Instituto Superior Tecnológico "Los Andes" ISTLA

CÓDIGO CIENTÍFICO REVISTA DE INVESTIGACIÓN

Vol. 5 – Núm. 2 / Julio – Diciembre – 2024

Estudio de las técnicas y tecnologías que se emplean en la informática forense para afrontar la esteganografía digital

Study of the techniques and technologies used in computer forensics to confront digital steganography

Estudo das técnicas e tecnologias utilizadas em informática forense para enfrentar a esteganografia digital

Alexis Javier Pisco Meneses[1]
Universidad Técnica de Manabí
apisco8635@utm.edu.ec
https://orcid.org/0009-0000-6768-2577

Christian Ronald Torres Moran[2]
Universidad Técnica de Manabí
christian.torres@utm.edu.ec
https://orcid.org/0000-0002-6393-3794

DOI / URL: https://doi.org/10.55813/gaea/ccri/v5/n2/616

Como citar:
Pisco, A. & Torres, C. (2024). Estudio de las técnicas y tecnologías que se emplean en la informática forense para afrontar la esteganografía digital. Código Científico Revista de Investigación, 5(2), 1133-1157.

Recibido: *01/09/2024* ***Aceptado:*** *04/10/2024* ***Publicado:*** *31/12/2024*

Resumen

Este estudio tuvo como objetivo analizar las técnicas y tecnologías empleadas en la informática forense para abordar la esteganografía digital, una disciplina que involucra la ocultación de información dentro de archivos digitales. El enfoque metodológico de este trabajo incluyó una investigación documental y un estudio descriptivo, respaldados por entrevistas a expertos en informática forense y esteganografía digital. Como resultados se identificaron desafíos significativos para los profesionales, como la creciente sofisticación de la esteganografía y la complejidad en el análisis de datos ocultos. Adicionalmente, se obtuvo una valoración con base a una escala de 1 a 4, por parte de especialistas de informática forense, teniendo en cuenta criterios como facilidad de uso, velocidad de procesamiento, precisión y capacidad de recuperación de datos, lo que facilitó precisar que herramientas como Foremost, especializada en la detección de archivos esteganográficos, StegExpose para el análisis en imágenes y archivos multimedia, y Autopsy para la examinación de discos duros y metadatos, son de mayor versatilidad y preferencia entre los especialistas, esto a partir de la calificación promedio obtenida de 4 puntos para la primera; 3,8 puntos para la segunda y 3,8 puntos para la tercera herramienta. De lo anterior se concluye que las herramientas que tienen mayor preferencia ofrecen funcionalidades claves y una capacidad efectiva para abordar una variedad de escenarios forenses, además que, la elección de la técnica o tecnología apropiada para detectar esteganografía digital depende de diversos factores, como el tipo de archivo analizado y la sofisticación de la esteganografía utilizada.

Palabras Clave: archivos digitales, esteganografía digital, informática forense, datos ocultos, evidencia digital.

Abstract

This study aimed to analyze the techniques and technologies employed in digital forensics to address digital steganography, a discipline involving the concealment of information within digital files. The methodological approach of this work included documentary research and a descriptive study, supported by interviews with experts in digital forensics and steganography. The results identified significant challenges for professionals, such as the increasing sophistication of steganography and the complexity in analyzing hidden data. Additionally, an assessment based on a scale of 1 to 4 was obtained from digital forensics specialists, considering criteria such as ease of use, processing speed, accuracy, and data recovery capability, facilitating the determination that tools such as Foremost, specialized in detecting steganographic files, StegExpose for analysis in images and multimedia files, and Autopsy for examining hard drives and metadata, are more versatile and preferred among specialists, based on the average rating of 4 points for the first; 3.8 points for the second, and 3.8 points for the third tool. From the foregoing, it is concluded that the tools with greater preference they offer key functionalities and effective capability to address a variety of forensic scenarios, in addition to the choice of appropriate technique or technology to detect digital steganography depending on various factors, such as the type of file analyzed and the sophistication of the steganography used.

Key Words: digital files, digital steganography, computer forensics, hidden data, digital evidence.

Resumo

Este estudo teve como objetivo analisar as técnicas e tecnologias utilizadas na informática forense para abordar a esteganografia digital, uma disciplina que envolve a ocultação de informações dentro de arquivos digitais. A abordagem metodológica deste trabalho incluiu uma pesquisa documental e um estudo descritivo, apoiados por entrevistas com especialistas em informática forense e esteganografia digital. Como resultados, foram identificados desafios significativos para os profissionais, como a crescente sofisticação da esteganografia e a complexidade na análise de dados ocultos. Além disso, uma avaliação foi obtida com base em uma escala de 1 a 4, por especialistas em informática forense, levando em consideração critérios como facilidade de uso, velocidade de processamento, precisão e capacidade de recuperação de dados, o que ajudou a identificar que ferramentas como Foremost, especializada na detecção de arquivos esteganográficos, StegExpose para análise em imagens e arquivos multimídia, e Autopsy para exame de discos rígidos e metadados, são as mais versáteis e preferidas entre os especialistas, com uma pontuação média de 4 pontos para a primeira; 3,8 pontos para a segunda e 3,8 pontos para a terceira ferramenta. Dessa forma, conclui-se que as ferramentas mais preferidas oferecem funcionalidades-chave e uma capacidade eficaz para lidar com uma variedade de cenários forenses, além disso, a escolha da técnica ou tecnologia apropriada para detectar esteganografia digital depende de diversos fatores, como o tipo de arquivo analisado e a sofisticação da esteganografia utilizada.

Palavras-chave: arquivos digitais, esteganografia digital, computação forense, dados ocultos, evidências digitais.

Introducción

El ámbito de la informática forense ha ganado relevancia ineludible en la era digital, proveyendo un conjunto de herramientas y metodologías para la detección y abordaje de actividades ilícitas en entornos virtuales (Kävrestad, 2019) En este contexto, el creciente riesgo que plantea la esteganografía digital conlleva desafíos significativos para la salvaguardia de la información y la preservación de la integridad de los datos. La esteganografía digital, una técnica que conlleva la ocultación de información confidencial dentro de datos digitales aparentemente inofensivos, ha evolucionado hacia un nivel de sofisticación y complejidad que subraya la urgencia imperativa de tácticas y herramientas eficaces para la detección y neutralización de estas prácticas encubiertas (Majeed, et al., 2021).

Dentro del ámbito extenso de las transgresiones informáticas, la esteganografía digital ha adquirido una prominencia considerable entre aquellos que pretenden eludir la identificación y encubrir sus conductas delictivas (De Rosal, et al., 2023). Los expertos en informática forense

requieren una capacitación adecuada para detectar y descifrar comunicaciones encubiertas mediante el uso de metodologías y herramientas de análisis avanzadas (Nawal, et al., 2020) no obstante, a pesar de los avances notables en el campo de la informática forense, persiste una brecha evidente en la comprensión integral de las técnicas y tecnologías específicas empleadas para enfrentar la esteganografía digital. La necesidad de cerrar esta brecha se intensifica en un entorno en el que los perpetradores cibernéticos están empleando cada vez más tácticas encubiertas para evadir la detección y poner en peligro la seguridad de la información confidencial.

Aun cuando se han efectuado abordajes investigativos en torno al tema, la literatura existente sobre las técnicas y tecnologías aplicadas en la informática forense para contrarrestar la esteganografía digital se mantiene restringida en su alcance. A pesar de los esfuerzos continuos para mitigar las amenazas cibernéticas, se ha prestado escasa atención a la comprensión exhaustiva de las estrategias específicas que podrían fortalecer la capacidad de detección y recuperación de datos ocultos en medios digitales. De ahí la urgencia de realizar una exploración profunda y sistemática de dichas técnicas y tecnologías. En este contexto, una documental brinda una oportunidad valiosa para llenar el vacío existente y obtener una comprensión integral de las técnicas y tecnologías empleadas en la informática forense para enfrentar la esteganografía digital. Mediante un análisis crítico de la investigación existente y la recopilación de evidencia sustancial, esta revisión posee el potencial de arrojar luz sobre las prácticas más efectivas, herramientas destacadas y enfoques prometedores que podrían reforzar la capacidad de detección y mitigación de riesgos en entornos digitales cada vez más complejos.

Se anticipa que este estudio contribuirá significativamente al ámbito de la informática forense y la seguridad cibernética, proporcionando conocimientos fundamentales que puedan orientar la implementación de estrategias eficaces y el perfeccionamiento de las técnicas de

detección en la batalla contra la esteganografía digital. Al abordar las deficiencias existentes y resaltar las áreas de interés para futuras investigaciones, este artículo aspira a fomentar progresos notables en la protección de la integridad de los datos y la seguridad de la información en el entorno digital contemporáneo.

El propósito fundamental de este estudio implica llevar a cabo un análisis exhaustivo de las técnicas y tecnologías fundamentales que respaldan la práctica de la informática forense en el contexto específico de la esteganografía digital. Este enfoque comprende una evaluación minuciosa de las herramientas, enfoques y métodos empleados para la detección y el análisis de información enmascarada en archivos digitales, así como una valoración de su eficacia y limitaciones inherentes. Así mismo, se persigue la identificación de posibles deficiencias en las prácticas actuales de informática forense en lo referente a la esteganografía digital, junto con la formulación de recomendaciones dirigidas a mejorar la capacidad de detección y análisis forense en este campo.

Metodología

La metodología para el estudio tiene una investigación de tipo documental y alcance descriptivo. La investigación documental implica el análisis y revisión de documentos, registros, y literatura existente sobre el tema de estudio. En este caso, se utilizó para recopilar información detallada sobre las técnicas y tecnologías empleadas en la informática forense para abordar la esteganografía digital. Por otro lado, la investigación descriptiva persigue describir las características, propiedades y fenómenos del objeto de estudio sin manipular variables. En este contexto, se buscó describir detalladamente las prácticas y enfoques utilizados por profesionales de la informática forense en casos de esteganografía digital.

La estrategia de búsqueda documental se basó en un flujo de indagación aplicado en diversas fuentes académicas de renombre, como Scopus, Science Direct, Google Académico, Dialnet y Redalyc. Se utilizó una combinación de operadores booleanos AND, OR, NOT y

palabras claves para construir ecuaciones de búsqueda precisas como se visualiza en la Tabla 1. Esta metodología permitió obtener un conjunto representativo de fuentes relevantes que abordan específicamente las técnicas y tecnologías de la informática forense relacionadas con la esteganografía digital. La aplicación rigurosa de operadores booleanos en las ecuaciones de búsqueda garantizó la inclusión de estudios pertinentes y la exclusión de información no relevante para los objetivos de este trabajo.

Tabla 1
Términos empleados en la indagación en bases de datos científicas

	Término 1	**Término 2**	**Término 3**	**Término 4**
Sinónimo 1	Técnicas	Tecnologías	Informática Forense	Esteganografía digital
Sinónimo 2	Métodos	Herramientas	Peritaje digital	Ocultamiento digital
Sinónimo 3	Procedimientos	Dispositivos	Investigación forense digital	

En el proceso de indagación documental se establecieron criterios rigurosos de inclusión y exclusión para garantizar la relevancia y calidad de las fuentes seleccionadas. En primer lugar, se consideraron únicamente aquellas publicaciones científicas que datan de los últimos cinco años. Este criterio temporal se aplicó para asegurar la actualidad de la información y reflejar los avances más recientes en las técnicas y tecnologías de la informática forense relacionadas con la esteganografía digital. Además, se priorizaron fuentes provenientes de repositorios con destacada trayectoria científica y académica. Este enfoque buscó asegurar que las fuentes empleadas provengan de entornos de investigación respetados y que hayan sido sometidas a un proceso de revisión por pares, fortaleciendo así la validez y confiabilidad de la información recopilada.

El idioma de las fuentes no fue un criterio restrictivo, permitiendo la inclusión de estudios en diversos idiomas. Esta decisión se tomó para abarcar la mayor cantidad posible de conocimiento y perspectivas en el campo de la informática forense, así como de la esteganografía digital, independientemente del idioma de publicación. El objetivo principal fue asegurar una cobertura amplia y representativa de la literatura científica disponible en este

ámbito específico de estudio. Del proceso de indagación y cribado se obtuvieron 22 documentos claves para el abordaje del tema.

En la investigación, se dio especial atención a la calidad y relevancia de las fuentes empleadas. Se optó por una metodología que incluyó el análisis de información proveniente de empresas de renombre mundial en el ámbito de la tecnología y el desarrollo de soluciones tecnológicas aplicadas a la informática forense. Estas fuentes, con su reconocida trayectoria en el campo, aportaron perspectivas valiosas y datos fundamentales que enriquecieron la comprensión de las tendencias actuales y las tecnologías emergentes en la investigación forense digital.

El empleo de fuentes provenientes de estas empresas líderes permitió obtener información de primera mano sobre las innovaciones, avances y desafíos que enfrenta la informática forense en la actualidad. Además, se aseguró la confiabilidad y actualidad de los datos recopilados, ya que estas empresas suelen estar a la vanguardia de la investigación y el desarrollo en el ámbito tecnológico. Este enfoque metodológico fortaleció la calidad y la robustez de los resultados obtenidos, contribuyendo así a un análisis integral y actualizado de la intersección entre la tecnología y la informática forense. Entre las empresas consideradas se encuentran: IBM Corporation, Binary Intelligence LLC, Guidance Software Inc, AccessData Group LLC, KLDiscovery Inc, entre otros.

También, se utilizó la técnica de entrevistas a expertos para obtener evaluaciones y aportaciones fundamentales de especialistas cualificados en informática forense. Se aplicó una guía de entrevista estructurada para recopilar información valiosa de profesionales con experiencia en el campo, enriqueciendo así el estudio con perspectivas y conocimientos expertos. La guía fue estructura con planteamientos o preguntas específicas que facilitaran comprender las herramientas empleadas por especialistas en informática forense y esteganografía, así como compilar su valoración en torno a nivel de precisión en la detección

de datos ocultos, velocidad de procesamiento, facilidad de uso y capacidad de recuperación de datos.

La selección de entrevistados se basó en criterios que garantizan la relevancia y calidad de la información recopilada, centrándose en individuos altamente calificados y con experiencia en el campo. La utilización de una guía de entrevista estructurada aseguró la consistencia en la obtención de datos, abordando aspectos clave y facilitando un análisis más preciso de las respuestas de los entrevistados.

Para el análisis el estudio adoptó el método sintético, una estrategia de investigación científica que se destaca por su aplicación en la resolución de problemas complejos o en el estudio exhaustivo de fenómenos (López & Ramos, 2021) el enfoque sintético parte de analizar los componentes de manera aislada, ya que se orienta hacia la síntesis, buscando comprender las interrelaciones y mutuas influencias entre los elementos (Reyes, et al., 2022), bajo este método, se considera el sistema en su totalidad, abarcando el conjunto de técnicas y tecnologías que respaldan la informática forense en el tratamiento de la esteganografía digital.

Resultados

Beneficios y desafíos de la informática forense ante la esteganografía digital

El análisis de la Tabla 1 revela una serie de beneficios asociados con la aplicación de la informática forense en el contexto de la esteganografía digital. Autores como Moreno (2023) destacan la mejora en la detección de delitos mediante el uso de técnicas forenses avanzadas. Esta capacidad de identificar actividades delictivas ocultas dentro de datos digitales es fundamental para la aplicación efectiva de la justicia y la seguridad cibernética. Sin embargo, los beneficios no están exentos de desafíos (Arévalo & Hernández, 2021) la sofisticación creciente de las técnicas de esteganografía digital presenta un desafío considerable para los expertos en informática forense. La complejidad en el análisis de datos ocultos impone la

necesidad de desarrollar y perfeccionar constantemente las herramientas y metodologías utilizadas en la disciplina forense.

Prakash et al. (2021) resaltan la importancia de la colaboración interdisciplinaria como un beneficio adicional. La sinergia entre expertos en informática forense y especialistas en esteganografía digital permite abordar de manera más efectiva la complejidad de los delitos cibernéticos. No obstante, el desafío persiste en la necesidad de integrar tecnologías específicas para abordar la diversidad de métodos de ocultación de datos. En la Tabla 2 se sinterizan las ideas de los autores consultados en relación a los desafíos y beneficios de la informática forense.

Tabla 2
Síntesis de beneficios y desafíos comunes identificados

Beneficios	Desafíos
Mejora en la detección de delitos	Sofisticación creciente de esteganografía
Eficiencia en la recuperación de datos	Complejidad en el análisis de datos ocultos
Colaboración interdisciplinaria	Necesidad de técnicas avanzadas
Aplicación de algoritmos de aprendizaje	Integración de tecnologías específicas
Mejoras en la seguridad cibernética	Colaboración entre expertos especializados

Fuente: Elaborado con base en datos de estudios consultados.

Beneficios de la informática forense en distintas áreas

La aplicación de la informática forense abarca diversas áreas, siendo una herramienta valiosa en la litigación civil. Se destaca, según Al-Dhaqm et al. (2020) su papel en la recolección y análisis de evidencia incriminatoria que puede ser fundamental para procesar crímenes cometidos contra organizaciones y personas. Casos de fraude, discriminación, acoso y divorcio pueden, tal como destacan Mothi et al. (2020) beneficiarse significativamente de las técnicas y tecnologías de la informática forense, proporcionando una base sólida de evidencia para respaldar los procesos legales. En el ámbito de la investigación de seguros, la informática forense desempeña un papel crucial al ayudar a las compañías a disminuir los costos asociados con reclamos por accidentes y compensaciones. La evidencia recopilada de computadoras y otros dispositivos electrónicos puede según Arévalo et al. (2021) proporcionar una visión

detallada de los incidentes, permitiendo una evaluación precisa de la validez de los reclamos y contribuyendo a la detección de posibles fraudes.

En el entorno corporativo, la informática forense en palabras de Alcívar (2019) se convierte en una herramienta esencial para abordar una variedad de casos, desde acoso sexual hasta robo, mal uso o apropiación de información confidencial o propietaria. Además, la disciplina desempeña un papel fundamental en la investigación de casos relacionados con espionaje industrial y suplantación de marca, proporcionando a las empresas los medios necesarios para proteger sus activos y preservar la integridad de su información sensible.

Dispositivos y sistemas sujetos a investigación forense digital

La investigación forense digital se enfoca en analizar y examinar una amplia gama de dispositivos y sistemas para recolectar evidencia digital en el contexto de delitos informáticos. La aplicación de esta disciplina se extiende a dispositivos como computadoras, servidores, dispositivos móviles, redes y sistemas de almacenamiento. Al-Dhaqm et al. (2020) mencionan que la informática forense aborda el examen de sistemas y medios electrónicos para descubrir, analizar y preservar evidencia digital.

En el ámbito de las computadoras, la informática forense se aplica para investigar intrusiones, identificar malware y analizar el comportamiento de programas sospechosos. Autores como Nawal et al. (2020) señalan la importancia de la recolección de datos en sistemas operativos, registros de eventos y archivos de registro para comprender las actividades en una computadora en el momento de un incidente. Los dispositivos móviles, como teléfonos inteligentes y tabletas, también son objeto de investigación forense digital. Tully et al. (2020) destacan la necesidad de examinar la memoria, el sistema de archivos y las aplicaciones de estos dispositivos para recuperar datos relevantes en investigaciones criminales.

En el dominio de las conexiones y comunicaciones de red, la informática forense se centra en el análisis de tráfico, registros y configuraciones para identificar patrones de

comportamiento malicioso. Autores como Jaeyoung et al. (2020) resaltan la importancia de entender la topología de la red y la interacción entre dispositivos para reconstruir incidentes.

Los sistemas de almacenamiento, incluidos discos duros y unidades de almacenamiento externas son esenciales en investigaciones forenses. Autores como Abdul et al. (2022) subrayan la importancia de preservar la integridad de los datos durante la adquisición y el análisis de dispositivos de almacenamiento.

Entornos de almacenamiento susceptibles a la ocultación de información a través de técnicas esteganográficas digitales

La esteganografía digital, un arte ancestral de ocultar información en otros datos digitales, ha evolucionado significativamente y se ha vuelto una herramienta versátil para la ocultación de información. Diversos medios, como imágenes, archivos de audio, video o documentos digitales, sirven como sustrato para insertar datos encubiertos. Esta diversidad de medios proporciona a los usuarios una amplia gama de opciones para ocultar información, dificultando la detección y revelación de datos ocultos para terceros no autorizados (Vintimilla, 2023). En la actualidad, existen técnicas novedosas en la esteganografía digital que desafían incluso las capacidades de la informática forense. Según Muñoz (2020) la inserción de datos en el dominio de la frecuencia, la modificación de características específicas de archivos y el uso de algoritmos sofisticados son solo algunos ejemplos de las tácticas avanzadas empleadas. Estas técnicas avanzadas presentan un desafío adicional para los investigadores forenses, ya que requieren un conocimiento profundo y herramientas especializadas para su detección.

La diversificación de las técnicas esteganográficas y la constante evolución de nuevas estrategias para ocultar información hacen que la esteganografía digital sea un campo dinámico y desafiante. La investigación continua en este dominio es esencial para desarrollar contramedidas efectivas y fortalecer las capacidades de la informática forense en la detección

de datos ocultos (Sanchis, 2022). De manera general se han presentado diversos medios, los cuales se presentan en la Tabla 3.

Tabla 3
Síntesis de los medios de ocultación de información

Medios	Descripción
Imágenes digitales	La esteganografía es frecuentemente aplicada en archivos de imágenes, como JPEG, PNG o BMP. Los datos pueden ser ocultados en la estructura de píxeles de la imagen, aprovechando características visuales imperceptibles para el ojo humano.
Archivos de audio	Los archivos de audio, como MP3 o WAV, también son susceptibles de contener información oculta. Técnicas como la modificación de frecuencias o la manipulación de muestras de audio permiten la inserción de datos sin afectar significativamente la calidad perceptible del sonido.
Archivos de video	Al igual que en imágenes y audio, los archivos de video pueden utilizarse para ocultar información. La esteganografía puede aplicarse a diferentes niveles, desde la inserción de datos en fotogramas hasta la modificación de características temporales de la secuencia.
Documentos digitales	Archivos de texto y documentos digitales, como PDF o DOC, pueden ser utilizados para ocultar información mediante esteganografía. La manipulación sutil de espacios en blanco, caracteres especiales o formatos de texto puede ser empleada con este propósito.
Tráfico de red	La esteganografía también puede aplicarse en el tráfico de red, ocultando datos en paquetes de información. Este enfoque es común en entornos de comunicación digital, donde los datos pueden ser transferidos sin levantar sospechas.

Fuente: Elaborado con base en datos de estudios consultados.

Tecnologías y recursos de informática forense para el estegoanálisis

En el ámbito de la informática forense, se ha observado según Prakash et al. (2021) el surgimiento de diversas técnicas y herramientas especializadas destinadas a enfrentar los desafíos de la esteganografía digital. Estas técnicas tal como resalta Nawal et al. (2020) han evolucionado para adaptarse a las complejidades de las prácticas de ocultamiento de información en archivos digitales, ya sea mediante imágenes, audio, video o texto. Los profesionales de la informática forense ahora cuentan con enfoques más avanzados, como el estegoanálisis basado en redes neuronales, que utiliza algoritmos de aprendizaje profundo para detectar patrones sutiles y anomalías en los datos digitales, revelando así la presencia de información oculta.

Además, las herramientas de estegoanálisis han experimentado mejoras significativas en términos de precisión y eficacia. Herramientas como OutGuess, Stegdetect y ExifTool son empleadas para identificar y extraer datos ocultos de archivos digitales. Estas soluciones ofrecen una gama de funciones, desde la detección de patrones específicos de esteganografía

hasta la revelación de información encubierta en diversos formatos de archivo. La constante evolución de estas técnicas y herramientas refleja el compromiso continuo de la informática forense en mantenerse a la vanguardia para abordar los constantes desafíos planteados por la esteganografía digital en investigaciones criminales y procesos judiciales.

Tabla 4

Síntesis de los medios de ocultación

Grupo de técnica o Herramientas	Descripción
Herramientas de Estegoanálisis Convencional	▪ **Stegdetect:** Un programa diseñado para detectar archivos esteganográficos mediante el análisis de patrones y firmas específicas. ▪ **OutGuess:** Una herramienta que se utiliza para detectar y extraer información oculta en archivos digitales.
Herramientas de Análisis de Metadatos	▪ **ExifTool:** Permite examinar y modificar los metadatos de archivos digitales, revelando información oculta en imágenes, audio o video.
Herramientas Basadas en Redes Neuronales	▪ **Enfoques de Aprendizaje Profundo:** Se emplean algoritmos de redes neuronales convolucionales para realizar estegoanálisis, identificando patrones sutiles y anomalías en datos digitales.
Sistemas de detección de frecuencias	▪ **Análisis de Frecuencias en Señales:** Técnicas que evalúan las frecuencias presentes en archivos para descubrir posibles alteraciones introducidas por esteganografía.
Herramientas de Análisis de Texto	▪ **Esteganografía en Archivos de Texto:** Enfoques que se centran en la manipulación de espacios en blanco, caracteres especiales o formatos de texto para ocultar información en documentos de texto.
Esteganografía en Multimedia	▪ **Método de Sustitución de Bits (LSB):** Técnica que implica la ocultación de información al reemplazar los bits de menor significancia en archivos de imagen, audio o video.
Investigación Forense en Dispositivos Móviles	▪ **Extracción de Datos de Dispositivos Móviles:** Herramientas especializadas para la recuperación de información oculta en smartphones y tablets.

Fuente: Elaborado con base en datos de estudios consultados.

Evaluación de las herramientas de software y técnicas específicas utilizadas en informática forense

La informática forense juega un papel esencial en la identificación, análisis y recuperación de evidencia digital en investigaciones legales. La evaluación de las herramientas de software y técnicas utilizadas en este campo es un aspecto crítico para garantizar la eficacia de los procesos de investigación. Uno de los criterios fundamentales para evaluar estas herramientas es la precisión en la detección de datos ocultos, ya que cualquier falta o error en esta área podría comprometer la integridad de la evidencia. La capacidad de identificar de manera confiable información encubierta es crucial para el éxito de una investigación forense

digital. Durante el proceso investigativo, se recopiló la perspectiva de autores y especialistas con base a los cuales se construyó un cuadro resumen el cual se indica a continuación.

Otro de los aspectos evaluados fue la velocidad de procesamiento el cual es otro factor clave a considerar en la evaluación de herramientas de informática forense. La rapidez con la que una herramienta puede analizar grandes conjuntos de datos digitales puede marcar la diferencia en investigaciones que requieren respuestas rápidas. La eficiencia en este sentido no solo aumenta la productividad, sino que también puede ser crucial para abordar casos en tiempo real o con plazos ajustados. En la Tabla 4 se sintetiza la calificación otorgada a cada herramienta teniendo en cuenta el criterio de velocidad de procesamiento.

La facilidad de uso fue un tercer criterio importante, ya que una interfaz intuitiva y herramientas de fácil comprensión permiten a los investigadores forenses maximizar su eficacia sin perder tiempo en aprendizaje técnico innecesario. Además, la compatibilidad con formatos de archivos específicos es esencial, ya que los diferentes tipos de archivos digitales requieren enfoques particulares en términos de análisis y recuperación de datos. Una herramienta versátil en este aspecto puede adaptarse a diversas situaciones y formatos, facilitando la labor del profesional forense.

Por último, la capacidad de recuperación de datos es un criterio que destaca la importancia de asegurar que las herramientas de informática forense no solo detecten datos ocultos, sino que también permitan su recuperación sin comprometer su integridad. Esta característica es vital para la presentación de evidencia en procedimientos legales y la construcción de casos sólidos. En conjunto, la evaluación de herramientas y técnicas en informática forense bajo estos criterios proporciona una base sólida para el desarrollo de investigaciones digitales eficaces y éticas.

Tabla 5

Calificación de las herramientas de estegoanálisis según velocidad de procesamiento

Técnica o Herramienta	Descripción o Funcionalidad	Nivel de Precisión en la Detección de Datos Ocultos (1-5)	Velocidad de Procesamiento (1-5)	Facilidad de Uso (1-5)	Capacidad de Recuperación de Datos (1-5)	Razones de la calificación
Stegdetect	Herramienta de análisis de archivos en busca de patrones esteganográficos.	4	3	3	2	Su precisión es alta, pero puede generar falsos positivos en casos de esteganografía menos convencional. La velocidad depende del tamaño del archivo y la complejidad de los patrones. La interfaz de usuario podría ser más intuitiva, requiere ciertos conocimientos técnicos. Su capacidad de recuperación es limitada ya que se enfoca más en la detección.
ExifTool	Utilidad para leer y escribir metadatos en diversos tipos de archivos.	3	3	4	3	La precisión puede ser moderada, ya que la presencia de datos ocultos en los metadatos puede variar. La velocidad es moderada, ya que depende del tamaño del archivo y la cantidad de metadatos a analizar. Interfaz de línea de comandos puede ser menos amigable para usuarios no técnicos. La capacidad de recuperación depende de la presencia de información útil en los metadatos.
OutGuess	Herramienta de esteganografía que busca ocultar información en archivos de imágenes.	3	4	3	2	La precisión es moderada, y su detección depende de la complejidad de la esteganografía utilizada. La velocidad puede ser relativamente rápida, pero depende del tamaño de la imagen y la cantidad de datos a ocultar. La configuración y la comprensión de parámetros pueden ser complicadas para usuarios novatos. La capacidad de recuperación puede ser baja si se utiliza una esteganografía fuerte.
Foremost	Herramienta de recuperación de datos que puede identificar y extraer archivos ocultos.	4	4	4	4	La precisión es buena, pero puede verse afectada por la fragmentación y la complejidad del sistema de archivos. La velocidad es buena, especialmente en archivos comunes, pero puede variar según la complejidad de la recuperación. Interfaz intuitiva y sencilla, adecuada para usuarios con diferentes niveles de experiencia. Ofrece una capacidad razonable de recuperación de datos, especialmente en sistemas de archivos comunes.
StegExpose	Herramienta que revela información oculta en imágenes mediante análisis de patrones y entropía.	5	3	5	2	Su precisión es alta, ya que utiliza múltiples enfoques para la detección. La velocidad es moderada, ya que implica análisis detallado. Interfaz gráfica simple y fácil de entender, adecuada para usuarios no técnicos. Su capacidad de recuperación es limitada ya que se enfoca más en la detección que en la recuperación.

Autopsy	Plataforma forense digital que incluye herramientas para la extracción y análisis de datos ocultos.	3	3	4	5	La precisión varía según las herramientas específicas utilizadas dentro de Autopsy. La velocidad puede ser moderada debido a su amplio conjunto de funciones. Interfaz gráfica intuitiva, aunque puede ser compleja para usuarios sin experiencia en informática forense. Ofrece una buena capacidad de recuperación de datos, especialmente en casos de investigación forense digital.
Binwalk	Herramienta para analizar archivos embebidos y realizar análisis de entropía.	3	3	3	3	Analiza archivos embebidos y realiza análisis de entropía. La precisión puede ser buena, pero su eficacia depende de la complejidad de las técnicas de esteganografía. La velocidad puede ser variable según el tamaño y complejidad del archivo. Requiere conocimientos técnicos, la interfaz puede resultar abrumadora para principiantes. La capacidad de recuperación puede ser variable dependiendo de la complejidad de las técnicas de esteganografía.
Hashcat	Herramienta de recuperación de contraseñas que también puede utilizarse para verificar la integridad de archivos.	2	4	2	2	No está diseñada específicamente para la detección de datos ocultos, por lo que su precisión en este contexto es limitada. La velocidad es alta y eficiente en operaciones de hash, pero no está diseñada específicamente para la detección de datos ocultos. Interfaz de línea de comandos avanzada, puede ser difícil de manejar para usuarios no técnicos. No está diseñada específicamente para la recuperación de datos esteganográficos, por lo que su capacidad en este aspecto es limitada.

Fuente: Elaborado con base en datos bibliográficos y la opinión de especialistas.

En el análisis de los resultados obtenidos mediante diversas metodologías y herramientas aplicadas en el ámbito de la informática forense con el propósito de detectar datos ocultos, se destacan tendencias significativas. En la dimensión de facilidad de uso, se otorgan altas calificaciones a Foremost y Autopsy, con un promedio de 4, indicando su percepción como herramientas intuitivas y de fácil manejo. ExifTool también resalta con una calificación de 4 en este aspecto. Contrariamente, Hashcat registra la puntuación más baja en facilidad de uso, obteniendo un 2.

En el ámbito de la velocidad de procesamiento, Foremost y OutGuess sobresalen con calificaciones promedio de 4, indicando eficiencia en términos de rapidez. Hashcat también destaca con una calificación de 4 en este aspecto. En lo referente a la precisión en la detección

de datos ocultos, StegExpose lidera con una calificación perfecta de 5, seguido de cerca por Foremost y OutGuess con un promedio de 4. Autopsy y ExifTool reciben una calificación de 3 en este parámetro. En cuanto a la capacidad de recuperación de datos, Foremost y Autopsy se distinguen con una puntuación perfecta de 5, indicando una alta eficacia en la recuperación de datos ocultos. ExifTool también registra una calificación respetable de 3 en este aspecto.

En la síntesis de las puntuaciones promedio de las tres mejores herramientas en general, Foremost sobresale con un destacado promedio de 4, seguido de cerca por StegExpose y Autopsy, ambos con un promedio de 3.8. Este análisis sugiere que, en términos generales, estas tres herramientas exhiben la mayor eficacia conjunta para la detección y recuperación de datos ocultos en contextos de investigaciones forenses.

Tabla 6
Promedio de calificación de las técnicas o herramientas de estegoanálisis

Técnica o Herramienta	Facilidad de Uso (1-5)	Velocidad de Procesamiento (1-5)	Nivel de Precisión en la Detección de Datos Ocultos (1-5)	Capacidad de Recuperación de Datos (1-5)	Promedio
Stegdetect	3	3	4	2	3,0
ExifTool	4	3	3	3	3,3
OutGuess	3	4	3	2	3,0
Foremost	**4**	**4**	**4**	**4**	**4,0**
StegExpose	**5**	**3**	**5**	**2**	**3,8**
Autopsy	**4**	**3**	**3**	**5**	**3,8**
Binwalk	3	3	3	3	3,0
Hashcat	2	4	2	2	2,5

Fuente: Elaborado con base en la opinión de especialistas.

Perspectiva común de especialistas en estenografía digital y la actividad del forense informático.

Los investigadores forenses digitales y los especialistas en estenografía digital que fueron entrevistados coinciden en que existe una serie de desafíos a la hora de detectar y extraer datos ocultos mediante esteganografía. Los entrevistados destacan que las técnicas de esteganografía se han vuelto cada vez más sofisticadas, lo que dificulta su detección. Los atacantes utilizan técnicas avanzadas para ocultar los datos, como el uso de algoritmos de

compresión, cifrado o transformación. Los datos digitales pueden encontrarse en una amplia variedad de formatos, como imágenes, vídeos, archivos ejecutables o documentos. Cada formato tiene sus propias características únicas, lo que puede dificultar la detección de datos ocultos.

Teniendo en consideración las opiniones emitidas a los planteamientos de la entrevista aplicada a especialistas en informática forense, se tuvo que, el Especialista 1, destaca la creciente complejidad de la esteganografía digital como uno de los mayores desafíos en la informática forense. En sus palabras, "la utilización de algoritmos más avanzados y métodos sofisticados de ocultamiento presenta un reto constante para los investigadores". Coincidiendo con esto, el Especialista 2, menciona la importancia de la colaboración entre profesionales de la ciberseguridad y la informática forense para abordar estos desafíos en evolución. En cuanto a las herramientas, el Especialista 3 elogia Foremost por su capacidad para recuperar datos ocultos en archivos, destacando su versatilidad en situaciones donde se sospecha la presencia de esteganografía. Sin embargo, el Especialista 1 prefiere StegExpose, argumentando que "la capacidad de identificar la presencia de esteganografía de manera rápida y precisa es crucial en entornos forenses". Destaca la importancia de la eficiencia y la precisión en la detección.

La discusión sobre Autopsy revela opiniones diversas. El Especialista 3 valora su enfoque integral, mencionando que "la capacidad de realizar análisis forenses en múltiples plataformas y formatos facilita la investigación". En contraste, Especialista 1 sugiere que, aunque Autopsy es útil, su enfoque general podría no ser tan específico para casos de esteganografía. "Prefiero herramientas más especializadas", comenta. Como síntesis de las perspectivas de los expertos se tiene que estos concuerdan en que la esteganografía digital presenta desafíos continuos en la informática forense, con la evolución constante de técnicas y algoritmos. La colaboración interdisciplinaria y el conocimiento actualizado son esenciales. En cuanto a las herramientas, Foremost destaca por su versatilidad, StegExpose por su eficiencia

en la detección, y Autopsy por su enfoque integral, aunque algunos preferirían herramientas más especializadas según el caso. La elección entre estas herramientas dependerá de la naturaleza específica de la investigación y las preferencias del investigador forense.

Descripción técnica de las principales herramientas valoradas positivamente por los especialistas

Teniendo en consideración las valoraciones emitidas por los especialistas entrevistados y las expuestas en los estudios científicos evaluados en el proceso investigativo, se expone a continuación aspectos técnicos de las principales herramientas de estegoanálisis en apoyo a la informática forense.

Foremost es una herramienta de estegoanálisis y recuperación de datos forenses que se utiliza para extraer información oculta de archivos, especialmente en el contexto de investigaciones forenses. Se determinó que las características y funcionalidades clave de Foremost, son que esta se centra en la recuperación de datos ocultos en archivos, siendo particularmente eficiente en la identificación y extracción de información de archivos multimedia, como imágenes y videos. En lo que respecta a los formatos de archivo soportados, la herramienta es capaz de trabajar con una variedad de formatos de archivos, incluyendo imágenes (JPEG, GIF, PNG), videos (AVI, MOV), archivos comprimidos (ZIP, TAR), documentos (PDF, DOC), entre otros.

Foremost utiliza algoritmos específicos para analizar archivos en busca de patrones que sugieran la presencia de datos ocultos. Emplea técnicas avanzadas para identificar firmas digitales y estructuras de archivos que podrían indicar la existencia de información encubierta.

Una de las fortalezas principales de Foremost es su capacidad para recuperar datos incluso en situaciones donde la información ha sido eliminada o está parcialmente dañada. La herramienta puede reconstruir archivos a partir de fragmentos dispersos en el sistema de almacenamiento.

Interfaz de usuario de Foremost permite que pueda ser utilizada desde la línea de comandos, lo que proporciona flexibilidad en su integración en entornos forenses y la automatización de procesos. La interfaz es robusta y facilita a los investigadores configurar diversos parámetros según las necesidades específicas de la investigación.

La herramienta permite a los usuarios especificar criterios de filtrado para extraer solo los datos relevantes de interés. Además, tiene la capacidad de clasificar los archivos recuperados en categorías según su tipo, facilitando la organización y análisis de la información recuperada. Finalmente, este recurso ha sido objeto de desarrollo continuo y actualizaciones, lo que asegura que la herramienta esté equipada para abordar las últimas técnicas de esteganografía y cambios en los formatos de archivos.

Otras de las herramientas con mejor valoración fue StegExpose que se enfoca en la detección de esteganografía en imágenes y otros archivos multimedia. Su propósito principal es identificar si una imagen dada contiene información oculta. La herramienta utiliza técnicas de análisis de firma digital para examinar imágenes en busca de patrones característicos asociados con la presencia de datos ocultos. Esto implica la identificación de huellas digitales específicas dejadas por algoritmos de esteganografía. StegExpose realiza análisis de frecuencia y entropía en las imágenes para identificar anomalías que podrían indicar la presencia de datos ocultos. Este enfoque se basa en la idea de que la esteganografía puede alterar la distribución de datos en la imagen.

La herramienta evalúa diversas características estadísticas de las imágenes, como la varianza y la media, para determinar si hay discrepancias que sugieran la presencia de esteganografía. En relación con la Interfaz Gráfica de Usuario (GUI), este recurso con un interfaz que facilita su uso para investigadores y analistas forenses. Esto permite una interacción más intuitiva y amigable con la herramienta.

Como funcionalidad destacada, la herramienta genera informes detallados que proporcionan resultados específicos sobre la presencia o ausencia de esteganografía en una imagen determinada. Estos informes incluyen detalles sobre las características analizadas y las posibles implicaciones forenses. StegExpose permite a los usuarios personalizar parámetros y ajustes según las necesidades específicas de la investigación. Esto incluye la capacidad de establecer umbrales para alertas y personalizar el nivel de sensibilidad del análisis. La herramienta es de código abierto, lo que facilita su examen y contribución por parte de la comunidad. Además, su mantenimiento activo garantiza que esté actualizada y lista para abordar las últimas técnicas de esteganografía.

Finalmente, la tercera herramienta mejor valorada es Autopsy la cual es un recurso de análisis forense digital de código abierto que se utiliza para examinar discos duros y dispositivos de almacenamiento en busca de evidencia digital. Esta dispone de una interfaz gráfica de usuario intuitiva que facilita la navegación y el uso de la herramienta. Esta interfaz permite a los investigadores realizar análisis forenses de manera eficiente y sin la necesidad de comandos complicados. La herramienta es capaz de analizar discos duros, unidades flash, tarjetas de memoria y otros dispositivos de almacenamiento para buscar evidencia digital. Esto incluye la recuperación de archivos eliminados, la identificación de actividades sospechosas y la reconstrucción de eventos. Autopsy se destaca por su capacidad para recuperar datos eliminados y fragmentos de archivos, permitiendo a los investigadores reconstruir información importante incluso después de la eliminación.

Uno de los elementos fuertes de Autopsy es el análisis de imágenes y metadatos, incluye módulos de análisis de imágenes que permiten a los investigadores examinar imágenes en busca de información oculta. Además, Autopsy analiza metadatos para proporcionar detalles sobre la creación, modificación y ubicación de archivos. Autopsy incluye módulos específicos para el análisis de correos electrónicos, permitiendo a los investigadores examinar mensajes,

adjuntos y metadatos relacionados con la correspondencia digital. La herramienta ofrece funciones de filtrado y clasificación para ayudar a los investigadores a enfocarse en áreas específicas de interés. Esto facilita la gestión y visualización de grandes conjuntos de datos forenses.

Integración con herramientas externas es otro de los atributos más destacados de esta herramienta Autopsy puede integrarse con otras herramientas forenses y utilidades externas, lo que amplía su funcionalidad y capacidad de análisis. Esto permite a los investigadores aprovechar una gama más amplia de recursos en sus investigaciones. La herramienta proporciona la capacidad de generar informes forenses detallados que documentan los hallazgos y las acciones realizadas durante el análisis. Estos informes son valiosos para presentar evidencia en procesos legales. Autopsy es un proyecto de código abierto con un desarrollo activo y una comunidad de usuarios comprometida. Esto asegura que la herramienta se mantenga actualizada y sea mejorada con nuevas funcionalidades y capacidades.

Conclusiones

Los informáticos forenses a menudo enfrentan restricciones de tiempo y recursos al analizar datos digitales. Esto puede dificultar la detección de datos ocultos, especialmente si se utilizan técnicas de esteganografía sofisticadas A pesar de los desafíos, los investigadores forenses cuentan con una variedad de recursos y técnicas modernas que pueden ayudarles a detectar y extraer datos ocultos mediante esteganografía. Existe una amplia gama de software de detección de esteganografía disponible, el cual puede ser útil para identificar información oculta. Entre las técnicas destacadas se encuentra el Análisis de Frecuencia, que se basa en la identificación de patrones de bits poco comunes dentro del contenido del archivo. Por ejemplo, un investigador forense podría buscar patrones de bits repetidos o cambios bruscos en la frecuencia de bits. Las bases de datos de esteganografía pueden ayudar a los investigadores a identificar técnicas de esteganografía conocidas. Estas bases de datos contienen ejemplos de

datos ocultos generados utilizando diferentes técnicas de esteganografía. La detección de esteganografía es un proceso complejo que requiere una combinación de técnicas y recursos.

En cuanto a las herramientas con mejor valoración por parte de especialistas, Foremost se destaca como un recurso integral en el ámbito del estegoanálisis forense. Ofrece avanzadas capacidades de recuperación de datos ocultos en una variedad de formatos de archivos. Su flexibilidad, capacidad para reconstruir datos y su continua evolución lo posicionan como una elección sólida para profesionales de la informática forense.

Por otro lado, StegExpose resalta como una herramienta especializada en estegoanálisis, brindando a los investigadores y analistas forenses una solución eficaz para la detección de esteganografía en archivos multimedia. Su enfoque basado en análisis de firma digital y características estadísticas proporciona una capa adicional de seguridad en investigaciones forenses relacionadas con datos ocultos en imágenes.

Autopsy es una herramienta integral de análisis forense digital que proporciona a los investigadores una plataforma poderosa para examinar dispositivos de almacenamiento, recuperar datos, analizar imágenes y correos electrónicos, y generar informes forenses detallados. Su interfaz amigable y su integración con otras herramientas lo convierten en una elección popular en el campo de la informática.

Para optimizar la eficacia de las técnicas y herramientas contemporáneas de informática forense, es recomendable que los especialistas establezcan procedimientos de análisis sistemáticos y rigurosos. Este enfoque implica una exploración exhaustiva de las capacidades de las herramientas disponibles, utilizando una variedad de métodos y técnicas de análisis para obtener una comprensión integral de los datos digitales. Además, se requiere una atención meticulosa a la calidad y precisión de los resultados, llevando a cabo validaciones cruzadas y verificaciones exhaustivas para garantizar la fiabilidad de las conclusiones obtenidas.

La informática forense es un campo en constante evolución. Los informáticos forenses deben estar al tanto de las últimas tendencias en esteganografía para poder seguir siendo eficaces. La elección de la técnica o tecnología adecuada para detectar esteganografía digital depende de una variedad de factores, como el tipo de archivo que se está analizando, el nivel de sofisticación de la esteganografía utilizada y las limitaciones de recursos del investigador forense.

Referencias bibliográficas

Abdul, R., Ahmed, W., Alazab, M., Jalil, Z., & Kashif, K. (2022). A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions. *IEEE Acces, 10*(2022), 11065-11089. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9678340

Alcívar, C. (2019). Aplicación de la ciencia forense en los delitos informáticos en el Ecuador y su. *Revista Espacios, 39*(42), 1-15. https://www.revistaespacios.com/a18v39n42/a18v39n42p15.pdf

Al-Dhaqm, A., Razak, S., Adeyemi , R., Kebande, V., & Siddique, K. (2020). A Review of Mobile Forensic Investigation Process Models. *Digital Object Identifier, 8*(1), 1-42. Retrieved from https://ieeexplore.ieee.org/abstract/document/9160916

Arévalo, M., & Hernández, D. (2021). Análisis preliminar de la ciberseguridad asociada al sistema financiero en algunos países de Latinoamérica y la contribución de la informática forense. *Cuaderno de investigaciones semilleros, 2021*(14), 93-116.

De Rosal, M., Supriadi, R., Pulung, A., Guruh, S., ., & . (2023). Digital image steganography survey and investigation (goal, assessment, method, development, and dataset). *Signal Processing, 206*(1), 1-12. doi:https://doi.org/10.1016/j.sigpro.2022.108908

Jaeyoung, K., Park, H., & Park, J. (2020). CNN-based image steganalysis using additional. *Multimedia Tools and Applications, 79*(1), 1355–1372. doi:https://doi.org/10.1007/s11042-019-08251-3

Kävrestad, J. (2019). *Fundamentals of Digital Forensics* (Second ed.). Springer. https://sci-hub.se/https://link.springer.com/book/10.1007/978-3-030-38954-3

López, A., & Ramos, G. (2021). Acerca de los métodos teóricos y empíricos de investigación: significación para la investigación educativa. *Revista Conrado, 17*(3), 22-31.

Majeed, M., Sulaiman, R., Shukur, Z., Hasan, M., ., ., & . (2021). A Review on Text Steganography Techniques. *Mathematics Journal, 9*(21), 1-28. doi:https://doi.org/10.3390/math9212829

Moreno, J. (2023). *Estudio de la detección de ciberataques de estenografia para evitar ingreso de software malicioso y evitar pérdidas de información en la cámara de comercio de Barrancabermeja.* [Tesis de Grado, Universidad nacional abierta y a distancia], Repositotio institucional unad. https://repository.unad.edu.co/bitstream/handle/10596/54993/Jamorenoja.pdf?sequence=3&isAllowed=y

Mothi, D., Janicke, H., Wagner, I., ., ., & . (2020). A novel principle to validate digital forensic models. *Forensic Science International: Digital Investigation, 33*(1), 1-9. doi:https://doi.org/10.1016/j.fsidi.2020.200904

Muñoz, R. (2020). *Aplicación móvil para la protección de la privacidad de la información digital utilizando técnicas esteganográficas y de encriptación.* [Tesis de Grado, Universidad Autónoma de Bucaramanga], Repositorio institucional unab. https://repository.unab.edu.co/handle/20.500.12749/14330

Nawal, A., Majda, A., Afnan, A., Maram, A., & Asia, A. (2020). Digital Steganography in Computer Forensics. *International Journal of Computer Science and Information Security (IJCSIS), 18*(2), 54-61.

Prakash, V., Williams, A., Garg, L., Savaglio, C., & Bawa, S. (2021). Cloud and Edge Computing-Based Computer Forensics: Challenges and Open Problems. *Electronics, 10*(1229), 1-42. Retrieved from https://www.mdpi.com/2079-9292/10/11/1229

Reyes, I., Damián, E., Ciriaco, N. C., Corimayhua, O., & Urbina, M. (2022). Métodos científicos y su aplicación en la investigación pedagógica. *Revista Dilemas Contemporáneos, 9*(2), 1-19. doi:https://doi.org/10.46377/dilemas.v9i2.3106

Sanchis, C. (2022). *Esteganografía y ocultación de información aplicadas a bibliotecas.* [Tesis de Maestría, Universidad Cralos III de Madrid], Repositorio institucional uc3m. https://e-archivo.uc3m.es/handle/10016/36296

Tully, G., Cohen, N., Compton, D., Davie, G., Isbell, R., & Watson, T. (2020). Quality standards for digital forensics: Learning from experience in England & Wales. *Forensic Science International: Digital Investigation, 32*(1). Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S2666282519300374

Vintimilla, J. (2023). *Aplicación de la técnica de esteganografía para el mejoramiento de la integridad de la información en sistemas académicos basados en la web, caso práctico.* [Tesis de Maestría, Escuela Superior Politécnica de Chimborazo], Repositorio institucional espoch. http://dspace.espoch.edu.ec/bitstream/123456789/18312/1/20T1678.pdf