DOI: https://doi.org/10.34070

Metodología para el análisis forense de imágenes de unidades de almacenamiento

Methodology for the forensic analysis of images of storage units

Susana Gabriela Patiño Rosado, MSc.
Pontificia Universidad Católica del Ecuador, Ecuador
https://orcid.org/0000-0001-5405-5224
susanapatinor@gmail.com

Junior Manfredo Rojas Rosado, MSc.
Universidad Técnica "Luis Vargas Torres", Ecuador
https://orcid.org/0000-0003-0037-4283
jun17_1988@hotmail.com

Hector Andres Sacon Klinger, MSc.
Universidad Técnica de Esmeraldas "Luis Vargas Torres, Ecuador
https://orcid.org/0000-0001-6585-4793
hector.sacon.klinger@utelvt.edu.ec

Palabras claves: metodología de análisis, normativa RFC-3227, informática forense, evidencias digitales, peritajes.

Recibido: 31 de marzo de 2022

Keywords: analysis methodology, RFC-3227 regulations, computer forensics, digital evidence, expert reports.

Aceptado: 28 de abril de 2023

RESUMEN

El presente artículo tiene como objetivo principal presentar una Metodología de Análisis Forense para especialistas en peritaje informático cuyas actividades en los encargos judiciales sea en investigación de periféricos de almacenamiento en Sistemas Operativos Linux o Windows; con la finalidad de obtener evidencias digitales. La estructura que conforma las etapas de la metodología están basados en los criterios establecidos dentro de la normativa RFC 3227 para las directrices que permitan realizar la recolección de evidencias y su almacenamiento estandarizado en el tratamiento de incidentes de seguridad; la UNE 71506:2013 permitió mediante la metodología del análisis forense guiar el desarrollo de las etapas; para la elaboración de los informes periciales se obtuvo soporte en la UNE 197010:2015 la cual cuenta con varios criterios para la elaboración de los dictámenes en el ámbito de las TIC y para fortalecer la metodología se analizó la UNE-EN ISO/IEC 27037:2016 para incluir varias de las normas que permiten realizar los procesos de identificación, recolección, adquisición y preservación de las potenciales evidencias digitales. Los resultados obtenidos concluyen que las metodologías tradicionales pueden mejorar la experiencia investigativa y procedimental del especialista mediante la implementación de figuras de flujo sin perder la calidad en el proceso.

ABSTRACT

The main objective of this article is to present a Forensic Analysis Methodology for specialists in computer expertise whose activities in judicial assignments are in the investigation of storage peripherals in Linux or Windows Operating Systems; for the purpose of obtaining digital evidence. The structure that makes up the stages of the methodology are based on the criteria established within the RFC 3227 standard for the guidelines that allow the collection of evidence and its standardized storage in the treatment of security incidents; UNE 71506:2013 allowed, through the forensic analysis methodology, to guide the development of the stages; for the preparation of the expert reports, support was obtained in the UNE 197010:2015, which has several criteria for the preparation of opinions in the field of ICT and to strengthen the methodology, the UNE-EN ISO/IEC 27037 was analyzed: 2016 to include several of the standards that allow the processes of identification, collection, acquisition and preservation of potential digital evidence to be carried out. The results obtained conclude that traditional methodologies can improve the investigative and procedural experience of the specialist through the implementation of flowcharts without losing quality in the process.

INTRODUCCIÓN

Los equipos tecnológicos hoy en día ocupan una postura bastante 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.

En este entorno, la Fiscalía General del Estado Ecuatoriano requiere 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 nace a buscar de los individuos jurídicas (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 menciona que debería 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 existen varios estudios que han comparado las diferentes normas y metodologías de análisis forense informático utilizadas en la examinación de datos en medios digitales (Cajo, Pucuna, Cajo, Coronado & Orozco, 2018, Cajamarca & Lima, 2018, Pineda, 2016). Los estudios anteriores permiten establecer el punto de partida para la metodología propuesta que tiene los procesos sobre la indagación a lo largo de cada uno de los periodos del desarrollo, cubriendo todas las metas por medio de la utilización correcta de los instrumentos informáticos.

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, Fornaroli, Santana, Jacobo & Díaz, 2017).

Este archivo está formado de 3 secciones, aparte de esta introducción. En la segunda parte se muestra la metodología de estudio forense para unidades de almacenamiento, en la tercera parte se muestran los resultados logrados, seguido de las conclusiones determinadas.

DESARROLLO

Modelo propuesto

Existe metodología de análisis forense que comprende el estudio de la zona afectada, manipulación de los datos, análisis de la evidencia, y presentación de resultados (Jaime & Fuente, 2012). Sin embargo, la metodología propuesta plantea la posibilidad de estructurar mediante Figuras 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, se presenta el Figura general de las etapas que la comprenden:

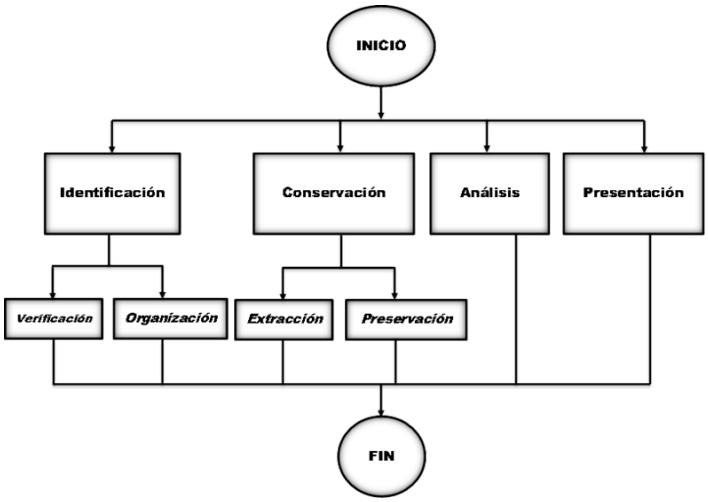

Figura 1. Fases de la metodología de análisis forense informático propuesto. Jaime & Fuente (2012).

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.

Dentro de la esta fase se tienen dos sub-fases:

Verificación de la escena. -La cadena de custodia es la aplicación de una serie de normas tendientes a cerrar, embalar y proteger cada uno de los elementos probatorios para evitar su destrucción, suplantación o contaminación, lo que podría implicar serios tropiezos en la investigación de una conducta punible. 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 por lo que el Figura 2 detalla los pasos a seguir para el correcto manejo de evidencia.

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 (Oquendo, 2022).

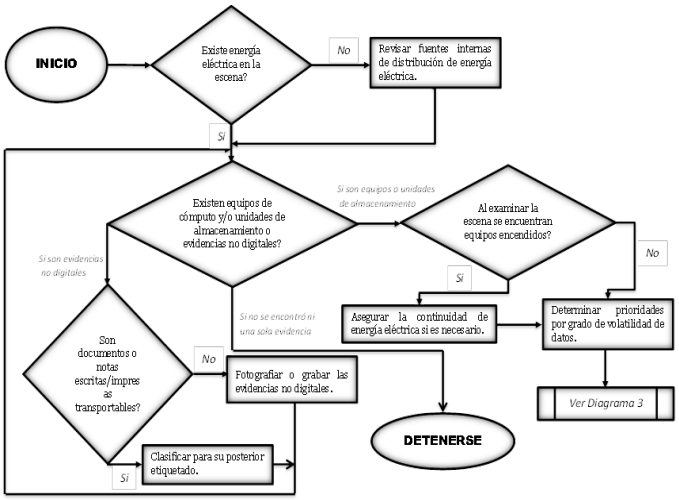

Figura 2. Flujo para realizar la verificación de potenciales evidencias digitales. Oquendo (2022).

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 (Figura 3). En este paso es importante documentar toda la información que pudiera asociarse al equipo informático, como por ejemplo notas que contengan contraseñas.
El papel que desempeña la observación en la investigación, ya que permite encontrar los indicios o testigos mudos que no miente cuyo diligente y adecuado examen hace señalar al autor o autores del ilícito penal, así como su reconstrucción.
El éxito de la investigación depende, por lo tanto, del cuidadoso examen de la escena del crimen, en busca de indicios, objeto propio, formal y específicamente determinado de estudio de la criminalística, es decir hallar el material sensible significativo relacionado con los hechos investigados también denominados evidencia física, evidencia digital

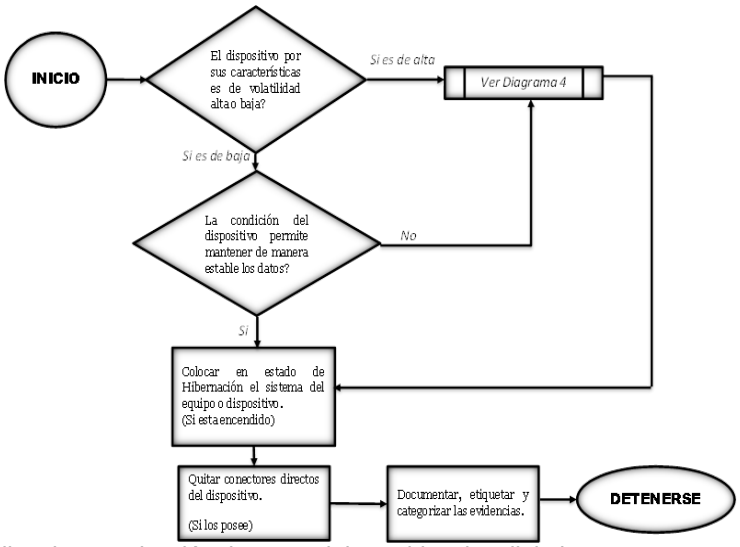

Figura 3. Flujo para realizar la organización de potenciales evidencias digitales

Fase de conservación
Se debe tener presente, que las computadoras son evidencia. La evidencia debe ser preservada en su estado original. Cuando la información es analizada, los datos de los archivos pueden cambiar, lo que puede ser relevante en un proceso judicial. Los sistemas tradicionales para realizar copias de seguridad no captan toda la información en un sistema, y parte de la información puede perderse. Por lo que es necesario realizar copias de seguridad de todos los canales de bits, como discos rígidos, diskettes, unidad flash USB, cámaras, etc.

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.

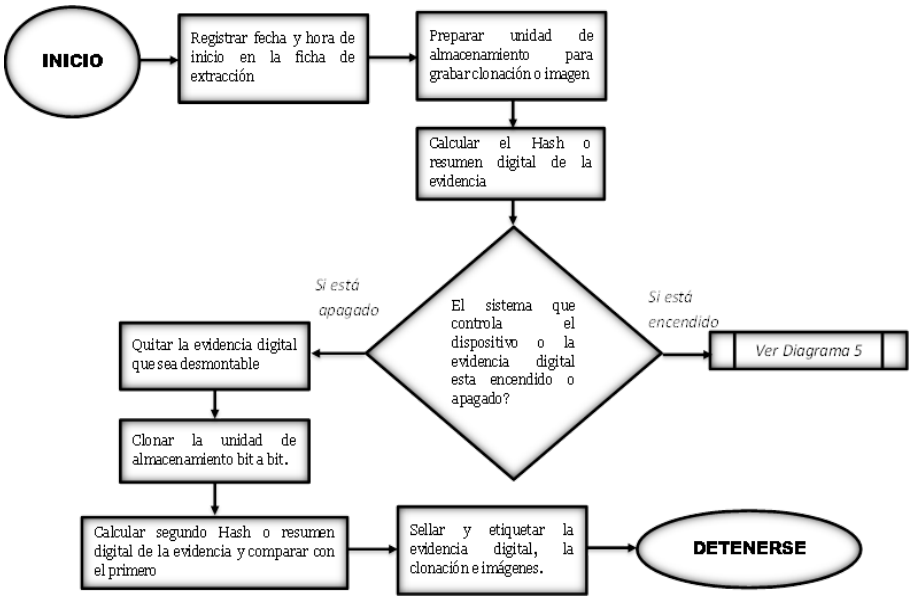

Figura 4. Flujo para realizar la extracción de potenciales evidencias digitales en dispositivos apagados

Tratamiento de evidencias digitales con sistemas encendidos.

La memoria RAM es el componente de más grande volatilidad que si cambia de un equipo informático se podría perder información de alta relevancia. Es innegable que al aplicar una técnica intrusiva hay una probabilidad mínima de ocasionar alguna modificación.

Las extracciones en sistemas encendidos no constantemente significan laborar en ámbitos inapropiados o complicados además brindan sus ventajas al permitir que el DES y DEFR no estén sometidos a tener que apagar los accesorios para definido proceso (Figura 4).

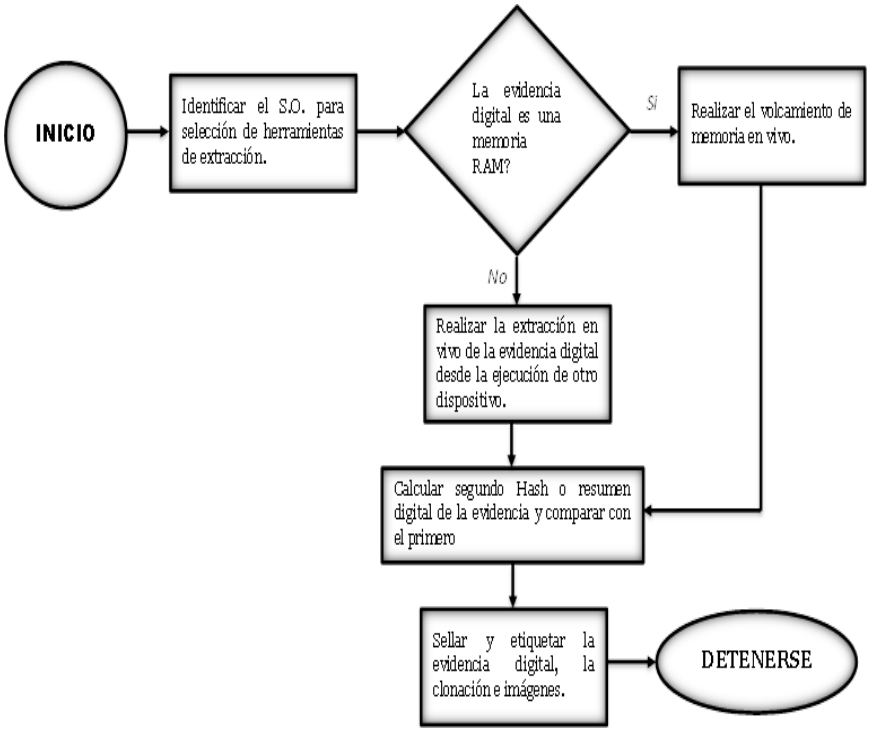

Figura 5. Flujo para realizar la extracción de potenciales evidencias digitales en dispositivos encendidos

Si se hallan equipos de escritorio se debería hacer el desmontaje de la carcasa para analizar las unidades de almacenamiento existentes y tarjetas complementarias (red, clip de video, audio), de esta forma establecer otro tipo de pistas que conlleven a decidir si los equipamientos estaban siendo conectado a internet o si poseía tarjeta de clip de video con gran capacidad de procesamiento era viable que se estuviese llevando a cabo versión de clip de videos.

Las laptops tienen que ser llevadas cuidadosamente para no arriesgar su integridad sin desarmarlos, debido a que si se pretende solo llevar su disco duro y memorias es posible que por incompatibilidad no funcionen al ser implantados en otro equipo aun teniendo las mismas propiedades, lo que involucre peligro de pérdida de la evidencia. Las potenciales pruebas digitales tienen que ser etiquetadas y categorizadas, las leyendas no deben obstruir información acerca de las características del dispositivo.

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.

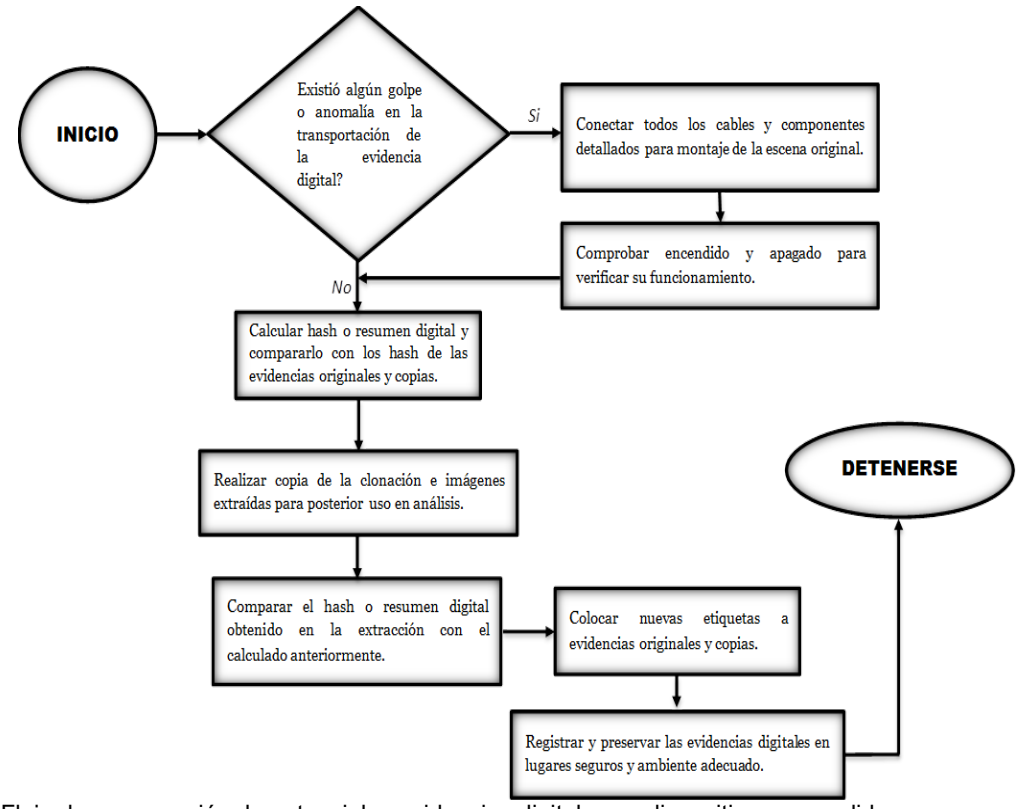

Figura 6. Flujo de preservación de potenciales evidencias digitales en dispositivos encendidos

Fase 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 (Oquendo, 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 (Figura 6).

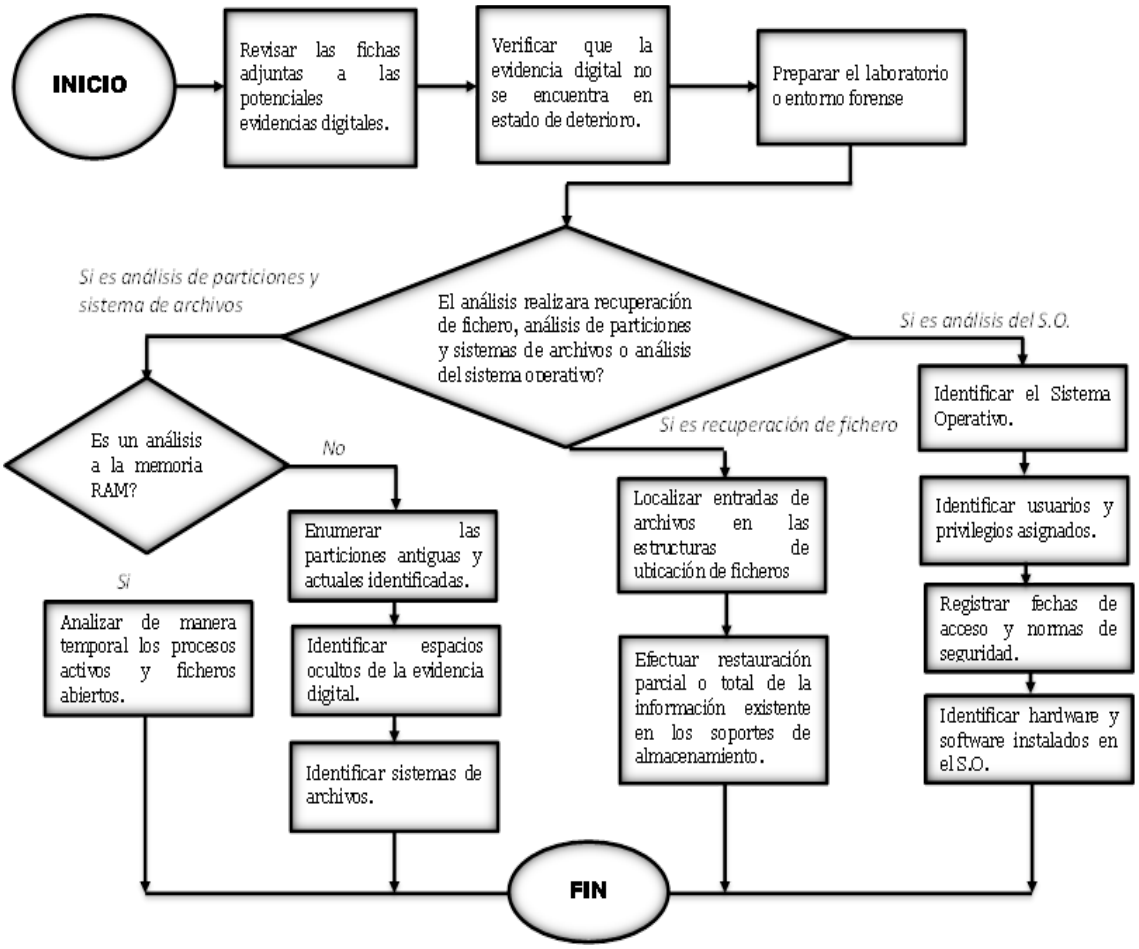

Figura 7. Flujo de análisis de potenciales evidencias digitales

Presentación de informes de la potencial evidencia digital

Se basa en formar 2 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 (Figura 7).

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.

CONCLUSIONES

El modelo propuesto en el presente artículo proyecta una guía metodológica ágil y sencilla para lograr la consecución de un análisis forense correcto de evidencias digitales, centrándose en específico a trabajar con medios de almacenamiento de datos de un proceso investigativo.

Se implementó un escenario para la indagación, en el que se procedieron a hacer las próximas ocupaciones: clonación del disco duro, de la unidad flash USB y el volcamiento de la Memoria RAM; con ello se enseñó que en el procedimiento de las pruebas y la información obtenida ha sido distinto, sin embargo, que al relacionarlas logran conformar criterios asociativos que facilitaron la toma final de elecciones.

La presentación de informes ejecutivos e informes técnicos tienen que ser detallados correctamente y explicados según quienes vayan dirigidos debido a que de aquello dependerá en parte importante su admisibilidad en el método judicial como potencial prueba digital, en este laboratorio a gusto se han realizado estos informes siguiendo los criterios en general para la preparación de informes y dictámenes periciales del marco de alusión UNE 197010 – 2015.

Los Figuras de flujo implementados han permitido esquematizar de forma práctica las secuencias a continuar de todas las etapas contempladas en la metodología, los Figuras presentados tienen la posibilidad de usar para empezar un proceso de indagación a partir de cero o para seguir uno que ya ha empezado de tal forma que da una localización en el periodo y ahorrará tiempo, guía complementada por los Figuras de flujo mejoró la vivencia comparativamente a los clásicos.

Una línea de trabajo futuro a considerar debería contemplar la implementación de una metodología para el análisis forense de dispositivos móviles o celulares debido a la connotación enorme en el uso diario, lo cuál sería posible y muy utilizado.

BIBLIOGRAFÍA

1. Cajo, I. M. H., Pucuna, S. Y., Cajo, B. G. H., Coronado, V. M. O., & Orozco, F. V. S. (2018). Estudio comparativo de las metodologías de análisis forense informático para la examinación de datos en medios digitales. *European Scientific Journal*, 14(18), 40-45.
2. Cajamarca, B. G. L., & Lima, J. S. G. (2018). Desarrollo de una guía metodológica para el análisis forense en equipos de cómputo con Sistema Operativo Mac OS X. *Revista Publicando*, 5(14), 24-67.
3. Calderón, F. A. C., & Martínez, M. R. A. (2020). Guía integral de empleo de la informática forense en el proceso penal de Ecuador. *Universidad y Sociedad*, 12(1), 182-190.
4. Cano, J., 2009. Computación forense descubriendo los rastros informáticos. En: Computación forense descubriendo los rastros informáticos. Editorial Alfa Omega, México, 1-7, 153-287.
5. Cano M. (2009). Jeimy en Computación Forense: Descubriendo los Rastros Informáticos, Editorial ALFAOMEGA, Primera Edición, México, 2009, pp.10
6. Carrier, B., E. Spafford, 2004. An event-based digital forensic investigation framework. Center for Education and Research in Information Assurance and Security - CERIAS Purdue University, West Lafayette, Indianapolis, USA. http://www.dfrws.org/2004/day1/Carrierevent.pdf
7. Castro Guerra, C. D. (2014). Análisis y aplicación de software para la recuperación forense de evidencia digital en dispositivos móviles android. Quito, Ecuador: Pontificia Universidad Católica del Ecuador.

8. DFRW, 2001. A road map for digital forensic research. New York. Disponible en http://www.dfrws.org/2001/dfrws-rm-final.pdf.
9. Eloff, J.H.P., M. Kohn, M.S Olivier, 2008. Information and computer security architectures (ICSA). Research Group. Department of Computer Science, University of Pretoria, South Africa. http://icsa.cs.up.ac.za/issa/2008/Proceedings/Full/25.pdf.
10. Hitchcock, B., Le-Khac, N.-A., & Scanlon, M. (2016). Tiered forensic methodology model for Digital Field Triage by non-digital evidence specialists. *Digital Investigation*, 16, S75-S85. https://doi.org/10.1016/j.diin.2016.01.010
11. Jaimes, L. M. S., & Fuentes, A. S. F. (2012). Metodología para el análisis forense en Linux. *Revista Colombiana de Tecnologías de Avanzada (RCTA)*, 2(20).
12. 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).
13. Mateus, J. C., Aran-Ramspott, S., & Masanet, M.-J. (2017). Análisis de la literatura sobre dispositivos móviles en la universidad española. *RIED - Revista Iberoamericana de Educación a Distancia*, 20(2), 49-72.
14. Oquendo, H. G. (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).
15. 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).
16. Rico-Bautista, D., & Rueda-Rueda, J. S. (2016). La informática forense en dispositivos Android. *Revista Ingenio*, 9(1), 21-34.
17. 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.
18. Rueda-Rueda, J. S., Rico-Bautista, D., & Florez-Solano, E. (2019). Guía práctica abierta para el análisis forense digital en dispositivos Android*. RISTI - Revista Ibérica de Sistemas y Tecnologías de La Información*, 18, 442-457.
19. Satti, R. S., & Jafari, F. (2015). Domain specific cyber forensic investigation process model*. Journal of Advances in Computer Networks*, 3(1), 75-81.
20. 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.