INTRODUCCIÓN AL MANEJO DE EVIDENCIA DIGITAL

Mayr. Efraín Argüello Arellano
JEFE DEL DEPARTAMENTO DE ANÁLISIS DE LA INFORMACIÓN DE LA DINITEC

La evolución de las Tecnologías de la Información y Telecomunicaciones (TIC´s), han permitido que la evidencia digital se posicione como una herramienta esencial para la investigación de un evento que ha trasgredido la norma, proporcionando una invaluable información que puede ser preponderante para generar hipótesis dentro un caso criminal. Este artículo explora de manera sucinta los fundamentos del manejo de evidencia digital, destacando sus características únicas, los métodos de recolección y preservación, así como a los desafíos que los expertos deben enfrentar.

¿Qué es la evidencia digital?

La evidencia digital tiene varias acepciones y conceptualizaciones, sin embargo, vamos a considerar lo expuesto por el Grupo de trabajo sobre estándar de evidencia digital (SWGDE, por sus siglas en inglés), que la define como cualquier información que se encuentre almacenada o transmitida en formato digital y que pueda ser utilizada en un proceso judicial, esto incluye datos de computadoras, teléfonos móviles, dispositivos de almacenamiento extraíbles, redes y otros medios digitales. Aquello, permite hacer una diferenciación entre la evidencia digital con la evidencia física y biológica, en razón que la primera de estas (evidencia digital), tiene la posibilidad de ser duplicada sin perder información "en el mejor de los escenarios", aunque también puede ser alterada o eliminada relativamente fácil (Casey, 2011).

Características propias de la evidencia digital

La evidencia digital, al ser concebida como un conjunto de caracteres binarios, es decir 0 y 1, posee una naturaleza intangible y la peculiar capacidad de contener metadatos, estos, proporcionan información adicional sobre el origen, la estructura y las modificaciones que experimentaron los datos, brindando un contexto importante para una investigación, puesto que admiten la identificación de acciones posiblemente dolosas. Estas caracteristicas permiten que la evidencia digital pueda estar contenida y dispersa en múltiples dispositivos, lo que en su momento puede complicar su recolección y análisis (Nelson, Phillips, & Steuart, 2018).

Ciclo de vida de la evidencia digital

Este periplo puede contener varias etapas que se deslizan entre la identificación hasta la puesta en escena en un tribunal, sin embargo, de manera simplificada se abordaran los siguientes:

Identificación.- Esta etapa se encuentra asociada a la caracterización de las posibles fuentes de datos, las cuales pueden incluir: computadoras, teléfonos móviles, relojes inteligentes, servidores, dispositivos de almacenamiento externo, entre otros. En esta etapa, los investigadores deben tener un conocimiento sólido de los tipos de dispositivos y datos que podrían ser relevantes para el caso que se está investigando (Sammons, 2012).

Preservación.– Esta etapa implica asegurar que los datos no sean alterados durante su recolección y almacenamiento, por lo tanto, es indispensable que se realice la crea-

ción de imágenes forenses, es decir, que se generen copias exactas del medio de almacenamiento que se está preservando, lo cual permite que los expertos analicen los datos sin correr el riesgo de modificar la evidencia original (Carrier, 2005).

Adquisición.- Esta etapa se enfoca en la extracción de datos de los dispositivos que en la primera etapa fueron identificados, este proceso se debe realizar con la utilización de herramientas, técnicas y métodos forenses; probados, aceptados y que se puedan replicar para llegar a obtener un mismo resultado, con la finalidad de asegurar la integridad de los datos. Estas actividades deben ser documentadas para cumplir con los recaudas necesarios que la norma jurídica lo establece, es decir, mantener la cadena de custodia (Casey, 2011).

Análisis.– Esta etapa es una de las más complejas de este ciclo del manejo de evidencia digital, en razón, que implica examinar, interpretar y comprender los datos recolectados para que se conviertan en información relevante para la investigación. En muchas ocasiones en esta etapa las actividades que realizan por los expertos forenses pueden incluir recuperación de archivos borrados, análisis de registros de actividades, la extracción de metadatos y aclarar sus hallazgos (Nelson, Phillips, & Steuart, 2018).

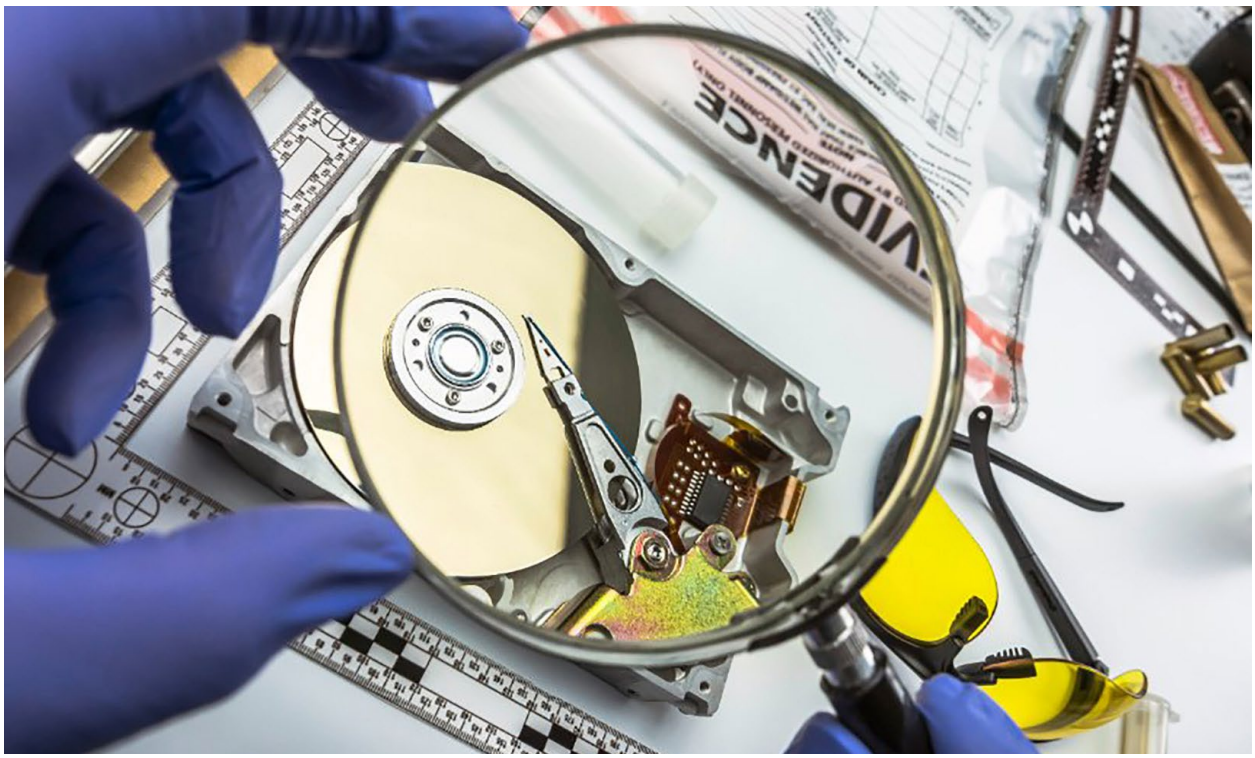
Presentación.– En esta etapa, quizás la última pero no la menos importante, es donde el experto forense presentara, explicará y defenderá sus hallazgos y métodos frente a un tribunal, con una disertación clara y comprensible, permitiendo que tanto el juez como los demás sujetos procesales entiendan su relevancia, fiabilidad y comprobación científica (Sammons, 2012).

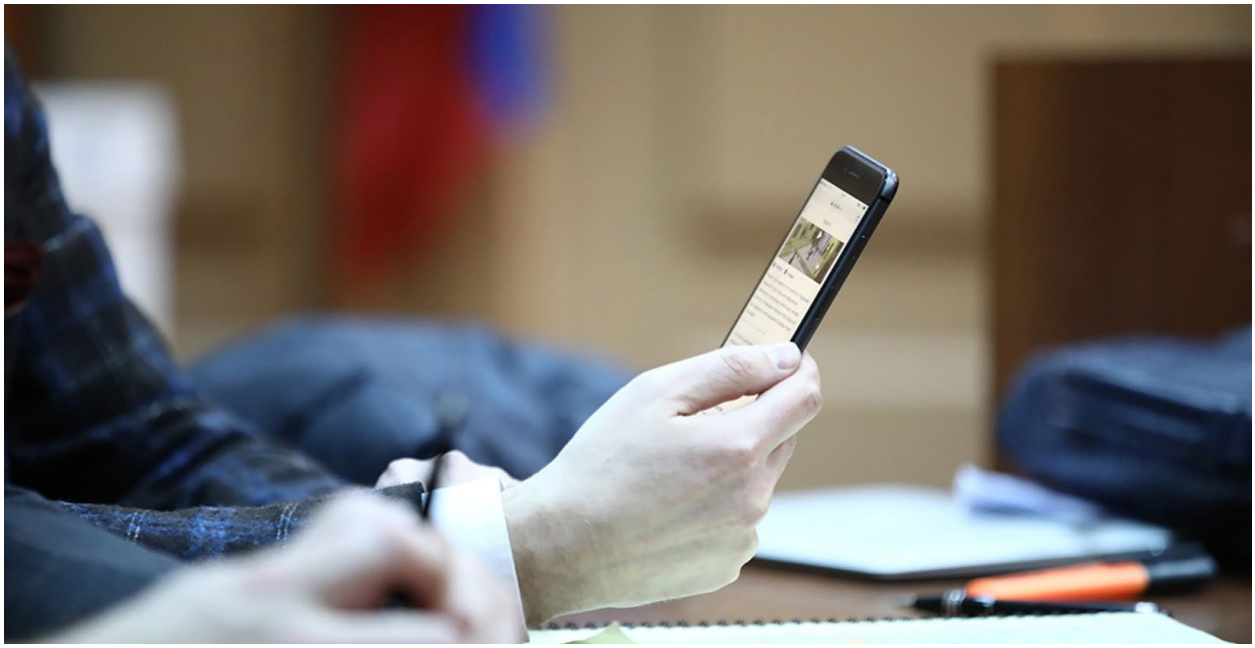
Desafíos

Siempre existirán desafíos asociados a cualquier actividad en el mundo físico y más aún en el mundo digital, donde el manejo de evidencia digital siempre estará expuesto por su naturaleza y los embates asociados a los avances tecnológicos, a continuación, se mencionarán algunos:

Integridad y Autenticidad.- Este desafío implica una importancia relevante puesto que, cualquier alteración que puedan experimentar los datos, ya sea dolosa, culposa o accidental, puede poner en riesgo la validez de la evidencia. Para mitigar este desafío es trascendental que se aplican técnicas hash que permitan verificar la integridad de los datos (Carrier, 2005).

Complejidad Técnica.- El análisis de evidencia digital requiere un alto nivel de habilidad técnica y conocimiento especializado, es por ello, que los expertos forenses deben estar siempre a la vanguardia de los avances tecnológicos y familiarizados con una amplia variedad de sistemas operativos, aplicaciones y tecnologías de almacenamiento y por consiguiente deben mantenerse





actualizados sobre nuevas técnicas y herramientas forenses (Nelson, Phillips, & Steuart, 2018).

Volumen de Datos.- Este desafío está asociado a la cantidad de datos que pueden ser recolectados en una investigación, lo cual para el experto forense puede resultar abrumador, angustioso y en ocasiones dificultoso al momento de interpretar y generar información significativa, por consiguiente, los expertos e investigadores del caso deberán poseer la capacidad de filtrar, ubicar y priorizar la información relevante, lo cual puede representar una tarea compleja y que demanda mucho tiempo (Sammons, 2012).

Privacidad y legalidad.– Dentro del ambiente englobante que está asociado a una investigación donde se vaya a realizar el manejo de evidencia digital, es preponderante que se cumpla con los recaudos legales necesarios para que la información resultante tenga una validez jurídica, así como también conocer, comprender y practicar las regulaciones contenidas en la protección y privacidad de los datos y de las personas. Con lo cual se asegura que la recolección y el análisis se realicen de manera legal y ética (Casey, 2011).

Conclusión

El manejo de evidencia digital es un campo en constante evolución que juega un papel crucial en la investigación forense en la actualidad. Sus características únicas y desafíos requieren un enfoque especializado y riguroso para asegurar la integridad y validez de los datos presentados ante un tribunal. De igual forma con el avance continuo de las tecnologías de información y telecomunicaciones, es fundamental que los expertos forenses se mantengan a la vanguardia de las actualizaciones de las últimas técnicas y herramientas disponibles; y todo esto compenetrado con la capacitación continua eficiente y eficaz.

Referencias

Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed., pp. 15-18). Academic Press.

Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley Professional.

National Institute of Standards and Technology. (2015). SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. Retrieved from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

Nelson, B., Phillips, A., & Steuart, C. (2018). Guide to Computer Forensics and Investigations. Cengage Learning.

Sammons, J. (2012). The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Syngress.

Scientific Working Group on Digital Evidence. (2016). SWGDE Digital & Multimedia Evidence Glossary (Version 3.0). https://www.swgde.org/documents/Current%20Documents/SWGDE%20Digital%20and%20Multimedia%20Evidence%20Glossary