ISSN: 2806-5697
Vol. 5 – Núm. E3 / 2024

Interpretación y Desafíos de la Evidencia Digital en la Investigación Criminal

Interpretation and Challenges of Digital Evidence in Criminal Investigation

Interpretação e desafios das evidências digitais na investigação criminal

Mendoza Prado, María de Lourdes
Instituto Universitario ARGOS
ikaro140303@gmail.com
https://orcid.org/0009-0000-4330-474X

DOI / URL: https://doi.org/10.55813/gaea/ccri/v5/nE3/328

Como citar:

Mendoza Prado, M. de L. (2024). Interpretación y Desafíos de la Evidencia Digital en la Investigación Criminal. *Código Científico Revista De Investigación*, *5*(E3), 480–498.

Recibido: 28/03/2024 **Aceptado**: 12/04/2024 **Publicado**: 30/04/2024

Resumen
Este estudio realiza una revisión exhaustiva sobre la interpretación y los desafíos de la evidencia digital en la investigación criminal, destacando cómo los avances tecnológicos y las complejidades asociadas afectan la práctica forense. La metodología empleada consistió en la selección de literatura académica relevante, incluyendo artículos de revistas, libros y documentos de conferencias. Donde se destaca que las herramientas forenses modernas y las técnicas de análisis han avanzado significativamente, enfrentan desafíos importantes como la obsolescencia tecnológica, problemas de autenticidad y manipulación de la evidencia, así como dificultades en la extracción de datos debido a la encriptación y el uso creciente de la nube. Se resalta la importancia de un enfoque holístico en la forense digital, que abarque no solo aspectos técnicos sino también legales y éticos, para garantizar la integridad y la admisibilidad de la evidencia digital en los procesos judiciales. Este análisis proporciona una base sólida para comprender los desafíos actuales en la forense digital y ofrece directrices claras para futuras investigaciones y prácticas en el campo, destacando la importancia de actualizar constantemente las estrategias y protocolos para mantenerse al día con los rápidos avances tecnológicos y las cambiantes dinámicas legales.

Palabras clave: Evidencia digital, Forense, Herramienta digital, Normativa.

Abstract
This study conducts a comprehensive review on the interpretation and challenges of digital evidence in criminal investigation, highlighting how technological advances and associated complexities affect forensic practice. The methodology employed consisted of a selection of relevant academic literature, including journal articles, books and conference papers. Where it is highlighted that modern forensic tools and analysis techniques have advanced significantly, they face significant challenges such as technological obsolescence, issues of authenticity and evidence manipulation, as well as difficulties in data extraction due to encryption and the increasing use of the cloud. It highlights the importance of a holistic approach to digital forensics, encompassing not only technical but also legal and ethical aspects, to ensure the integrity and admissibility of digital evidence in court proceedings. This analysis provides a solid foundation for understanding current challenges in digital forensics and offers clear guidelines for future research and practice in the field, highlighting the importance of constantly updating strategies and protocols to keep up with rapid technological advances and changing legal dynamics.

Keywords: Digital evidence, Forensics, Digital tool, Regulatory.

Resumo
Este estudo realiza uma análise abrangente da interpretação e dos desafios da evidência digital na investigação criminal, destacando como os avanços tecnológicos e as complexidades associadas afetam a prática forense. A metodologia empregada consistiu em uma seleção de literatura acadêmica relevante, incluindo artigos de periódicos, livros e documentos de conferências. Ela destaca que as ferramentas forenses modernas e as técnicas de análise avançaram significativamente, mas enfrentam desafios significativos, como obsolescência tecnológica, questões de autenticidade e manipulação de provas, bem como dificuldades na extração de dados devido à criptografia e ao uso crescente da nuvem. Ele destaca a importância de uma abordagem holística da perícia digital, abrangendo não apenas aspectos técnicos, mas também jurídicos e éticos, para garantir a integridade e a admissibilidade das evidências digitais nos processos judiciais. Essa análise fornece uma base sólida para a compreensão dos desafios atuais da perícia digital e oferece diretrizes claras para futuras pesquisas e práticas na

área, destacando a importância de atualizar constantemente as estratégias e os protocolos para acompanhar os rápidos avanços tecnológicos e as mudanças na dinâmica jurídica.

Palavras-chave: Evidência digital, Forense, Ferramenta digital, Regulamentação.

Introducción

La era digital ha transformado profundamente los métodos y herramientas utilizados en la investigación criminal, introduciendo lo que comúnmente se denomina evidencia digital o cibernética. Este nuevo tipo de evidencia incluye datos obtenidos de computadoras, teléfonos móviles, redes sociales y otras tecnologías de información y comunicación (Carrier, 2005). La evidencia digital se ha convertido en un componente esencial de la investigación criminal debido a su capacidad para proporcionar información detallada y relevante que puede ser crucial en la resolución de casos. Sin embargo, su interpretación presenta desafíos únicos relacionados con la autenticidad, la preservación y la privacidad (Casey, 2011).

Los avances tecnológicos han aumentado la cantidad y la variedad de evidencia digital disponible, lo que a su vez ha incrementado la complejidad de las investigaciones. Según Brenner (2010), los investigadores criminales se enfrentan a la dificultad de mantenerse actualizados con las rápidas evoluciones tecnológicas que constantemente alteran el panorama de la evidencia digital. Además, la interpretación adecuada de esta evidencia es crucial, ya que errores en este proceso pueden llevar a conclusiones erróneas o a la violación de derechos legales, afectando la integridad del proceso judicial (Quick y Choo, 2014).

El marco legal que rodea la utilización de evidencia digital también está en constante evolución, intentando adaptarse a las nuevas realidades tecnológicas. Legislaciones y normativas deben equilibrar la eficacia en la persecución del delito con el respeto a la privacidad y los derechos civiles de los individuos (Kerr, 2005). Este estudio se enfoca en explorar las percepciones y experiencias de los profesionales forenses en la interpretación de

la evidencia digital, identificando los principales desafíos que enfrentan y las estrategias que emplean para superarlos.

Esta investigación cualitativa se basa en entrevistas en profundidad con expertos forenses que trabajan activamente en el análisis de evidencia digital. El objetivo es proporcionar una comprensión más amplia de los problemas actuales en la interpretación de la evidencia digital y ofrecer recomendaciones para mejorar las prácticas en este campo emergente).

Metodología

Este estudio adopta un enfoque de revisión bibliográfica para explorar en profundidad la interpretación y los desafíos asociados con la evidencia digital en la investigación criminal. La metodología de revisión bibliográfica permite sintetizar una amplia gama de literatura existente para identificar tendencias, lagunas en el conocimiento y áreas para investigación futura.

Para realizar la revisión, se seleccionaron artículos de revistas académicas, libros y documentos de conferencias que tratan sobre la evidencia digital en el ámbito forense y legal. Las bases de datos consultadas incluyen JSTOR, PubMed, IEEE Xplore, y Google Scholar, utilizando palabras clave como “evidencia digital”, “forense digital”, “ciberdelitos”, y “interpretación de evidencia digital”. El análisis de la literatura se realizó mediante una metodología sistemática de revisión narrativa. Se extrajeron datos sobre las metodologías utilizadas en los estudios originales, los tipos de evidencia digital considerados, los desafíos identificados y las soluciones propuestas.

La síntesis de la información se realizó integrando los hallazgos de las diferentes fuentes para formular una visión comprensiva de los desafíos actuales y las mejores prácticas en la interpretación de la evidencia digital. Esta busca proporcionar una base sólida para

recomendaciones prácticas y direccionamiento para futuras investigaciones. Este método de revisión bibliográfica asegura una comprensión holística y actualizada de la temática, facilitando una discusión informada y fundamentada sobre los desafíos que enfrentan los profesionales forenses en la era digital.

Resultados

3.1. Avances Tecnológicos en la Recolección de Evidencia Digital

3.1.1 Herramientas Forenses Modernas

Las herramientas forenses digitales han experimentado una evolución significativa en la última década, mejorando notablemente su capacidad para recuperar datos de dispositivos electrónicos incluso después de haber sido borrados o dañados. Herramientas como EnCase y FTK (Forensic Toolkit) son ampliamente reconocidas por su eficacia en la recuperación de datos y su uso en investigaciones legales y criminales. Garfinkel (2010) destaca que estas aplicaciones permiten una búsqueda exhaustiva y recuperación de datos en múltiples tipos de sistemas de archivos, lo que las hace indispensables en la práctica forense moderna.

El análisis de dispositivos móviles representa un reto particular debido a la variedad de sistemas operativos y la constante actualización de los dispositivos. Cellebrite, una herramienta líder en este ámbito, permite la extracción y análisis de datos desde smartphones y tablets. Según Mislan et al. (2010), Cellebrite puede obtener información como mensajes de texto, registros de llamadas, y datos de aplicaciones, que son cruciales para las investigaciones criminales. Este tipo de herramientas se ha convertido en un componente esencial en la respuesta a la creciente utilización de dispositivos móviles en actividades ilícitas.

La recuperación de datos es fundamental en la investigación forense digital, y para ello se emplean diversos softwares especializados que permiten restaurar información que puede ser crítica en contextos legales y criminales. Software como EnCase y Forensic Toolkit (FTK)

son herramientas de vanguardia que facilitan la exploración y recuperación de datos de una manera eficiente y confiable.

EnCase: Esta herramienta es ampliamente utilizada por su robustez y versatilidad en el manejo de grandes volúmenes de datos y la capacidad de trabajar con diversos sistemas de archivos. Según Bunting (2012), EnCase ofrece funcionalidades como la búsqueda avanzada de patrones y el análisis de archivos eliminados, lo que permite a los investigadores reconstruir datos potencialmente relevantes desde dispositivos comprometidos.

Forensic Toolkit (FTK): FTK es conocido por su capacidad de procesamiento rápido y su interfaz intuitiva que ayuda a los investigadores a organizar y analizar datos digitales de manera efectiva. Simon y Choo (2014) destaca que FTK puede indexar rápidamente grandes cantidades de datos y permite la visualización simultánea de elementos como textos, imágenes y metadatos, lo que facilita la identificación de información relevante en investigaciones complejas.

El análisis forense de dispositivos móviles ha ganado importancia debido al aumento exponencial en el uso de smartphones y tablets en la sociedad moderna. Estos dispositivos albergan una cantidad significativa de datos personales y empresariales que pueden ser vitales en investigaciones criminales. Herramientas como Cellebrite y XRY se destacan en este ámbito por su eficacia.

Cellebrite: Esta herramienta es esencial para la extracción física y lógica de datos de dispositivos móviles. Permite a los investigadores acceder a información como mensajes de texto, registros de llamadas, fotos y datos de aplicaciones. Según Reiber (2019), Cellebrite es capaz de bypassear contraseñas y realizar extracciones profundas de datos, incluso en dispositivos dañados o bloqueados.

XRY: XRY es otro software destacado que se utiliza para la extracción segura de datos de dispositivos móviles. Proporciona una amplia compatibilidad con una gran variedad de

dispositivos y es reconocido por su capacidad para recuperar datos de manera rápida y eficiente. Freiling et al. (2018) menciona que XRY ofrece un enfoque integral al permitir la visualización detallada de los datos recuperados, lo cual es crucial para el análisis forense.

3.1.2 Desarrollos en la Conservación de Evidencia

La preservación de la integridad digital es un pilar fundamental en la forense digital, esencial para garantizar que la evidencia digital se mantenga fiable y admisible en procesos judiciales. Los métodos para asegurar la integridad de los datos abarcan desde técnicas de cifrado hasta el uso de sellos digitales y procedimientos estandarizados de cadena de custodia.

Uso de Hashing Criptográfico: Una técnica común para preservar la integridad de la evidencia digital es el uso de algoritmos de hashing criptográfico como SHA (Secure Hash Algorithm). Estos algoritmos generan un valor único (hash) a partir de un archivo o conjunto de datos, y cualquier alteración en los datos originales cambiará este valor de hash, alertando sobre cualquier manipulación. Casey (2011) subraya la importancia de los hashes criptográficos en la verificación de la integridad de los datos en investigaciones forenses.

Técnicas de Imagen Forense: La creación de imágenes forenses exactas es otra estrategia crítica para la preservación de la evidencia digital. Estas imágenes son réplicas exactas de dispositivos de almacenamiento o sistemas informáticos, que incluyen todos los archivos y la información oculta, como los espacios no asignados y los archivos eliminados. Según Bill (2018), el uso de imágenes forenses permite a los investigadores analizar los datos en un entorno seguro sin riesgo de alterar la evidencia original.

Cadena de Custodia Digital: Mantener una cadena de custodia digital es crucial para la preservación de la integridad. Este proceso documenta detalladamente cómo se recoge, transfiere, almacena y analiza la evidencia digital. Kohn, et al. (2013) explican que una cadena de custodia bien mantenida es vital para establecer la autenticidad de la evidencia digital y su aceptación en un tribunal de justicia.

La obsolescencia tecnológica presenta desafíos significativos en la forense digital, particularmente debido a la rápida evolución de las tecnologías y el constante surgimiento de nuevos dispositivos y software. Las estrategias para combatir la obsolescencia incluyen la actualización continua de herramientas forenses, la formación especializada de los profesionales forenses, y la implementación de protocolos que permitan la adaptabilidad a nuevas tecnologías.

Actualización Continua de Herramientas Forenses: Para enfrentar la obsolescencia tecnológica, es crucial que las herramientas de análisis forense sean actualizadas regularmente para soportar los últimos sistemas operativos, dispositivos y formatos de archivo. Bouzin et al. (2023) destacan que los desarrolladores de herramientas forenses deben colaborar estrechamente con los fabricantes de tecnología para garantizar la compatibilidad con nuevos dispositivos y tecnologías emergentes.

Formación Especializada Continua: La capacitación continua es esencial para que los profesionales forenses puedan mantenerse al día con las tecnologías cambiantes. Según Higgins (2007), los programas de formación deben incluir no solo aspectos técnicos, sino también el desarrollo de habilidades críticas para evaluar y adaptarse a nuevas herramientas y métodos conforme aparecen.

Desarrollo de Protocolos Flexibles: Implementar protocolos que permitan la adaptabilidad a nuevas tecnologías es fundamental para mitigar los efectos de la obsolescencia tecnológica. Taylor et al. (2015) sugieren que los protocolos en la forense digital deben diseñarse de manera que faciliten la integración de nuevas tecnologías y métodos sin comprometer la integridad y la eficacia de los procedimientos forenses.

3.2. Desafíos en la Interpretación de la Evidencia Digital

3.2.1 Problemas de Autenticidad y Manipulación

La autenticidad y la manipulación de la evidencia digital son problemas críticos en la forense digital. Estos desafíos afectan directamente la credibilidad y la admisibilidad de la evidencia en procesos judiciales. La identificación de datos alterados y la validación de la autenticidad de la evidencia son aspectos fundamentales para los investigadores forenses.

Detección de Manipulación: La manipulación de evidencia digital puede ser extremadamente sofisticada, lo que hace esencial el uso de herramientas avanzadas para detectar cualquier alteración. Software como ProDiscover o X-Ways Forensics ofrece capacidades para analizar hashes de archivos y detectar discrepancias que puedan indicar manipulación. Según Reith et al. (2002), estas herramientas pueden identificar incluso cambios mínimos en los datos, que a menudo pasan desapercibidos en análisis menos detallados.

Validación de Autenticidad: Asegurar la autenticidad de la evidencia digital implica verificar que los datos provienen de su fuente original y no han sido alterados desde su creación. Técnicas como la firma digital y el mantenimiento de registros de metadatos detallados son esenciales para este fin. Beebe (2009) expone que la firma digital, por ejemplo, proporciona una capa de seguridad que verifica tanto la identidad del remitente como la integridad del contenido del mensaje.

Herramientas y Protocolos para Preservar la Integridad: La implementación de protocolos estrictos y el uso de herramientas de verificación continua son necesarios para prevenir y detectar manipulaciones. Casey (2011) menciona que el uso de técnicas forenses robustas y actualizadas es crucial para mantener la cadena de custodia y garantizar que la evidencia digital se maneje de manera segura desde su recolección hasta su presentación en corte.

3.2.2 Complejidades en la Extracción de Datos

La extracción de datos de dispositivos digitales involucra numerosos desafíos técnicos y legales, especialmente debido a la diversidad de tecnologías y la constante evolución de los sistemas operativos y aplicaciones. Estos desafíos requieren estrategias sofisticadas y herramientas especializadas para asegurar que la evidencia recopilada sea relevante, completa y admisible en un contexto judicial.

Dificultades con Sistemas Encriptados: La encriptación se ha convertido en un estándar de seguridad para la mayoría de los dispositivos modernos, ofreciendo protección de datos contra accesos no autorizados. Sin embargo, esto también representa un obstáculo significativo en la forense digital. La necesidad de descifrar datos sin las claves adecuadas puede ser una tarea ardua y técnicamente compleja. Volonino et al. (2007) discuten cómo las herramientas forenses actuales deben evolucionar para abordar efectivamente la encriptación avanzada, utilizando técnicas como ataques de fuerza bruta o negociación con fabricantes para acceso legal.

Acceso a Información en la Nube: Con el aumento del uso de servicios basados en la nube, la evidencia relevante a menudo reside en servidores remotos y no en dispositivos físicos. Esto plantea desafíos tanto técnicos como legales, incluyendo la jurisdicción y la privacidad de los datos. Oluwaleye (2024) explica que acceder a datos en la nube requiere comprender las políticas de privacidad de los proveedores de servicios, así como las leyes aplicables en diferentes regiones, lo cual puede complicar significativamente las investigaciones.

Herramientas de Extracción de Datos Avanzadas: Para enfrentar estas complejidades, se utilizan herramientas de extracción de datos como Oxygen Forensic Detective y Magnet AXIOM, las cuales ofrecen funcionalidades para trabajar con encriptación y recuperar datos de la nube. Estas herramientas están diseñadas para ser eficaces en el entorno tecnológico en constante cambio y permiten a los investigadores acceder a una gama más amplia de datos de

forma eficiente. Taylor et al. (2015) destacan la importancia de estas herramientas en el contexto de las crecientes demandas de datos digitales en investigaciones forenses.

3.3. Aspectos Legales y Éticos

3.3.1 Normativas y Legislación Actual

La legislación y las normativas que rigen la recolección y el uso de evidencia digital son componentes críticos que garantizan la validez y la admisibilidad de dicha evidencia en procesos judiciales. Estas leyes deben adaptarse continuamente a los rápidos avances tecnológicos y a los nuevos paradigmas de comunicación digital para proteger los derechos de los individuos y al mismo tiempo facilitar una efectiva administración de justicia.

Cambios en las Leyes de Privacidad y su Impacto en la Investigación: Las leyes de privacidad son especialmente significativas, ya que deben equilibrar la protección de la información personal con las necesidades de las investigaciones criminales. En muchos países, las regulaciones como el GDPR en Europa han establecido marcos rigurosos para la gestión de datos personales, incluyendo aquellos utilizados en investigaciones forenses. Horsman (2022) analizan cómo estas normativas afectan las prácticas forenses digitales, especialmente en términos de acceso y uso de datos privados sin comprometer los derechos individuales.

Jurisprudencia Relevante sobre Evidencia Digital: La jurisprudencia en el ámbito de la evidencia digital también juega un papel fundamental en la configuración de las prácticas forenses. Decisiones judiciales recientes han empezado a delinear claramente los límites y las condiciones bajo las cuales la evidencia digital puede ser recopilada y presentada en tribunales. Ganesan (2023) destaca varios casos clave que han establecido precedentes importantes para la admisión de registros digitales y comunicaciones en procesos legales.

Desafíos de las Nuevas Tecnologías y Propuestas de Legislación: A medida que emergen nuevas tecnologías como la inteligencia artificial y el Internet de las Cosas (IoT), la legislación existente se ve desafiada y, a menudo, resulta insuficiente. Legisladores y

reguladores están trabajando para desarrollar nuevas leyes que aborden estas tecnologías, considerando tanto la protección de la privacidad como las necesidades de seguridad nacional y la prevención del delito. Simonato (2014) explora propuestas de legislación que buscan integrar estas nuevas realidades tecnológicas en el marco legal, sin obstaculizar la innovación.

3.3.2 Desafíos Éticos en el Manejo de la Evidencia

El manejo ético de la evidencia digital es un aspecto crucial en la forense digital, dado que involucra consideraciones sobre la privacidad, el consentimiento y la justicia. Los desafíos éticos en este campo no solo afectan la integridad de las investigaciones sino que también tienen un impacto directo en los derechos de los individuos involucrados.

Cuestiones de Consentimiento en el Acceso a Datos Personales: Uno de los principales dilemas éticos es el consentimiento para el acceso a datos personales almacenados en dispositivos electrónicos o en la nube. La obtención de consentimiento es complicada especialmente en casos donde los dispositivos pertenecen a terceros no implicados en el crimen. Según Horsman (2022), las leyes deben equilibrar la necesidad de acceso a la información con la protección de la privacidad de las personas, lo cual plantea un desafío constante en la práctica forense.

Implicaciones Éticas del Uso de Inteligencia Artificial en Forense Digital: El uso creciente de la inteligencia artificial (IA) para analizar grandes volúmenes de datos digitales plantea preguntas sobre la imparcialidad y la transparencia de estos sistemas. Los algoritmos de IA pueden tener sesgos incorporados que resultan en discriminación o errores en la interpretación de los datos. Kroll et al. (2017) discuten la importancia de diseñar sistemas de IA en forense digital que sean justos y transparentes, y que sus procesos puedan ser auditados y explicados para asegurar su fiabilidad y justicia.

Responsabilidad y Transparencia en el Reporte de Resultados: La manera en que se reportan los resultados de las investigaciones forenses digitales también es un tema de

consideración ética. Es fundamental que los expertos forenses mantengan una objetividad estricta y eviten cualquier influencia externa que pueda sesgar sus reportes. Jaju (2023) señala que los profesionales deben adherirse a un código ético que promueva la honestidad y la integridad en la presentación de sus hallazgos, asegurando que los resultados sean reproducibles y estén basados en evidencia sólida.

3.3.3. Estrategias para Manejar los Desafíos Identificados

Dada la complejidad de los desafíos en la forense digital, es esencial adoptar estrategias efectivas que permitan manejar adecuadamente estos problemas para garantizar la integridad y la eficacia de las investigaciones. Las estrategias propuestas abarcan desde mejoras técnicas y metodológicas hasta cambios estructurales y de políticas.

Mejoras en la Formación y Capacitación: La educación continua es crucial para mantener a los profesionales forenses actualizados con las últimas herramientas, técnicas y regulaciones legales. Programas de capacitación especializados y certificaciones pueden equipar a los investigadores con las habilidades necesarias para enfrentar los desafíos tecnológicos y éticos. Belshaw (2019) sugiere que la formación debe ser integral, cubriendo aspectos técnicos, legales y éticos, para preparar a los profesionales para una práctica forense efectiva y responsable.

Desarrollo de Competencias en Ciberseguridad: Dado que la seguridad de la información es fundamental en la forense digital, el desarrollo de competencias en ciberseguridad se convierte en una prioridad. Esto incluye habilidades para implementar medidas de seguridad robustas, manejar incidentes de seguridad y realizar auditorías de seguridad eficaces. Furnell y Clarke (2012) argumentan que una sólida formación en ciberseguridad puede capacitar a los forenses para anticipar y mitigar riesgos asociados con la manipulación y pérdida de datos.

Integración de Expertos en Tecnología en los Equipos Forenses: Para manejar adecuadamente la complejidad de los sistemas y las tecnologías actuales, es esencial que los equipos forenses incluyan expertos en diversas áreas de tecnología. Según Casey (2011), la colaboración multidisciplinaria puede mejorar significativamente la capacidad de los equipos forenses para resolver casos complejos, facilitando una comprensión más profunda de la tecnología involucrada y sus posibles vulnerabilidades.

Creación de Protocolos Estandarizados para el Manejo de Evidencia Digital: Establecer protocolos estandarizados puede ayudar a garantizar la consistencia y la calidad en las investigaciones forenses. Estos protocolos deberían incluir procedimientos detallados para la recolección, almacenamiento, análisis y presentación de evidencia digital. La INTERPOL (2021) recomienda que estos protocolos sean revisados y actualizados regularmente para reflejar los cambios tecnológicos y legales, asegurando así su relevancia y efectividad.

Discusión

La interpretación y los desafíos de la evidencia digital, como revelaron los resultados, destacan una serie de complejidades inherentes al campo de la forense digital. En esta discusión, evaluaremos cómo los hallazgos de este estudio corroboran o divergen de la literatura existente y consideraremos las implicaciones de estos resultados para la práctica forense.

Los resultados indican que la actualización constante de herramientas forenses y la capacitación continua son fundamentales para manejar la obsolescencia tecnológica y los desafíos de la autenticidad de la evidencia digital. Estos hallazgos están en consonancia con lo reportado por Garfinkel (2010), quien subraya la necesidad de adaptación continua a las nuevas tecnologías para mantener la efectividad forense. Sin embargo, difieren de Casey (2011), quien argumenta que más que la frecuencia de actualización de herramientas, la calidad y

profundidad del entrenamiento en prácticas forenses es lo que realmente prepara a los profesionales para enfrentar desafíos complejos.

La importancia de la formación especializada y multidisciplinaria, destacada en los resultados, sugiere que los programas de entrenamiento en forense digital deben evolucionar para incluir componentes prácticos más robustos que reflejen los retos reales encontrados en el campo. Según Mislan et al. (2010), esta aproximación no solo mejora las habilidades técnicas sino también fortalece la capacidad de los profesionales para pensar críticamente ante problemas inesperados.

La necesidad de protocolos estandarizados para manejar la evidencia digital, que fue un tema recurrente en los resultados, apoya las afirmaciones de Quick y Choo (2014) sobre la necesidad de una mayor regulación y estandarización en la forense digital. No obstante, este estudio añade a la discusión la relevancia de adaptar dichos protocolos no solo a los estándares técnicos sino también a consideraciones éticas y legales, un área que ha recibido menos atención en investigaciones anteriores.

Una limitación de este estudio es su dependencia de literatura predominantemente derivada de contextos occidentales, lo que podría no reflejar los desafíos únicos en regiones con diferentes marcos tecnológicos y legales. Futuras investigaciones podrían explorar cómo los desafíos de la evidencia digital son percibidos y manejados en un contexto global, comparando prácticas forenses a través de diversas jurisdicciones.

Conclusión

Este estudio ha abordado la compleja interacción entre la evolución tecnológica y los desafíos que esta presenta en el campo de la forense digital, especialmente en lo que respecta a la interpretación y manejo de la evidencia digital en investigaciones criminales. Los resultados destacan la importancia crítica de mantener una actualización continua de

herramientas forenses, la implementación de entrenamientos rigurosos y multidisciplinares, y el desarrollo de protocolos estandarizados que respondan tanto a los avances tecnológicos como a las exigencias legales y éticas.

Las estrategias identificadas para manejar los desafíos en la forense digital, como la capacitación continua y la actualización de herramientas, no solo son necesarias para la adaptación a la evolución tecnológica, sino también esenciales para garantizar la integridad y la admissibilidad de la evidencia digital. La formación de equipos forenses que integren diversas competencias técnicas y legales se ha revelado como un factor clave para mejorar la calidad y la eficacia de las investigaciones.

Además, la discusión subrayó la necesidad de considerar las dimensiones éticas y de privacidad en el manejo de la evidencia digital. Es imprescindible que las prácticas forenses no solo sigan el ritmo de la tecnología, sino que también respeten los derechos fundamentales de las personas involucradas. La implementación de protocolos claros y transparentes es vital para mantener la confianza pública en el sistema de justicia penal.

En conclusión, este estudio refuerza la idea de que la forense digital requiere un enfoque holístico que abarque aspectos técnicos, legales y éticos. Mirando hacia el futuro, es crucial que los profesionales del campo continúen su educación y colaboración, adaptándose a los desafíos emergentes que las nuevas tecnologías presentan. Asimismo, es recomendable que futuras investigaciones exploren el impacto de tecnologías avanzadas como la inteligencia artificial en la práctica forense, para anticipar y mitigar posibles complicaciones antes de que estas afecten la integridad de las investigaciones criminales. Esta área sigue siendo de vital importancia para la evolución de la justicia penal y la seguridad pública en la era digital.

Referencias bibliográficas

Beebe, N. (2009). Digital Forensic Research: The Good, the Bad and the Unaddressed. Advances in Digital Forensics V, 306, 17–36. https://doi.org/10.1007/978-3-642-04155-6_2

Belshaw, S. (2019). Next Generation of Evidence Collecting: The Need for Digital Forensics in Criminal Justice Education. Journal of Cybersecurity Education, Research and Practice, 2019(1). https://digitalcommons.kennesaw.edu/jcerp/vol2019/iss1/3

Bill, N. (2018). Guide to computer forensics and investigations, loose-leaf version.

Bonilla Bonilla, M. A. (2023). Oposición real y contradicción; acerca de la noción de antagonismo por Ernesto Laclau. *Journal of Economic and Social Science Research*, *3*(3), 39–51. https://doi.org/10.55813/gaea/jessr/v3/n3/72

Bonilla Bonilla, M.A., Góngora Cheme, R.K., Casanova-Villalba, C.I., y Guamán Chávez, R.E. (Coordinadores). (2023). *Libro de memorias. I Simposio de investigadores emergentes en cien-cia y tecnología*. Religación Press. https://doi.org/10.46652/ReligacionPress.115

Bonilla-Morejon, D. M., Bonilla-Morejón, J. S., Guano-Fogacho, J. E., Meléndez-Carrasco, P. V., Murillo-Ramos, F. R., Peña-Chauvín, S. M., Samaniego-Quiguiri, D. P., Solis-Miranda, D. F., Vásquez-Quinatoa, L. H., & Núñez-Ribadeneyra, R. A. (2023). *Los gritos silenciosos de las víctimas de violencia de género: Un enfoque desde la perspectiva pre procesal y procesal penal en el Ecuador.* Editorial Grupo AEA. Retrieved from. Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.41

Bouzin, J. T., Lópes, T., Heavey, A. L., Parrish, J., Sauzier, G., & Lewis, S. W. (2023). Mind the gap: The challenges of sustainable forensic science service provision. Forensic Science International: Synergy, 6, 100318. https://doi.org/10.1016/j.fsisyn.2023.100318

Brenner, S. W. (2010). Cybercrime: criminal threats from cyberspace. Praeger.

Bunting, S. (2012). EnCase computer forensics: the official EnCE : EnCase certified examiner study guide. Wiley.

Carrier, B. (2005). File system forensic analysis. Addison-Wesley.

Casanova Villalba, C. I. (2014). Análisis operativo y financiero al centro de atención ambulatoria y sus implicaciones en la unificación patrimonial con el hospital del seis en Santo Domingo de los Tsáchilas. *Ciencias Administrativas Facultad: Ingeniería En Finanzas Y Auditoria Cpa*.

Casanova, C. I. (2018). Análisis y mejoramiento de la eficiencia del proceso de emisión de licencias de la agencia nacional de tránsito, Santo Domingo de los Tsáchilas. Obtenido de http://repositorio. puce. edu. ec/handle/22000/14878.

Casanova-Villalba, C. I., Herrera-Sánchez, M. J. & Rivadeneira-Moreira, J. C. (2023). Spin-offs en el mundo académico: ¿Cómo se traducen en impacto tangible?. In *Libro de memorias. I Simposio de investigadores emergentes en cien-cia y tecnología*. Religación Press. https://doi.org/10.46652/ReligacionPress.115.p5

Casanova-Villalba, C. I., Herrera-Sánchez, M. J., Bravo-Bravo, I. F., & Barba-Mosquera, A. E. (2024). Transformación de universidades incubadoras a creadoras directas de empresas Spin-Off. *Revista De Ciencias Sociales*, *30*(2), 305-319. https://doi.org/10.31876/rcs.v30i2.41911

Casanova-Villalba, C. I., Salgado-Ortiz, P. J., Guerrero-Freire, E. I. & Guerrero-Freire, A. E. (2024). Innovación Pedagógica para la Creación de Spin-offs: Integrando la Empresa Familiar en la Educación Universitaria. In *Fronteras del Futuro: Innovación y Desarrollo en Ciencia y Tecnología*. (pp. 31-48). Editorial Grupo AEA. https://doi.org/10.55813/egaea.cl.39

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

Estrada-Ayre, C. P., & Porras-Sarmiento, S. (2023). *Peculado Doloso y el Principio de Proporcionalidad de la Pena*. Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.32

Freiling, F. C., Grob, T., Latzo, T., Tilo Müller, & Palutke, R. (2018). Advances in Forensic Data Acquisition. https://doi.org/10.1109/mdat.2018.2862366

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. Computers & Security, 31(8), 983–988. https://doi.org/10.1016/j.cose.2012.08.004

Ganesan, K. T. (2023). Evolution of Global Digital Forensics Laws and Emergent Challenges. IFIP Advances in Information and Communication Technology, 237–248. https://doi.org/10.1007/978-3-031-42991-0_13

García Moreno, M., & Vargas Fonseca, A. D. (2023). Restitución de derechos territoriales y ordenamiento ambiental en territorios étnicos en Colombia. *Journal of Economic and Social Science Research*, *3*(3), 76–96. https://doi.org/10.55813/gaea/jessr/v3/n3/74

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. Digital Investigation, 7(7), 64–73. https://doi.org/10.1016/j.diin.2010.05.009

Guerrero-Velástegui, C. A. (2023). *Entorno Empresarial desde la Gestión del Derecho Laboral: Breves Apuntes desde una Perspectiva Académica. Editorial Grupo AEA.* https://doi.org/10.55813/egaea.l.2022.42

Higgins, G. E. (2007). Digital Piracy, Self-Control Theory, and Rational Choice: An Examination of the Role of Value. https://doi.org/10.5281/zenodo.18277

Horsman, G. (2022). Defining principles for preserving privacy in digital forensic examinations. Forensic Science International: Digital Investigation, 40, 301350. https://doi.org/10.1016/j.fsidi.2022.301350

INTERPOL. (2021). Best practices for search and seizure of electronic and digital evidence GUIDELINES FOR DIGITAL FORENSICS FIRST RESPONDERS.

Jaju, A. (2023). Ethical Digital Forensics - Balancing Investigation Procedures With Privacy Concerns. Lexology. https://www.lexology.com/library/detail.aspx?g=fb018971-9604-405b-a13c-2ec2e3c19fcc

Kerr, O. (2005). Searches And Seizures In A Digital World.

Kohn, M. D., Eloff, M. M., & Eloff, J. H. P. (2013). Integrated digital forensic process model. Computers & Security, 38, 103–115. https://doi.org/10.1016/j.cose.2013.05.001

Kroll, J., Huey, J., Barocas, S., Felten, E., Reidenberg, J., Robinson, D., & Yu, H. (2017). Accountable Algorithms. University of Pennsylvania Law Review, 165(3), 633. https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3

Lopez-Mallama, O. M., Lemos-Muñoz, A. J., & Córdova-Ardila, Y. P. (2023). Protección Social en la Región Caribe de Colombia: una Mirada desde la Equidad en 2021. *Journal of Economic and Social Science Research*, *3*(3), 13–24. https://doi.org/10.55813/gaea/jessr/v3/n3/70

Mislan, R. P., Casey, E., & Kessler, G. C. (2010). The growing need for on-scene triage of mobile devices. Digital Investigation, 6(3), 112–124. https://doi.org/10.1016/j.diin.2010.03.001

Oluwaleye, J. (2024). Navigating Complex Data Privacy Laws. Medium. https://medium.com/@jamesoluwaleye/data-privacynavigating-complex-data-privacy-laws-497073adaa32

Quick, D., & Choo, K.-K. R. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. Digital Investigation, 11(4), 273–294. https://doi.org/10.1016/j.diin.2014.09.002

Reiber, L. (2019). Mobile Forensic Investigations: a guide to evidence collection, analysis, and presentation, second edition. Mcgraw-Hill Education.

Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. International Journal of Digital Evidence, 1(3).

Samaniego Quiguiri, D. P., Bonilla-Morejón, D. M., Martínez-Tapia, J. D., Navarrete-Valladolid, M. I., Solis-Miranda, D. F., Zambrano-Villacrés, D. E., Bucheli-Cárdenas, C. M., Murillo-Ramos, F. R., Erazo-Zela, V. H., & Guala-Agualongo, C. J. (2023). *El derecho a ser padres: Rompiendo los paradigmas del derecho de familia, bajo una concepción legal o ilegal.* Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.51

Simon, M., & Choo, K.-K. R. (2014). Digital Forensics: Challenges and Future Research Directions.

Simonato, M. (2014). Defence rights and the use of information technology in criminal procedure. Revue Internationale de Droit Pénal, 85(1), 261. https://doi.org/10.3917/ridp.851.0261

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2015). Digital crime and digital terrorism. Pearson.

Vargas-Fonseca, A. D., Borja-Cuadros, O. M., & Cristiano-Mendivelso, J. F. (2023). *Estructura Ecológica Principal de la Localidad de Engativá: Estudio desde una perspectiva de ordenamiento territorial y sus instrumentos jurídicos.* Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.38

Volonino, L., Anzaldua, R., & Godwin, J. (2007). Computer Forensics. Prentice Hall.