evidencia se mantiene en su estado original y que no se contamina ni se altera de ninguna manera durante el proceso de recolección, almacenamiento y análisis. Además, es importante destacar que cualquier violación de la cadena de custodia puede tener consecuencias graves en un juicio penal. Para salvaguardar la información de los dispositivos de almacenamiento no volátil (disco duro) y en especial el volátil (memoria RAM) es primordial mantener conectada la energía eléctrica del equipo computacional. Debido a la criticidad de la estabilidad de la información en la memoria RAM es primordial salvar la información porque posteriormente será analizada por herramientas que permitan detectar y recuperar que afecte menos la evidencia (Gutiérrez, 2022).

1.2. Organización de la evidencia

Luego de identificar la evidencia se procede a organizarla adecuadamente, considerando si el equipo está encendido o apagado y estableciendo la ruta a seguir. En este paso es importante documentar toda la información que pudiera asociarse al equipo informático, como por ejemplo notas que contengan contraseñas.

La observación juega un papel fundamental en la investigación, ya que permite detectar indicios y testigos mudos que no pueden mentir. Un examen diligente y adecuado de estos indicios puede señalar al autor o autores del delito y reconstruir lo sucedido. En este sentido, el éxito de la investigación depende de un cuidadoso examen de la escena del crimen en busca de indicios, que son el objeto propio, formal y específico de estudio de la criminalística. Este proceso implica encontrar el material sensible significativo relacionado con los hechos investigados, también conocido como evidencia física o evidencia digital.

2. Fase de conservación

La preservación adecuada de la evidencia digital es crucial en cualquier investigación judicial. Como señalan Debrota & Singh (2014), es esencial realizar copias de seguridad completas de todos los dispositivos de almacenamiento relevantes para garantizar la integridad y autenticidad de la evidencia durante el análisis forense. Esto se debe a que cualquier cambio en los datos de los archivos puede tener una relevancia crítica en un proceso judicial, y los sistemas tradicionales de copia de seguridad pueden no capturar toda la información en un sistema, lo que significa que parte de la información puede perderse.

La adquisición de evidencia digital es un proceso crítico en la informática forense y debe ser realizada con precisión y cuidado para garantizar la integridad de la evidencia recolectada. Según Lee et al. (2019), la creación de copias bit a bit es una técnica comúnmente utilizada para preservar la evidencia digital en su estado original. Además, se recomienda el uso de herramientas de imágenes de disco, ya que estas permiten adquirir una imagen exacta del disco duro sin modificar la información original (Casey, 2018).

Otra técnica importante es la adquisición de datos en tiempo real, la cual permite la recolección de datos en vivo, sin tener que apagar el equipo o alterar su estado actual (Chong y Lee, 2020). Al seguir estas técnicas y procedimientos adecuados, se puede garantizar que la evidencia digital obtenida es válida y puede ser utilizada en un proceso judicial.

2.1. Extracción

El inicio de reproducibilidad debería ser una característica forzosa en la sustracción ya que de esta forma lo amerita la ejecución siguiente que es la investigación, según sea el ámbito la prueba digital adquirida puede manifestarse como una clonación o imágenes enteras o parciales de la información.

La sustracción se puede hacer en dos estados que condicionan plenamente el acceso a la evidencia y su posterior almacenamiento; uno de ellos es la potencial prueba digital en el sistema apagado, haciendo más fácil su funcionamiento y el otro se da una vez que el sistema está encendido, en aquel caso las medidas son diversas debido a que su desempeño involucra la aplicación de procedimientos intrusivos que siendo mínimos tienen la posibilidad de provocar alteraciones que tienen la posibilidad de llegar a comprometer la totalidad de la información si no se toma las precauciones que corresponden.

Los dispositivos de almacenamientos externos, unidad flash USB, discos duros externos, memorias de cámaras fotográficas, DVD. Además, se tendría las unidades de almacenamiento interno como disco duro, por lo que el computador debe estar apagado para así ser transportado a las oficinas de Ciencias Forenses Informáticas para su examinación.

2.2. Preservación

Las pruebas digitales extraídas por el DES y DEFR deberán ser sometidas al proceso de entrega y recepción por medio del registro de una totalmente nueva ficha técnica que contenga nombres de quien entrega y de quien obtiene, fecha, hora y sitio de donde viajó y donde está llegando, tipo de prueba, estado, y detalle de los procesos hechos.

Pese a ser la tercera fase en la metodología presentada puede llegar a ser la fase inicial en la situación de que se llegue a exponer la prueba y sea declarada sin fundamentado o invalida, siendo ésta la fase de alusión para empezar con la nueva averiguación, por esto la conservación de la prueba debería ser lo más limpia e integra viable.

3. Análisis de la potencial evidencia digital

Es importante verificar que las probables pruebas no sufrieran deterioro o se encuentren vulnerables debido a un almacenamiento incorrecto que permita que la calidad disminuya el empleo de las herramientas específicas como DumpIt, FTK Imager, Windows Forensic Toolchest (WFT), OS Forensic y RamCapture (Gutiérrez, 2022).

Por lo que es primordial que el análisis de las potenciales evidencias se realice en un laboratorio dotado con herramientas informáticas para análisis forense de igual forma tener infraestructura y hardware que asegure la confidencialidad e integridad de la información analizada (Larrea, 2016).

Durante esta fase el proceso para realizar el análisis será del correspondiente a volcados de memoria RAM, clonación de disco duros y copias potenciales de pruebas digitales.

4. Presentación de informes de la potencial evidencia digital

Se basa en formar dos documentos, uno de orden técnico y el otro de orden ejecutivo. En el Informe Técnico se utilizará un lenguaje que cualquier profesional de la rama va a poder entender; determinando los métodos, herramientas usadas y los resultados logrados de las metas planteadas. El Informe Ejecutivo va a ser hecho con un lenguaje de simple conocimiento y sin tecnicismos, para que se pueda tomar como prueba lo cual ahí se explica.

A continuación, se indican los elementos que deben constar en la Presentación del Informe Pericial de tipo técnico:

- Cabecera.
- Identificación.
- Detalle de evidencias.
- Contenido del informe. Se describirá los procesos, análisis y estudios realizados.
- Firma del perito forense.
- Resultados del estado de la evidencia digital.
- Conclusiones.

Elementos para elaborar los Informes ejecutivos:

- Cabecera.
- Identificación.
- Descripción breve de las actividades realizadas.
- Firma del perito forense.
- Resultados o conclusiones.

Para garantizar la eficacia y precisión de la metodología propuesta, esta fue evaluada por tres expertos en Seguridad Informática de la Universidad de la Rioja. A continuación, se presenta la tabla 1 con las preguntas del cuestionario de juicio de expertos.

Tabla 1. Preguntas de evaluación de la metodología forense

Elemento	Pregunta
Definición y Alcance:	¿Considera que la metodología propuesta aborda adecuadamente todas las fases de la investigación forense en dispositivos de almacenamiento?
Procedimientos:	¿Los procedimientos detallados en la metodología son prácticos y aplicables en un escenario real de investigación forense?
Herramientas:	¿La metodología sugiere herramientas adecuadas para cada fase de la investigación? ¿Existen otras herramientas que recomendaría incluir o excluir?
Documentación y Evidencia:	¿Se enfatiza adecuadamente la documentación y cadena de custodia en la metodología propuesta?
Consideraciones Éticas y Legales:	¿Se tratan adecuadamente las consideraciones éticas y legales asociadas con la investigación forense en la metodología?
Pruebas y Validación:	¿La metodología proporciona una guía clara sobre cómo probar y validar los resultados obtenidos en una investigación?
Capacitación y Conocimientos Requeridos:	¿Qué nivel de habilidad o conocimiento previo considera necesario para implementar esta metodología de manera efectiva?

Recomendaciones Generales:	¿Qué áreas considera que necesitan una revisión o mejora significativa?
Consideraciones Finales:	¿Tiene alguna otra sugerencia o comentario para mejorar la metodología propuesta?

Fuente: propia

A través de la metodología Delphi, los especialistas brindaron valiosas observaciones que fueron debidamente incorporadas a la metodología propuesta.

En el contexto de esta investigación, se estableció un escenario hipotético relacionado con un presunto caso de pornografía infantil con el objetivo de evaluar y validar las etapas de la metodología propuesta. Durante esta indagación, se identificaron varias posibles evidencias digitales, tanto físicas como lógicas. Estas evidencias, que se detallan a continuación, serán sometidas a un análisis exhaustivo siguiendo las fases de la metodología propuesta:

- Un equipo portátil que opera bajo el sistema Windows 7 Home Premium (Service Pack 1).
- Memoria RAM en uso, ubicada en el equipo anteriormente mencionado.
- Un conjunto de 38 discos DVD sin etiquetas o marcas distintivas visibles.
- Una memoria Flash.

Resultados y Discusión

Fase 1. Identificación de la potencial evidencia digital

El éxito del análisis forense radica en la precisión de cada una de sus fases. Por lo tanto, iniciar de manera adecuada es esencial. Una observación o exploración meticulosamente realizada minimiza significativamente el riesgo de pérdida o modificación de evidencia digital potencialmente crucial. Sin un enfoque experto, detalles valiosos, aunque estén a simple vista, pueden pasar inadvertidos y quedar fuera del alcance de la investigación.

1.1. Verificación de la evidencia digital recolectada

Se llevaron a cabo las acciones siguientes:

a. Al manipular potenciales evidencias digitales, se usaron guantes plásticos para evitar dejar rastros o huellas dactilares que pudieran alterar los elementos recopilados. Asimismo, se emplearon bolsas antiestáticas para resguardar los dispositivos.
b. Se identificaron los dispositivos que podrían contener información en formato digital. En este caso, las evidencias comprenden un computador portátil, una memoria flash y discos compactos.
c. Se manejaron con cuidado las evidencias digitales potenciales, clasificando los elementos encontrados según su volatilidad y riesgo de pérdida de datos, basándose en experiencia previa.
d. Se dispuso de etiquetas adhesivas para marcar las evidencias digitales recuperadas, indicando la fecha y hora de recolección. Es importante asegurarse de no obstruir información vital en la evidencia, como modelos, marcas o números de serie.
e. Se observó que la habitación carecía de cualquier infraestructura de red por cable, lo que sugiere que, si el implicado utilizó servicios de internet, probablemente fue a través de una

red WIFI compartida o a través de un dispositivo móvil propio. No se encontraron documentos ni notas vinculadas al caso en investigación. Se capturaron imágenes para documentar la disposición de los objetos en la escena.

1.2. Organización de la evidencia digital

Consiste en realizar la determinación acertada del estado de volatilidad de las potenciales evidencias digitales. A continuación, se dividen en alta y baja (ver tabla 2). Se procedió con el etiquetado, considerando fecha y hora en cintas adhesivas o membretes. Establecer normativa para diferenciar evidencias. Todas las evidencias tendrán formato: EviDigNúmeroTipo: EviDig (representa una evidencia digital), Número (refiere al ordinal en que fue etiquetada la evidencia) y Tipo (referente al tipo de evidencia encontrada).

Tabla 2. Volatilidad de las evidencias

Categoría de volatilidad	Organización de la evidencia	Evidencia etiquetada
Volatilidad Alta	Equipo encendido y conectado a una fuente de energía. Debido a los datos en la RAM, se embaló en bolsas antiestáticas. Se conectó un disco duro externo previamente preparado con AccesData FTK Imager. Se hizo un volcado inmediato de la RAM.	➢ EviDig01VolRam
Volatilidad Baja	Pila de discos y flash memory. Se almacenarán en bolsas antiestáticas. Los discos compactos se trasladan para revisión.	➢ EviDig02HD ➢ EviDig03USB ➢ EviDig04PilaDVD

Fuente: propia

En resumen, la fase de identificación implica asegurar la escena del incidente y ordenar los objetos hallados, tomando en cuenta tanto las pruebas físicas como lógicas y la potencial dependencia de recursos externos. Es de vital importancia, en esta fase, implementar una cadena de custodia que garantice la integridad y autenticidad de la evidencia (Reyes et al., 2016). Asimismo, la verificación de la escena se centra en la protección de la información contenida en los dispositivos y en preservar la data en la memoria RAM (Gutiérrez, 2022). Con la organización de la evidencia, se documenta toda la información relacionada con el equipo informático y se clasifica según si el equipo se encuentra encendido o apagado.

Fase 2. Conservación de la potencial evidencia digital

2.1. Extracción

La correcta gestión de las fases iniciales, tras identificar las potenciales evidencias digitales, establece el protocolo para extraer información de sistemas apagados.

Para las evidencias denominadas EviDig01VolRam, EviDig03USB y EviDig02HD, se empleó el software AccesData FTK Imager. En particular, se realizó una clonación bit a bit del disco duro.

Dado que el disco duro contaba con una capacidad de 320GB, el proceso demandó un tiempo de 4:59:27.

Ante dispositivos encendidos, se priorizó aquellos con un alto nivel de volatilidad. En este caso, al estar la computadora portátil en funcionamiento y ante el riesgo de perder información al apagarla, se ejecutó el volcado de la memoria RAM. Este paso es fundamental, ya que la RAM retiene información sobre las acciones realizadas previamente y puede albergar fragmentos de archivos eliminados, así como credenciales de usuarios. Es esencial que, al trabajar con dispositivos de almacenamiento, ya sean internos o externos, se realice una copia bit por bit. Esta metodología garantiza la integridad de la información durante los análisis subsiguientes.
Posteriormente, para asegurar la integridad de las evidencias, se generó un HASH utilizando la herramienta MD5 & SHA Checksum Utility, Para finalizar con esta fase se apagó el equipo y se lo empaquetó con el debido cuidado para su entrega, evitando golpes físicos que puedan poner en riesgo los elementos probatorios.

2.2. Preservación de la evidencia digital

Es imperativo garantizar la condición original de las evidencias recolectadas, previniendo cualquier alteración o daño que comprometa su integridad. A continuación, se detallan las acciones a ejecutar junto con el correspondiente diagrama de flujo:

- *Revisión de la Ficha de Extracción:* se verifica la ficha de extracción de la evidencia digital potencial para confirmar que toda la información recolectada esté adecuadamente registrada.
- *Respaldo de la Evidencia:* se realizan copias exactas de las evidencias con el fin de preservar el original y trabajar sobre las copias.
- *Cálculo de Hashes:* se computan los hashes de las evidencias para asegurar su integridad a lo largo del proceso de análisis.

En el laboratorio forense, se procede a la recepción de los dispositivos recolectados. Durante esta etapa, se verifica que los ítems concuerden con lo especificado en la ficha de extracción. Se evaluó la capacidad de encendido y la inicialización del sistema operativo de la computadora portátil. Posteriormente, se conecta la Flash Memory para comprobar su correcto funcionamiento en términos de conectividad y reconocimiento por el sistema.

Todos los HASH coincidieron y ello comprueba que en el proceso de traslado no existió factor que haya puesto en riesgo la integridad (ver tabla 3).

Tabla 3. Verificación de integridad de las imágenes clonadas

Evidencia	HASH Recibido de la extracción	HASH Calculado en la preservación
EviDig01VolRam	c6e8690255dfcc07ea4ae09530cf4e62	c6e8690255dfcc07ea4ae09530cf4e62
EviDig02HD	72dad8ad50bb1941767b44a899147b3c	72dad8ad50bb1941767b44a899147b3c
EviDig03USB	ba003d472c5685fd8bcd9916ec60d125	ba003d472c5685fd8bcd9916ec60d125

Fuente: propia

Es esencial llevar a cabo un etiquetado adecuado de las potenciales evidencias digitales. Para su conservación, estas deben ser almacenadas en bolsas antiestáticas, que protegen contra factores ambientales que pueden comprometer la información. Seguidamente, se organizan en estanterías, considerando la geometría y características del dispositivo, para asegurar una conservación óptima.

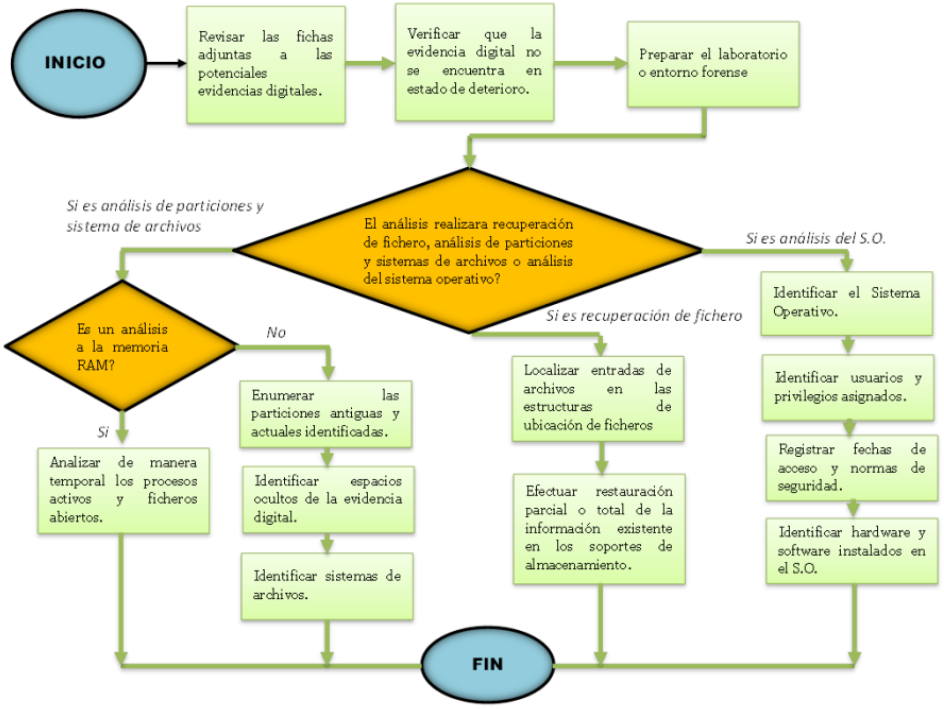
Al concluir esta fase, se documenta toda la información relevante en una ficha de extracción, que incluye detalles como la fecha, lugar, hora, y la duración total de los procesos de clonación, volcado y recuperación llevados a cabo en la etapa de preservación. En síntesis, la fase de conservación se dedica a garantizar que la información se mantenga en su estado original y asegurar la integridad de la evidencia (Casey, 2018); esto es crucial, pues la información puede sufrir alteraciones durante su análisis, y cierta data puede perderse al realizar copias de seguridad.

Fase 3. Análisis de la potencial evidencia digital

Para asegurar la integridad de los análisis en el laboratorio forense, es vital contar con sistemas de respaldo de energía que prevengan interrupciones o fluctuaciones eléctricas, especialmente cuando se manejan evidencias digitales que demandan procesos extensos de respaldo o análisis. Es crucial disponer de un UPS que ofrezca al menos tres horas de autonomía a máxima carga, salvaguardando así los procedimientos ante eventuales cortes de energía.

Durante el análisis (ver figura 2), se revisó la ficha de la fase de preservación para comprender la naturaleza de los elementos a investigar, y se emplearon herramientas específicas como Autopsy y Foremost de Kali Linux para identificar, descubrir y recuperar información pertinente.

Figura 2. Flujo de análisis de las evidencias de acuerdo con su tipo



Fuente: propia

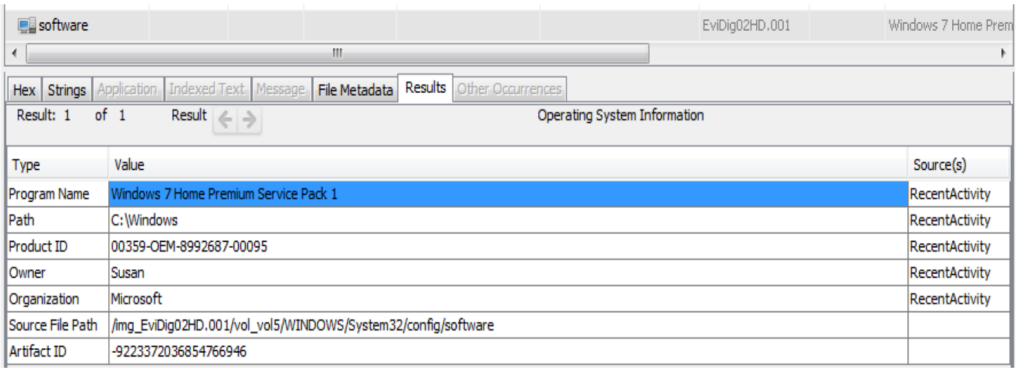
Disco Duro analizado como potencial evidencia digital

Se abrió la unidad externa en la que se había almacenado la imagen del disco duro, generando automáticamente un archivo de texto con indicaciones específicas. Para analizar dicha imagen, se estableció un caso utilizando la herramienta Autopsy versión 4.7.0 y se seleccionó la opción "Imagen de Disco" (Disk Image) como tipo de evidencia, dado que correspondía a esa clasificación. Posteriormente, se activaron todos los módulos disponibles para capturar la máxima cantidad de información. Una vez que se completó este proceso, se pudo visualizar la estructura generada a partir de la imagen cargada y se procedió con su verificación.

Análisis del Sistema Operativo

Dentro del árbol estructurado, se visualizó un directorio correspondiente al Sistema Operativo que estuvo instalado en el disco duro objeto de estudio. Al seleccionar la opción "Operating System Information", se desplegaron detalles relevantes del sistema (Figura 3).

Figura 3. Detalles de la información del Sistema Operativo



Type	Value	Source(s)
Program Name	Windows 7 Home Premium Service Pack 1	RecentActivity
Path	C:\Windows	RecentActivity
Product ID	00359-OEM-8992687-00095	RecentActivity
Owner	Susan	RecentActivity
Organization	Microsoft	RecentActivity
Source File Path	/img_EviDig02HD.001/vol_vol5/WINDOWS/System32/config/software	
Artifact ID	-9223372036854766946	

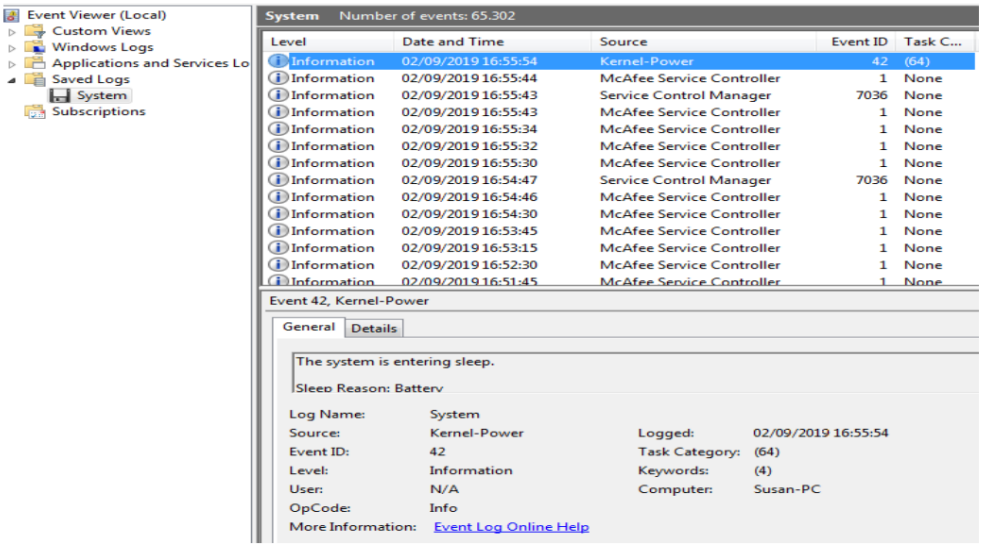
Fuente: propia

Búsqueda y Extracción de Logs de los usuarios en el Sistema

Para constatar si el computador portátil es cuenta con algún usuario que se vincule con el nombre del implicado, se realizó la exploración en la carpeta PerfLogs y se encontró únicamente una cuenta con privilegios de administrador.

Los logs del sistema son almacenados en el archivo System.evt, por ello se realiza la búsqueda en el árbol de carpetas generado, en la siguiente imagen se muestra la ubicación donde fue hallado. Ese archivo se lo exporta y luego se lo abre en el Visor de Eventos que proporciona Windows, al abrir el archivo se muestran cientos de eventos, para saber cuándo fue la última vez que se apagó, se busca en los eventos denominados Kernel Power (Figura 4).

Figura 4. Archivo exportado ejecutado en el Visor de Eventos de Windows



Fuente: propia

Búsqueda de imágenes eliminadas

Dentro del directorio Views/Files Types/By Extension/Images, se identificaron 24.616 imágenes. De esta cantidad, 14 fotografías presentaban contenido que podría estar asociado a pornografía infantil. Notablemente, dichos archivos estaban almacenados en la Papelera de Reciclaje. Para el análisis forense, se generó una imagen del disco duro, la cual fue restaurada en un equipo especializado para tal fin y se montó exitosamente. A pesar de una exhaustiva revisión en todos los posibles directorios donde se pudieran almacenar imágenes o videos, no se encontraron las fotografías mencionadas anteriormente.

Técnica de búsqueda por filtro de imágenes

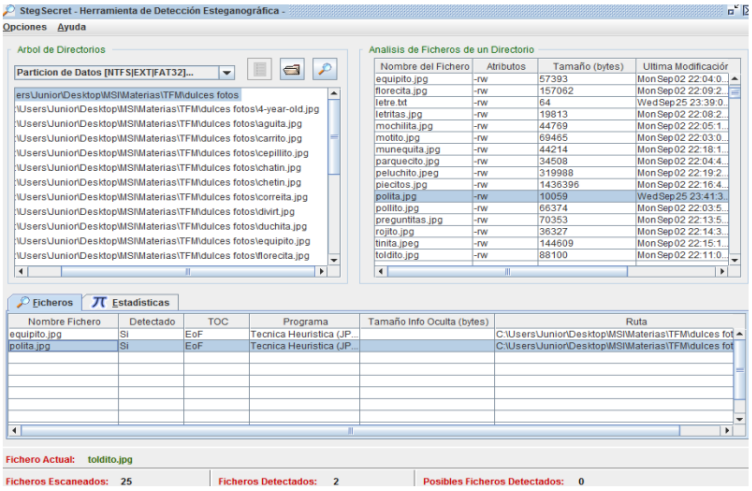
Las fotos recuperadas se someten a un análisis con la herramienta StegSecret, y de los 25 archivos escaneados se detectaron 2, que posiblemente contengan datos ocultos como se muestra a continuación en la Figura 5. Las imágenes "equipito.jpg" y "polita.jpg" fueron analizadas utilizando Foremost, una herramienta forense de Kali Linux especializada en recuperación y extracción de datos. Como resultado del análisis, se confirmó la existencia de un archivo llamado "letre.txt".

Fase 4: Presentación de Informes sobre la Evidencia Digital Potencial

A través de la investigación y análisis de los elementos incautados, se estableció que el sospechoso había almacenado fotografías en la Flash Memory. Posteriormente, transfirió estas imágenes a un equipo portátil y las eliminó de la Flash Memory. Esta acción dejó rastros en ambos dispositivos. A pesar de la búsqueda exhaustiva, las imágenes no se encontraron de manera directa en ningún directorio del equipo, ya que el implicado creó un volumen encriptado con TrueCrypt para ocultarlas de posibles intrusos en su sesión.

Al someter los 25 archivos a un análisis con la herramienta StegSecret, se identificaron 2 que podrían contener información oculta. Estos archivos se procesaron con Foremost, una herramienta que proporciona Kali Linux. Se concluyó que el archivo "polita.jpg" contenía un archivo de texto llamado "letre.txt".

Figura 5. Análisis con la herramienta StegSecret



Fuente: propia

En un mundo donde la información digital se ha convertido en un activo fundamental, es vital contar con metodologías de análisis forense sólidas y estructuradas. Estas garantizan que la evidencia recolectada sea fiable y pueda utilizarse para determinar la naturaleza y extensión de un incidente de seguridad, así como para adoptar medidas correctivas y preventivas en el futuro. Con un enfoque claro en la identificación, conservación y análisis, esta metodología se erige como una herramienta indispensable para los profesionales de la ciberseguridad.

Conclusiones

El presente artículo introduce un modelo que ofrece una guía metodológica clara y eficiente para realizar un análisis forense adecuado de evidencias digitales. Este modelo pone especial énfasis en el manejo de medios de almacenamiento de datos en el contexto de una investigación. Para ilustrar su aplicabilidad, se diseñó un escenario de indagación donde se llevaron a cabo tareas como la clonación del disco duro, la copia de una unidad flash USB y el volcado de la memoria RAM. A través de estas acciones, se demostró que, aunque los datos recopilados de cada prueba pueden variar, al interrelacionarlos se forman conexiones que simplifican la toma de decisiones finales.

Es importante presentar informes tanto ejecutivos como técnicos de manera meticulosa y adaptada al público al que van dirigidos, lo que es crucial para asegurar su validez y posible admisibilidad en el ámbito judicial como prueba digital. En el estudio, los informes se elaboraron siguiendo las directrices establecidas en el marco de referencia UNE 197010 -2015.

Los diagramas de flujo utilizados facilitan la visualización práctica y ordenada de cada paso de la metodología propuesta. Estas figuras pueden servir tanto para iniciar una investigación desde cero

como para dar seguimiento a una ya en curso, proporcionando claridad en el proceso y, por ende, optimizando el tiempo. Al integrar la guía con los diagramas de flujo, se mejora notablemente la experiencia en comparación con métodos tradicionales.

En cuanto a las proyecciones futuras, sería relevante desarrollar una metodología específica para el análisis forense de dispositivos móviles, dado su creciente uso en la vida cotidiana. Esta adaptación no solo sería viable, sino que también respondería a una demanda real y creciente en el campo de la investigación forense digital.

Referencias

Casey, E. (2018). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.* Academic Press.

Chong, J., & Lee, H. (2020). Real-time digital forensics: A survey. *Digital Investigation, 34*, 101006.

Debrota, S., & Singh, R. (2014). A study of digital evidence acquisition techniques. *International Journal of Computer Science and Mobile Computing, 3*(5), 82-88.

Gutiérrez, H. (2022). Evaluación de herramientas de software libre, para el sistema operativo Windows, en la adquisición de evidencias de la memoria RAM. *Publicaciones e Investigación, 16(*1). https://dialnet.unirioja.es/servlet/articulo?codigo=8660196

Hidalgo, I., Yasaca, S., Hidalgo, B., Oquendo, V., & Salazar, F. (2018). Estudio comparativo de las metodologías de análisis forense informático para la examinación de datos en medios digitales. *European Scientific Journal*, *14*(18). https://doi.org/10.19044/esj.2018.v14n18p40

Kessler, G.C., D'Amico, A., & Higgins, G.E. (2020). *Cybercrime and digital criminology*. In The Handbook of the Criminology of Terrorism (pp. 355-374). John Wiley & Sons.

Larrea Ronquillo, J. S. (2016). Estudio e Implementación de Metodología de Análisis Forense Digital Aplicables en un Laboratorio de Informática Forense en la Carrera de Ingeniería en Networking y Telecomunicaciones (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Telecomunicaciones). https://rraae.cedia.edu.ec/Record/UG_dd34ed82791c8ae408a0248732b54f3e

Lee, S. H., Lee, S., Lee, Y., & Kim, D. (2019). A Study on the Effectiveness of Bitstream Image Acquisition in Digital Forensics. *Journal of Digital Forensics, Security and Law, 14*(1), 31-46.

Loarte Cajamarca, B. G. & Grijalva Lima, J. S. (2018). Desarrollo de una guía metodológica para el análisis forense en equipos de cómputo con Sistema Operativo Mac OS X. *Revista Publicando, 5*(14 (1)), 24-67. https://revistapublicando.org/revista/index.php/crv/article/view/1093

Pineda Vaca, A. E. (2016). Diseño de un modelo de análisis forense informático en el Honorable Gobierno Provincial de Tungurahua (Bachelor's thesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Sistemas Computacionales e Informáticos). https://repositorio.uta.edu.ec/handle/123456789/23463

Pinto, D. (2014). Metodología de análisis forense orientada a incidentes en dispositivos móviles. *Revista MASKANA, Actas del Congreso Ecuatoriano de Tecnologías de la Información y Comunicación – TIC.EC 2014*, 5. Universidad de Cuenca.

Quick, D. & Choo, K.K.R. (2018). *Forensic investigation of digital devices*. John Wiley & Sons.

Reyes, H., Rojas, J., & Carmona, L. (2016). La cadena de custodia como elemento fundamental en la investigación criminal. *Revista Ciencias Penales, 23*(2), 12-24.

Rosero Paredes, D. S. (2019). *Diseño de una metodología de recolección de evidencia digital para análisis forense de unidades de disco duro, basada en la norma ISO/IEC 27037: 2012.* Universidad Internacional SEK. https://repositorio.uisek.edu.ec/handle/123456789/3609

Santos, L. & Florez, A. (2012). Metodología para el análisis forense en Linux. *Revista Colombiana de Tecnologías de Avanzada (RCTA), 2*(20). 90-96. https://revistas.unipamplona.edu.co/ojs_viceinves/index.php/RCTA/article/view/194

Tugnarelli, M. D., Fornaroli, M. F., Santana, S. R., Jacobo, E., & Díaz, F. J. (2017). Análisis de metodologías de recolección de datos digitales. In XIX Workshop de Investigadores en Ciencias de la Computación (WICC 2017, ITBA, Buenos Aires). https://sedici.unlp.edu.ar/handle/10915/62613