UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TITULO DEL TRABAJO DE TITULACIÓN

ANÁLISIS DE LA INTEGRIDAD DE IMÁGENES USANDO MÉTODOS ESTEGOANALÍTICOS Y ANÁLISIS DE NIVEL DE ERROR (ELA).

AUTOR

CARVAJAL SANTOS ANGIE GEOMAYRA

MODALIDAD DE TITULACIÓN

Examen de carácter Complexivo

Previo a la obtención del grado académico en
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

Ing. Haz López Lídice Victoria, MSI.

Santa Elena, Ecuador

Año 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
JOSE MIGUEL SANCHEZ AQUINO

Ing. José Sanchez A. Msc.
DIRECTOR DE LA CARRERA

Firmado electrónicamente por:
LIDICE VICTORIA HAZ LOPEZ

Ing. Lídice Victoria Haz López, Msi.
TUTOR

Firmado electrónicamente por:
DANIEL IVAN QUIRUMBAY YAGUAL

Lsi. Daniel Quirumbay Yagual, Msia.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
MARJORIE ALEXANDRA CORONEL SUAREZ

Ing. Marjorie Coronel S. Mgti.
DOCENTE GUÍA UIC

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por CARVAJAL SANTOS ANGIE GEOMAYRA, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 11 días del mes de diciembre del año 2023

TUTOR

Firmado electrónicamente por:
LIDICE VICTORIA HAZ LOPEZ

Ing. Haz López Lídice Victoria

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Carvajal Santos Angie Geomayra**

DECLARO QUE:

El trabajo de Titulación, Análisis de la integridad de imágenes usando métodos estegoanalíticos y análisis de nivel de error (ELA) previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 11 días del mes de diciembre del año 2023

EL AUTOR

Carvajal Santos Angie Geomayra

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado Análisis de la Integridad de Imágenes Usando Métodos Estegoanalíticos y Análisis de Nivel de Error (ELA), presentado por el estudiante, CARVAJAL SANTOS ANGIE GEOMAYRA fue enviado al Sistema Anti-plagio, presentando un porcentaje de similitud correspondiente al 6%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

TUTOR

Firmado electrónicamente por:
LIDICE VICTORIA HAZ LOPEZ

ING. HAZ LÓPEZ LÍDICE, MSI.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **CARVAJAL SANTOS ANGIE GEOMAYRA**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales del trabajo de titulación con fines de difusión pública, dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 11 días del mes de diciembre del año 2023

EL AUTOR

Carvajal Santos Angie Geomayra

AGRADECIMIENTO

Quisiera agradecer en particular a:

Dios, *porque ilumina mi mente y mi camino, porque me inspira con sabiduría, por sostenerme en momentos de duda, y por ser mi guía constante en este viaje académico.*

Mi Esposo Paul, e hijas Angie y Odalys, *por su amor incondicional, apoyo emocional, comprensión y sacrificio durante todo este tiempo.*

Mis padres, *por el apoyo incondicional.*

Mi Asesora de Tesis, *a la Ing. Lídice Haz, por su orientación académica y valiosos comentarios que fueron fundamentales para dar forma a este trabajo de investigación.*

Amigos y Compañeros*: Mayerly González, Melany Reyes, Armildo Salinas, Bryan Merejildo, Alexis Quimí y Marcelo Villacis quisiera expresar mi profunda gratitud que a pesar de las barreras de la distancia y cuando solo éramos rostros en una pantalla construimos lazos que trascendieron la virtualidad, y que al encontrarnos en personas se transformaron en gratos y hermosos momentos que atesoraré por siempre. Gracias por la calidez con la que me recibieron y por hacer que esos encuentros presenciales fueran tan especiales.*

Gracias a cada uno de Uds.

Angie Geomayra Carvajal Santos

.

DEDICATORIA

Le dedico a Dios, por permitirme terminar esta etapa en mi vida, por darme la oportunidad de empezar de nuevo. A mis padres por brindarme siempre apoyo incondicional. A mis hermanos por sus consejos y ayuda. A mi familia, a mi esposo e hijas que son mi fortaleza y mis motivos para seguir adelante y que me permitieron llegar al término de mi carrera profesional.

Angie Geomayra Carvajal Santos

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El trabajo se centra en el Análisis de la Integridad de Imágenes usando Métodos Estegoanalíticos y Técnicas de Nivel de Error (ELA) en el contexto de la informática forense. El objetivo principal es evaluar los algoritmos estegoanalíticos y de análisis de nivel de error mediante el uso de herramientas open source de informática forense para garantizar la integridad de los archivos de imágenes. Utilizando como metodología de mejores prácticas en el examen forense de tecnología digital, el proyecto se enfocará en las cinco fases de adquisición, preservación, análisis, documentación y presentación.

En los resultados se identificarán las posibles manipulaciones en las imágenes analizadas, respaldada por evidencia forense sólida, metadatos y análisis ELA. El análisis de integridad de imágenes combina métodos estegoanalíticos y ELA para evaluar la autenticidad de las imágenes en investigaciones forenses. Este enfoque proporciona resultados y documentación precisa, lo que lo convierte en una herramienta valiosa para la detección de manipulaciones en imágenes digitales en contextos legales y forenses.

Palabras claves: Integridad de imágenes, Estegoanálisis, Informática forense.

ABSTRACT

The paper focuses on Image Integrity Analysis using Stegoanalytic Methods and Error Level Analysis (ELA) Techniques in the context of computer forensics. The main objective is to evaluate stegoanalytic and error level analysis algorithms using open source computer forensics tools to ensure the integrity of image files. Using best practice methodology in digital technology forensic examination, the project will focus on the five phases of acquisition, preservation, analysis, documentation and presentation.

The results will identify possible manipulations in the analyzed images, supported by solid forensic evidence, metadata and ELA analysis. Image integrity analysis combines steganalytical and ELA methods to assess the authenticity of images in forensic investigations. This approach provides results and accurate documentation, making it a valuable tool for digital image tampering detection in legal and forensic contexts.

Keywords: Image integrity, Stegoanalysis, Computer Forensics.

INTRODUCCIÓN

La integridad de las imágenes digitales es esencial en un mundo donde la manipulación y la falsificación de imágenes se han vuelto generalizadas. En este contexto, el "Análisis de la Integridad de Imágenes usando Métodos Estegoanalíticos y Técnicas de Nivel de Error (ELA)" emerge como un campo crítico de la informática forense. Este enfoque se orienta en la evaluación de la autenticidad de las imágenes digitales, desempeñando un papel fundamental en investigaciones legales, ciberseguridad y muchas otras disciplinas.

Las imágenes digitales tienen algunas características que les permiten ser el medio anfitrión más utilizado, cuando se trata de ocultamiento de la información, en donde el propósito es incrustar información de forma casi arbitraria sin afectar visualmente la imagen. Dos son los procesos requeridos para incrustar datos en las imágenes, un mecanismo de incrustación y uno de extracción o detección.

El propósito principal de este proyecto es utilizar algoritmos estegoanalíticos y técnicas de ELA para detectar manipulaciones o alteraciones en imágenes digitales. Siguiendo la metodología basada en las mejores prácticas del examen forense de tecnología digital, se garantiza una evaluación específica en las fases de adquisición, preservación, análisis, documentación y presentación de evidencia.

Este proyecto indica la combinación de estas metodologías y herramientas open source de informática forense puede ser una valiosa contribución para garantizar la integridad de las imágenes en un mundo cada vez más digital y susceptible a la manipulación de datos visuales.

CAPÍTULO 1. FUNDAMENTACIÓN

1.1. Antecedentes

A medida que la tecnología en dispositivos digitales, las TIC's y la conexión a internet avanzan, se requiere más capacidad de procesamiento de información y almacenamiento de datos. Los smartphone, tabletas y computadoras poseen gran cantidad de archivos de todo tipo ya sean de audio, video, imágenes etc.; haciendo de los dispositivos una mina de información potencial que pueden caer en personas que operan fraudulentamente en crímenes cibernéticos, los cuales acceden a información importante de los usuarios cometiendo ilícitos digitales como fraudes, clonación de identidad, divulgación de información privada y un sinnúmero de posibles ciberdelitos [1].

El campo de la informática forense se inició a fines de los años 70, poco después de que los pc se convirtieran en una opción viable para los consumidores. En 1978, el estado de Florida reconoce los crímenes de sistemas informáticos en el Computer Crimes Act, en casos de sabotaje, copyright, modificación de datos y ataques similares. Nace Copy2pc de Central Point Software en 1981, que se usaba para la copia exacta de disquetes, que generalmente estaban protegidos para evitar copias piratas, posteriormente es integrado en las Pc Tools. En 1982 Peter Norton publica UnErase: Norton Utilities 1.0, la primera versión del conjunto de herramientas Norton Utilities, entre las que destacan UnErase, una aplicación que permite recuperar archivos borrados accidentalmente [2].

En 1984 el FBI forma el Magnetic Media Program, que más tarde, en 1991, será el Computer Analysis and Response Team (CART). En 1987 nace la compañía AccessData, pionera en el desarrollo de productos orientados a la recuperación de contraseñas y el análisis forense con herramientas como la actual Forensic Toolkit (FTK). En 1988 se crea la International Association of Computer Investigative Specialists (IACIS), que certificará a profesionales de agencias gubernamentales en el Certified Forensic Computer Examiner (CFCE), una de las certificaciones más prestigiosas en el ámbito forense. En agosto de 2001 nace la Digital Forensic

Research Workshop (DFRWS), un nuevo grupo de debate y discusión internacional para compartir información [2].

Los delincuentes pueden utilizar técnicas avanzadas de ocultamiento, como la esteganografía, para ocultar información dentro de las imágenes sin dejar rastros evidentes. Esto dificulta la detección de contenido oculto y puede llevar a la pérdida de información crucial en una investigación. Las imágenes digitales pueden ser fácilmente manipuladas o alteradas utilizando software de edición, lo que plantea un desafío para determinar si una imagen ha sido modificada y en qué medida. Esto puede comprometer la autenticidad y confiabilidad de la evidencia visual. Los metadatos de una imagen, como la fecha, hora, ubicación y configuración de la cámara, son importantes para establecer la autenticidad y el contexto de una imagen.

Sin embargo, los metadatos pueden perderse o ser manipulados, lo que afecta la integridad y confiabilidad de la evidencia. Las imágenes pueden sufrir pérdida de calidad o alteraciones durante los procesos de compresión o conversión de formatos. Esto puede afectar la precisión de los detalles y hacer que la imagen no sea una representación fiel de la escena original.

Para el desarrollo del presente proyecto se toma como referencia el análisis realizado por trabajos anteriores asociados al tema de investigación.

La tesis "Esteganografía em vídeos comprimidos mpeg-4. (São Carlos-Brasil)", presenta una técnica para la esteganografía en videos comprimidos, denominada MP4Stego, que explora las estructuras y tecnología de video estándar MPEG-4 con el fin de proceder con la recuperación de información sin pérdida y presentar una mayor capacidad de inserción de datos ocultos. La esteganografía en videos digitales permite ocultar un gran volumen de información en comparación con las técnicas de imagen. Sin embargo, esta tarea no es trivial cuando se aplica a videos comprimidos, ya que la inserción de información oculta puede agregar ruido, lo que dificulta su recuperación durante la decodificación [3].

Por otro lado, la tesis "Aplicación móvil para la protección de la privacidad de la información digital utilizando técnicas estenográficas y de encriptación.

(Bucaramanga-Colombia)", muestra el proceso de construcción de una solución que tiene como objeto, guardar información sensible para la protección de un medio digital mediante técnicas esteganográficas y criptográficas ya que el uso de la estenografía proporciona los medios para ocultar información en formatos de imagen, en que el destinatario empleará un método para aislar la información útil del archivo capturado ya que esta únicamente puede ser recuperada por el receptor, agregándole un nivel de protección en la confidencialidad de la información [4].

Y la tesis "Aplicación de la técnica de esteganografía para el mejoramiento de la integridad de la información en sistemas académicos basados en la web, caso práctico https://sisepec.espoch.edu.ec, 2021. (Chimborazo-Ecuador)", Su objetivo fue mejorar la integridad de los sistemas académicos basados en la web, mediante la aplicación de la esteganografía, como una medida de seguridad para cualquier sitio web, sin importar los servicios que brinde o la información que sea publicada. Utilizaron la esteganografía como un método para mitigar la vulnerabilidad de clonación de sitios web, en la cual se esconde el código que valida el dominio del sitio, desencadenando varios métodos de autenticación y anunciando al usuario que se encuentra navegando por un sitio web verídico [5]

En conclusión y congruente a las consultas realizadas ya antes mencionadas, dichos trabajos se centran en la esteganografía como un medio para proteger nuestros datos ya que hoy día, la esteganografía correctamente aplicada puede proteger nuestra información de una manera segura ya que muchos autores coinciden en que la esteganografía bien usada resulta prácticamente imposible de descubrir. Esta necesidad tiene una mayor relevancia en la protección de las comunicaciones digitales, donde la investigación y desarrollo de nuevas técnicas ha avanzado notoriamente en las últimas décadas para evitar, o minimizar, ataques de revelación, supresión o alteración de la información.

1.2. Descripción del Proyecto

En este proyecto se detallan las técnicas antiforense de esteganografía y los métodos de análisis forense ELA (análisis de nivel de error) y estegoanálisis para evaluar la manipulación digital de los archivos de imágenes, y determinar la

integridad de los mismos. Los resultados serán presentados mediante un informe que describirán el procedimiento de las pruebas realizadas, y el rendimiento de los algoritmos estegoanalíticos, y de análisis de nivel de error (ELA).

Este proyecto "**Análisis de la integridad de imágenes usando métodos estegoanalíticos y análisis de nivel de error (ELA)",** según Resolución RF-FST-SO-09 No. 03-2021, contribuye con la Sub-línea de investigación de TSI adaptables e inteligentes, al utilizar técnicas de inteligencia computacional para desarrollar sistemas de análisis de imágenes más avanzados y capaces de tomar decisiones inteligentes.

A continuación, se describen las herramientas de hardware y software que son utilizadas para el desarrollo de este proyecto:

Hardware

Para realizar las pruebas de integridad de las imágenes en virtual box se crearán las máquinas virtuales con un mínimo 2GB de memoria RAM y un disco duro de 20GB. También se utilizará una maquina portátil con un procesador Intel(R) Core (TM) i5-10210U CPU, con 16,0Gb de memoria RAM. Los formatos de las imágenes a utilizar para este proyecto serán JPG (o JPGE) y PNG, ya que son los más utilizados para la distribución de imágenes por su compatibilidad con la mayoría de los dispositivos y plataformas.

Software

Los sistemas operativos que se instalarán para este proyecto serán Caine OS, Kali Linux y Windows O.S., y herramientas open como Autopsy, AccessData FTK Imager, QFileHasher, Nomesoft USB Guard, OS Forensics, Exiftool GUI, Fotoforensics, EnCase Forensic, FOCA.

Para el desarrollo del proyecto se emplea la metodología del análisis forense [6] que consta de cinco fases las cuales nos enfocaremos en las cuatro primeras fases descritas a continuación:

Fase de Adquisición.

- ✓ Se obtendrán imágenes con formatos JPG (o JPGE) y PNG desde los dispositivos de almacenamientos como pen drive, memoria Ram y disco duro externo.
- ✓ Se utilizarán herramientas y técnicas forenses especializadas para adquirir la evidencia sin alterarla.

Fase de Preservación.

- ✓ Se realizarán copias exactas y completas de imágenes forenses, es decir, copias bit a bit a los dispositivos de almacenamiento para preservar la evidencia original y garantizar la no perdida de las evidencias.
- ✓ Se generará el hash a la imagen forense a analizar antes de ser manipulada y evitar que la información sea alterada, dañada o manipulada ya sea por causas humanas o naturales.

Fase de Análisis.

- ✓ Se preparan las herramientas y técnicas para examinar y analizar la evidencia digital recolectada.
- ✓ Se aplican las técnicas estegoanalíticas y de análisis de nivel de error (ELA)
- ✓ Se analiza los metadatos de la información recogida y si una imagen ha sido alterada o modificada.

Fase de Documentación.

- ✓ Se documentará de manera técnica todo el procedimiento forense realizado en cada fase donde la estructura tendrá cuatro secciones de introducción, análisis, resultados y conclusiones describiendo así el procedimiento de las pruebas realizadas.

1.3. Objetivos del Proyecto

1.3.1. Objetivos Generales

Implementar los algoritmos estegoanalíticos y de análisis de nivel de error

mediante el uso de herramientas open source de informática forense que permitan garantizar la integridad de los archivos de imágenes.

1.3.2. Objetivos específicos

- Diseñar pruebas experimentales mediante escenarios controlados con imágenes modificadas como evidencia digital.
- Aplicar métodos estegoanalíticos y de análisis de nivel de error para determinar la integridad de un archivo de imagen.
- Generar un reporte de los resultados obtenidos describiendo los procedimientos realizados.

1.4. Justificación del Proyecto

Increíblemente los delincuentes hoy están utilizando la tecnología para facilitar el cometimiento de infracciones y eludir a las autoridades. Este hecho ha creado la necesidad de que tanto la Policía Judicial, la Fiscalía General del Estado y la Función Judicial deba especializarse y capacitarse en estas nuevas áreas en donde las TICs se convierten en herramientas necesarias en auxilio de la Justicia y la persecución de delito y el delincuente [7]. El creciente y abrumante avance de la tecnología de redes y dispositivos digitales interconectados como smartphones hacen que la evidencia o rastro digital juegue un papel importante en los procesos legales en la última década [1]. La integridad de las imágenes en la computación forense es fundamental para garantizar la fiabilidad y la validez de la evidencia digital.

Al mantener la integridad de las imágenes, se obtienen varios beneficios como la autenticidad de la evidencia, ya que la integridad de las imágenes asegura que no se hayan realizado modificaciones no autorizadas en los datos visuales. Esto es esencial para demostrar que la evidencia digital presentada es auténtica y no ha sido manipulada con fines fraudulentos o engañosos. Otro beneficio se encuentra en la Preservación de la cadena de custodia ya que en la cadena de custodia está registro documentado de todas las personas que han tenido acceso a la evidencia y de las

acciones realizadas sobre ella. Al garantizar la integridad de las imágenes, se conserva la integridad de la cadena de custodia, lo que fortalece la validez legal de la evidencia y evita la pérdida o alteración accidental de datos.

Con la Fiabilidad en los procedimientos judiciales, las imágenes forenses juegan un papel crucial en los procedimientos judiciales. La integridad de estas imágenes proporciona una base sólida para la toma de decisiones judiciales, ya que se puede confiar en que la evidencia visual es exacta y no ha sido manipulada de manera fraudulenta. Asimismo, la Confianza en los resultados de la investigación, al mantener la integridad de las imágenes, se genera confianza en los resultados de la investigación forense. Los informes y conclusiones basados en evidencia visual confiable y no manipulada tienen un mayor grado de credibilidad y pueden influir en el curso de una investigación o un proceso legal.

Cabe mencionar que otros de los beneficios está la Protección de los derechos del acusado, la integridad de las imágenes es esencial para garantizar que los derechos del acusado sean respetados. Al contar con evidencia digital íntegra y confiable, se evitan falsas acusaciones y se brinda una defensa adecuada a la persona implicada en el proceso judicial. En resumen, la integridad de las imágenes en la computación forense proporciona beneficios claves, como la autenticidad de la evidencia, la preservación de la cadena de custodia, la fiabilidad en los procedimientos judiciales, la confianza en los resultados de la investigación y la protección de los derechos del acusado.

Cabe recalcar que la presente investigación a desarrollar es de tipo experimental y documental, mediante la recolección de información de diferentes fuentes bibliográficas y aprendizaje durante la realización de esta, serán necesarias para poder sustentar la información sustraída mediante el análisis digital.

Este proyecto "**Análisis de la integridad de imágenes usando métodos estegoanalíticos y análisis de nivel de error (ELA)",** se alinea al Plan de creación de oportunidades, según el eje del objetivo social: **Objetivo 7**. Potenciar las capacidades de la ciudadanía y promover una educación innovadora, inclusiva y de calidad en todos los niveles [8].

1.5. Alcance del Proyecto

En este proyecto se evaluará la manipulación digital de los archivos de imágenes y determinar la integridad de los mismos, utilizando como metodología de mejores prácticas en el examen forense de tecnología digital la cual se desarrollarán las cuatro primeras fases de adquisición, preservación, análisis y documentación.

Se utilizarán dos formatos de imágenes JPG (o JPGE) y PNG, los cuales son los más utilizados para la distribución de imágenes por su compatibilidad con la mayoría de los dispositivos y plataformas.

En la fase de adquisición, se obtendrán imágenes con formatos JPG (o JPGE) y PNG desde los dispositivos de almacenamientos como pen drive, memoria Ram y disco duro externo para determinar su integridad. Se utilizarán las herramientas y técnicas forenses especializadas para adquirir la evidencia sin alterarla.

En la fase de preservación de la evidencia digital, se resguardará la evidencia para evitar cualquier alteración o modificación no autorizada y garantizar la no perdida de las imágenes. En esta fase, se aplicarán técnicas y procedimientos específicos para avalar la integridad de las imágenes. Se crearán copias exactas y completas de imágenes forenses, es decir, se hará una copia bit a bit a los dispositivos de almacenamiento que contienen las imágenes que se emplearan para este proyecto para autenticar la integridad de las imágenes y así evitar cualquier manipulación o cambio sin autorización, también se realizará el hash a la imagen forense a analizar antes de ser manipulada.

Y en la fase de análisis de la evidencia digital**,** se preparan las herramientas y técnicas para examinar y analizar la evidencia digital recolectada. Se analiza los metadatos de la información recogida y si una imagen ha sido alterada o modificada. Además, se comparará la imagen original con la imagen editada. Se aplicarán las técnicas estegoanalíticas y de análisis de nivel de error (ELA).

Y como última fase a realizar será la de documentación, los resultados serán presentados mediante una documentación técnica con todo el procedimiento forense realizado en cada fase donde la estructura tendrá cuatro secciones de

introducción, análisis, resultados y conclusiones describiendo así el procedimiento de las pruebas realizadas.

CAPÍTULO 2. MARCO TEÓRICO Y METODOLOGÍA DEL PROYECTO

2.1. Marco Teórico.

2.1.1. Validación de integridad de imágenes.

Validar la integridad de una imagen se refiere al proceso de verificar que una imagen no haya sido modificada, alterada o corrompida de alguna forma. El hash nos permite saber que una copia de información digital es igual a la original [9]. Una función hash es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija [10].

Existen algunos métodos comunes para validar la integridad de las imágenes como el caso del método Checksums o Sumas de verificación (Hashing) que genera un valor único (hash), con el fin de proteger la integridad de la información por medio de estos algoritmos de verificación se puede asegurar que no existan diferencias entre los valores que se obtienen al principio y al final de una transmisión de datos [11].

Los algoritmos comunes incluyen MD5, SHA-1 y SHA-256, el rendimiento de estos algoritmos depende de varios factores, entre ellos el tamaño de los datos de entrada, el algoritmo que utilizamos y la capacidad de procesamiento que tenga el hardware empleado, cuanto más complejos sean los algoritmos hash, mayor impacto tendrán en el rendimiento [12].

2.1.2. Incidencia de los algoritmos estegoanalíticos en la integridad de las imágenes.

En las dos últimas décadas se han propuesto diferentes metodologías para la codificación y compresión de imágenes como el codificador de imágenes DCT (Transformado discreta del coseno), la transformada DWT (transformada wavelet discreta) y la transformada finita ridgelet [13]. Muchos artículos discuten cómo utilizar la inteligencia artificial en el estegoanálisis en medios digitales, pero la mayoría de ellos no son reproducibles ni tangibles debido a la información que

contienen, los artículos normalmente no son suficientes, ya que ninguna herramienta de software puede llegar hacerlo [14].

2.1.3. Aplicación de las técnicas de análisis de nivel de error en la integridad de imágenes.

Al aplicar estas técnicas, es importante mencionar que se requiere software especial, capacitaciones, conocimiento y experiencia para detectar errores de compresión, inconsistencia de zonas, patrones repetitivos, metadatos originales o alterados, ruido o interferencias en una imagen. otras características indicativas que permitan identificar la autenticidad de la imagen.

El análisis de nivel de error de la imagen se basa en mostrar el nivel de compresión de cada pixel, aplicando distintos colores a las áreas con mayor error. Esto brinda como resultado que la imagen pueda tener variaciones entre blanco, negro, azul y rojo. Una imagen sin comprimir o editar mostrará un ELA uniforme de muy baja intensidad (negro), pero los ajustes o fotomontajes muestran inconsistencias entre elementos de la imagen, haciendo que el ELA sea más intenso (blanco).

Es importante mencionar que la imagen JPEG original (nativa) tiene errores ELA altos, por lo que tiende a mostrar más tonos blancos, mientras que cada vez que se guarda la imagen reduce el posible nivel de error y da un resultado ELA. más oscuro El análisis de nivel de error (ELA) proporciona pistas, pero no confirma ni concluye que la imagen digital haya sido alterada [15].

2.2. Marco Conceptual

2.2.1. Introducción a la informática forense

La Informática Forense, según fue definida en el primer DFRWS (Taller de Investigación Digital Forense) celebrado por un grupo de expertos en el año 2001, consiste en el empleo de métodos científicos comprobables para preservar, recolectar, validar, identificar, analizar, interpretar, documentar y presentar evidencias digitales procedentes de fuentes digitales con el propósito de hacer posible la reconstrucción de hechos considerados delictivos o ayudar a la prevención de actos no autorizados y capaces de provocar una alteración en operaciones planificadas de organismos y empresas [16].

La Ciencia Forense juega un papel fundamental en las investigaciones criminales. Debe entenderse como una aproximación multidisciplinar que permite juntar todo tipo de evidencias en una investigación. Normalmente, durante el transcurso de una investigación, deberán aplicarse los principios y metodologías de diferentes disciplinas científicas para la presentación de evidencias ante un tribunal [17].

2.2.2. Principio de Transferencia de Edmon Locard

En la comunidad científica se ha pensado que la aplicación del Principio de Transferencia de Edmon Locard, como principio universal de las ciencias forenses, da sentido a la investigación científica criminal, ya que el trabajo criminal de un delincuente exige su presencia física y por lo tanto deja rastro; otra cosa es su aplicación en la disciplina forense digital, pues su campo de acción en la escena de un cibercrimen imprime retos a la investigación científica porque el trabajo criminal es digital, no existe presencia física del sujeto sino transmisiones de datos, emisiones electromagnéticas, impulsos eléctricos, entre otros [18].

Este principio es reinterpretado, a fin de ser aplicado en el campo de la computación forense, toda vez que su formulación objetiva y estática aparentemente parece no ser posible, sin embargo, los expertos de la computación forense han determinado que la aplicación del principio sí se presenta, teniendo en cuenta que existe una evidencia la cual fundamenta la escena del crimen, la cual involucra una víctima y un sospechoso, donde la escena del crimen presenta las alertas de los equipos monitoreados, frente a la víctima se evidencia en la traza de ficheros, es decir, se requiere el análisis de toda la actividad y eventos que ocurren en nuestro equipo y se encuentran almacenando, finalmente, de ambos sujetos y como fundamento de la evidencia digital, los ficheros o archivos, son obtenidos y validados bajo el mismo valor hash [19].

Figura 1 *Diagrama Principio de Locard en el contexto de la Computación Forense.*

2.2.3. Criptografía

La criptografía es una rama de las matemáticas que hace uso de métodos y técnicas cuyo objetivo principal es cifrar y proteger un mensaje o archivo oculto por medio de un algoritmo, usando una o más claves, sin ellas será realmente difícil obtener el archivo original [20].

2.2.4. Esteganografía

El término esteganografía proviene de la palabra "steganos" que en griego significa oculto, y "grafía" que significa escrito, por lo que el concepto de "escritura oculta o encubierta" [21]. La esteganografía es una técnica diseñada para poder esconder información, datos e incluso archivos dentro de un medio portador. A diferencia de la criptografía, donde el objetivo es cifrar la información de modo que si es interceptado su contenido no sea legible ni entendible, en la esteganografía, la idea es poder enviar mensajes, datos ocultos sin que genere sospechas para evitar que sea interceptado, con el fin de coordinar acciones y compartir datos secretos.

En el libro "las Historias", escrito por Heródoto de Halicarnaso unos 400 años antes de Cristo, se mencionan ejemplos muy interesantes sobre el uso de la esteganografía para el envío de mensajes secretos militares. En la Figura 2, se representa un caso donde el general Histieo [22] del ejército de Atenas, mandó a rasurar el cabello de uno de sus criados, y le tatuó un mensaje para coordinar una invasión a Persia.

Luego esperó a que le creciera el cabello y lo envió donde Aristágoras de Mileto, quien le envió a rasurar de nuevo la cabellera con el fin de ver el mensaje oculto.

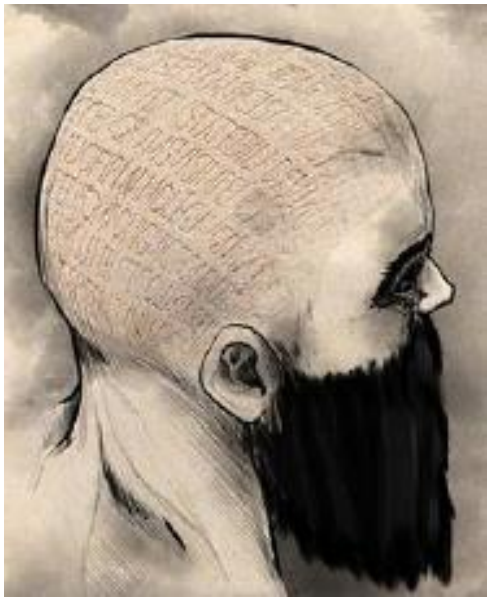

Figura 2 *Mensaje oculto enviado a modo de tatuaje.*

En la **Figura 3** Proceso de la Esteganografía se muestra el proceso de la esteganografía, se realiza el preprocesamiento a la imagen para eliminar el posible ruido que contenga, luego se incrusta el mensaje, después de eso se valida que la incrustación del mensaje se halla realizado correctamente para finalmente extraer el mensaje que se ha incrustado de forma oculta [23].

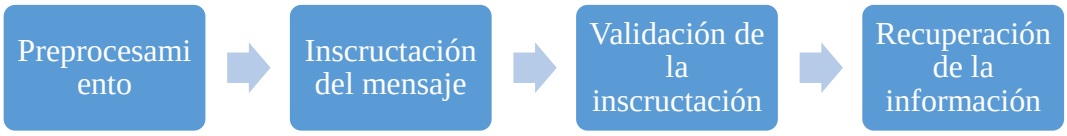

Figura 3 *Proceso de la Esteganografía*

2.2.5. Estegoanálisis

Es la técnica que permite detectar información oculta en archivos digitales sea cual sea la técnica de ocultación aplicada [24]. La ocultación de mensajes usando procedimientos esteganográficos puede tener fines legítimos o ilegítimos, que pueden ser beneficiosos para proteger la privacidad de las comunicaciones o burlar censuras, o, por el contrario, ser vehículos para perpetrar actos criminales es por

eso que el estegoanálisis es la ciencia y el arte que permite detectar esta información oculta [25].

2.2.6. Modelo de esteganografía de imágenes

En la esteganografía de imágenes se utilizan dos conceptos principales:

Proceso de incrustación: En el proceso de incrustación, el mensaje secreto se oculta en la imagen con la ayuda de la clave-Stego, de modo que nadie puede extraer la información sin conocer la clave-Stego y como resultado, se obtiene una imagen Stego que está lista para pasar al siguiente proceso [26].

Proceso de extracción. Como se muestra en la **Figura 4** Proceso de la esteganografía, en el proceso de extracción, una imagen-Stego con la clave-Stego se somete al proceso de extracción para obtener la información secreta y como la clave-Stego se utiliza en el proceso de incrustación, también se utiliza en el proceso de extracción [26].

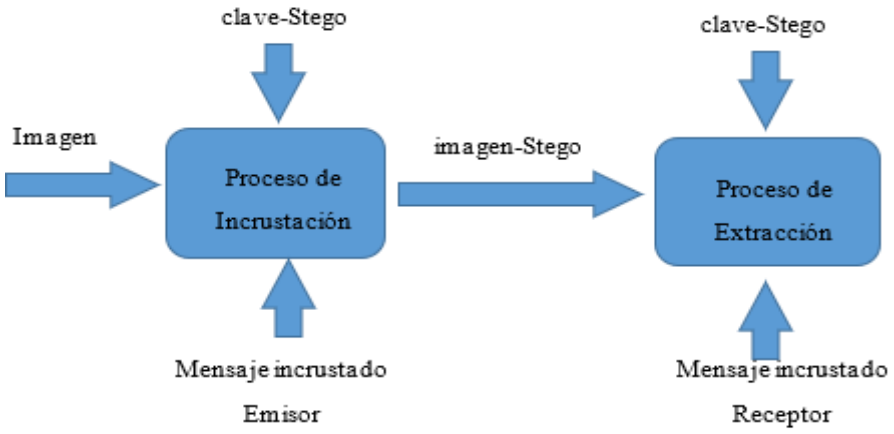

Figura 4 *Proceso de la esteganografía*

La clave se comparte entre el emisor y el receptor. La codificación se completa en el lado del emisor para obtener la imagen-Stego, mientras que la decodificación se lleva a cabo en el lado del receptor para obtener la información secreta [26].

2.2.7. Análisis de nivel de error (ELA, por sus siglas en inglés Error Level Analysis)

ELA se aplica exclusivamente a imágenes JPEG ya que se fundamenta en la naturaleza de su proceso de compresión ya que el algoritmo de compresión JPEG organiza la imagen en bloques de 8x8 pixels que una vez sometidos a diversos ciclos de compresión generan lo que se conoce como el "error level" [27].

En el proceso ELA, la imagen original que se está examinando se volverá a guardar con un determinado nivel de calidad jpeg, al volver a guardar se produce un grado de compresión conocido que se extiende a toda la imagen, esta imagen recién guardada se utiliza para compararla con la imagen original y el ojo humano apenas notaría un cambio, por lo tanto, la representación ELA visualizará en particular sólo la diferencia entre las dos imágenes, entonces, la imagen ELA resultante muestra los distintos grados de potenciales de compresión [28].

Mas allá del método de detección de imágenes jpeg manipuladas se encuentra la idea de que si una imagen ha sido manipulada, entonces cada cuadrado de 8x8 que se ve afectado por el cambio tiene un potencial de nivel de error más alto que el resto de la imagen.

2.2.8. Tipos de compresión de imágenes

2.2.8.1.Compresión sin pérdida

Esta técnica condensa las cadenas de código sin despreciar nada de la información que forma la imagen, por lo que ésta se regenera intacta al ser descomprimida, sin embargo, es menor la capacidad de compresión que provee este tipo de técnicas; dado que su fin es permitir una impresión de calidad, además de una exacta visualización de la imagen [29].

2.2.8.2.Compresión con pérdida

La compresión con pérdida hace que los algoritmos usados, para reducir las cadenas del código, desechen información redundante de la imagen así, los archivos comprimidos con este método pierden parte de los datos de la imagen, algunos

formatos, como el jpg, compensan esta pérdida con técnicas que suavizan los bordes y áreas que tienen un color similar, haciendo que la falta de información sea invisible a simple vista; este método permite un alto grado de compresión con pérdidas en la imagen que, muchas veces, sólo es visible si se realiza un fuerte acercamiento y es así que el grupo JPEG (Joint Photographic Experts Group) incluye este método de compresión en los archivos jpg y éste es, por mucho, el formato más difundido en el diseño para Internet. También otros archivos, como los pdf y los archivos basados en el lenguaje PostScrip (eps y ps), emplean este método de compresión [29].

2.2.9. Formato de archivos de imágenes

Están estandarizados para organizar y almacenar imágenes digitales. Un formato de archivo de imagen puede almacenar datos en un formato sin comprimir, en un formato comprimido (con pérdida o sin pérdida) o en formato de vector. Los archivos de imagen están compuestos de datos digitales en uno de estos formatos, de tal manera que los datos puedan ser escalados para su uso en la pantalla de la computadora/monitor de imagen o de la pantalla de la impresora [30].

2.2.9.1.Formato de imagen JPEG o JPG

El formato jpge o jpg nació como una respuesta a las limitaciones de otros formatos entre ellos el GIF en cuanto a calidad y tamaño de archivos, utiliza una compresión de imágenes con pérdida, cada proceso de recodificación (nuevo guardado) realizado en la imagen provoca una mayor pérdida de calidad es decir algo de la información que contiene esa imagen se reduce, aunque generalmente esta pérdida es imperceptible al ojo humano [31].

El algoritmo jpeg se basa en una cuadrícula de 8x8 píxeles, cada cuadrícula cuadrada de 8x8 se trata y comprime por separado; Si la imagen no se modifica, todos estos cuadrados de 8x8 mostrarán el mismo nivel de error potencial, si la imagen jpeg se guarda nuevamente, entonces cada cuadrado debe reducirse continuamente hasta aproximadamente el mismo nivel [28].

2.2.9.2.Formato de imagen PNG

El formato PNG fue creado como un reemplazo mejorado y no patentado para Graphics Interchange Format (GIF), y es el formato de compresión de imágenes sin pérdidas más utilizado en Internet [32].

PNG ofrece la posibilidad de determinar diferentes profundidades de color y gamas de color seleccionadas de manera flexible**,** también se ha desarrollado con la intención de crear una alternativa moderna de acceso libre al formato GIF que está sujeto a una licencia: al igual que el formato GIF, el PNG cuenta con un canal alfa para determinar zonas transparentes en la imagen que se precisan, entre otros, para crear logotipos e iconos para páginas web y aplicaciones [33].

Para el formato PNG los porcentajes de compresión en general son comparables con JPEG entre un 25 y un 50% de calidad. Estas características convierten a PNG en un formato altamente conveniente de emplear al igual que JPEG, a pesar de no tener la posibilidad de seleccionar la calidad de compresión [34].

2.2.10. Análisis forense digital

El análisis forense digital es una rama de la policía científica centrada en la detección, adquisición, tratamiento, análisis y comunicación de datos almacenados por medios electrónicos [35]. De manera más formal podemos definir el Análisis Forense Digital como un conjunto de principios y técnicas que comprende el proceso de adquisición, preservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial [36].

2.2.11. Integridad de la evidencia digital

La evidencia digital tiene la característica de ser volátil y fácilmente manipulable, siendo vital considerar los siguientes principios ya que estos permiten conocer qué se puede y no hacer cuando se trata con evidencia digital [37].

La evidencia debe ser admisible para poder ser utilizada en la corte, debe ser auténtica, real y relacionarse con el incidente de manera relevante, debe ser completa ser suficiente, demostrar una perspectiva integral del incidente y poder

probar las acciones o inocencia del atacante, la evidencia que se recolecta y posteriormente se analiza, no debe causar duda de su autenticidad y veracidad; en otras palabras, contar toda la historia, ser confiable y por último la evidencia debe ser creíble claramente entendible y convincente para un jurado [38].

2.2.12. Metadatos

El término se refiere a la información que complementa los datos propiamente dichos. A menudo, los metadatos proporcionan detalles sobre el contexto del contenido a mayores o dan indicaciones sobre cómo manejar los datos. De este modo, los metadatos desempeñan un papel importante tanto en la informática como en la computación de datos convencional [39].

2.2.13. Algoritmos Esteganográficos

2.2.13.1. Algoritmo Esteganográfico LSB (Least Significant Bit)

Es el algoritmo más fácil de implementar, por lo cual es muy utilizado para realizar Esteganografía con imágenes y archivos de audio. El proceso de embebido, consiste en sustituir x-bits de información secreta, por los x-bits, menos significativos, usados para representar el valor de un píxel de la imagen que se utilizará para cubierta. En el proceso de extracción, se toman los x-bits menos significativos de cada píxel de la estego-imagen y se reconstruye la información secreta como se muestra en la **Figura 5 Descripción del Algoritmo LSB**

OpenStego implementa el algoritmo básico de esteganografía para imágenes, LSB el modo de funcionamiento de esta herramienta es que acepta cualquier formato como imagen de entrada, el programa permite guardar la estego-imagen generada con el formato bmp sin importar su formato original [41].

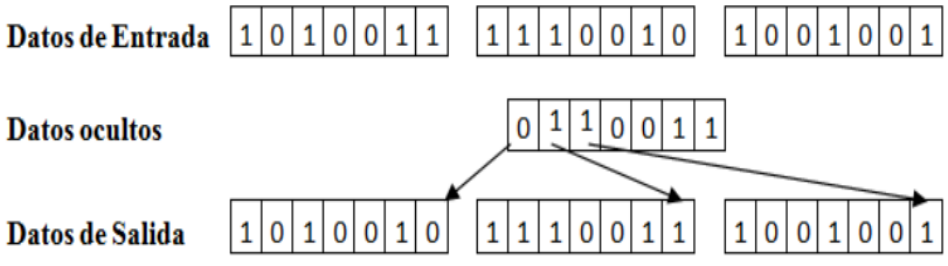

Figura 5 *Descripción del Algoritmo LSB*

2.2.13.2. Algoritmo Esteganográfico F5

F5 es un algoritmo para ocultar información en imágenes JPEG; para ocultar información, F5 suma 1 a los coeficientes con valor positivo y resta uno a los coeficientes con valor negativo. Los coeficientes con valor cero no se modifican, pues esto alteraría la estadística de la imagen significativamente. F5 usa técnicas de matrix embedding para ocultar la información. Esto permite realizar menos cambios en la imagen, para ocultar la misma cantidad de datos. La implementación original de F5 está realizada en Java esta implementación la usan diferentes herramientas como StegoSuite [42].

2.2.14. Algoritmos Estegoanalítico

2.2.14.1. Estegoanálisis estadístico en el dominio de la transformada

En este tipo de análisis se observa que los coeficientes DCT cuantificados se distribuyen simétricamente alrededor de cero para imágenes portadoras, mientras que cuando se incrusta un mensaje estas distribuciones se ven alteradas. Para detectar una estego-imagen en este caso se usa estadísticas chisquare. También existen otros ataques basados en el análisis de las pérdidas de simetría del histograma de coeficientes después de la incrustación de información [43].

2.3. Metodología del Proyecto

2.3.1. Metodología de la investigación

Por la poca información que existe sobre el análisis de la integridad de imágenes usando métodos estegoanalíticos y análisis de nivel de error que recopilen información de proyectos e investigaciones, se empleó la metodología de investigación de tipo exploratorio [44]. En base a revisión bibliográfica se investigó información de trabajos relacionados con el tema propuesto, comparando patrones y características para establecer diferencias y semejanzas frente el tema propuesto.

La metodología de investigación de tipo diagnóstico se centra en el análisis y evaluación de una situación actual [44]. Comparando las diferencias de compresión entre regiones de una imagen, se pueden resaltar las áreas con cambios significativos. Al comparar las tasas de compresión entre diferentes regiones de la

imagen, se podrán identificar áreas que han sido modificadas, la evaluación de la integridad de la imagen es necesaria para verificar autenticidad.

2.3.2. Técnicas e instrumentos de recolección de datos

Para la recolección de información se han usado dos tipos de técnicas como son la recopilación documental y bibliográfica. Al revisar la literatura existente, se puede obtener una mejor comprensión más profunda de los fundamentos teóricos que respaldan los métodos y enfoques con el fin de enriquecer y respaldar la investigación para este proyecto.

Además, la recopilación de imágenes de fuentes diversas sirve como ejemplos prácticos para ilustrar los conceptos teóricos. Los casos reales proporcionan ejemplos concretos de problemas y soluciones, lo que permite ayudar a entender mejor la aplicación práctica de los métodos forenses digitales.

En **recopilación documental y bibliográfica**, se busca información de diferentes fuentes bibliográficas de acuerdo con el tema establecido en proyectos similares.

2.3.3. Metodología de desarrollo

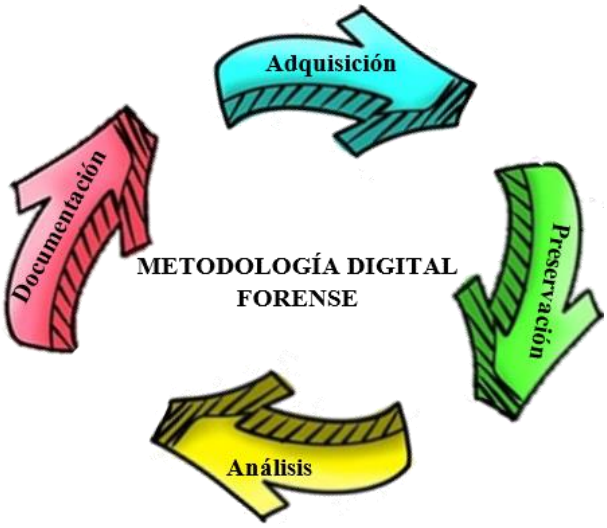

Figura 6 *Fases de la metodología digital forense*

Para llevar a cabo una investigación forense, es esencial seguir un método científico establecido y utilizar la tecnología disponible para descubrir, recopilar, procesar e interpretar datos, por ello se plantea la metodología la cual describe un conjunto de mejores prácticas en el examen forense de tecnología digital [45] y basado en los

lineamientos de la metodología del análisis forense [6], el proyecto se enfocará en las cuatro primeras fases descritas a continuación:

- **Fase de Adquisición:** Esta fase se apoya en afirmar la escena y ordenar los objetos hallados en el sitio, reconociendo al principio que las pruebas observadas tienen la posibilidad de manifestarse en forma física por medio de los dispositivos tangibles y de manera lógica por medio de los datos, y que además tienen la posibilidad de estar dependiendo funcionalmente en aquel instante de otros recursos como energía eléctrica o conexión a una red de datos [46].
- **Fase de preservación:** La evidencia debe ser preservada en su estado original. Cuando la información es analizada, los datos de los archivos pueden cambiar, lo que puede ser relevante en un proceso judicial. Los sistemas tradicionales para realizar copias de seguridad no captan toda la información en un sistema, y parte de la información puede perderse. Por lo que es necesario realizar copias de seguridad de todos los canales de bits, como discos rígidos, unidad flash USB, cámaras, etc. [46].
- **Fase de Análisis:** Una vez obtenida la evidencia digital, se procede hacer el uso de herramientas que permitan hacer legible la información. Durante esta fase el proceso para realizar el análisis será del correspondiente a volcados de memoria RAM, clonación de disco duros y copias potenciales de pruebas digitales [46].
- **Fase de Documentación:**

  En el Informe Técnico se utilizará un lenguaje que cualquier profesional de la rama va a poder entender; determinando los métodos, herramientas usadas y los resultados logrados de las metas planteadas [46].

CAPÍTULO 3. PROPUESTA

3.1. Análisis de requerimientos

3.1.1. Herramientas para el análisis forense

En la siguiente tabla se detallan las herramientas forenses a utilizar para este proyecto.

Herramienta	Descripción
VirtualBox [47].	• Software de virtualización multiplataforma de código abierto.
Kali Linux [48]	• Basado en Debian. • Diseñada para auditoria de seguridad, test de intrusión e informática forense.
Caine OS [49]	• Distribución GNU/Linux • Entorno forense completo
Autopsy [50]	• Plataforma forense digital • Código abierto
AccessData FTK Imager [51]	• Capacidades completas de imagen de disco • Imágenes de contenido personalizadas • Montaje de informe forense • Informes hash
MD5 & SHA Checksum Utility [52].	• Herramienta utilizada para verificar la integridad y autenticidad de archivos calculando y comparando sus valores de suma de verificación.
Fotoforensics [53]	• Algoritmo para el análisis forense de una imagen
Foca (Fingerprinting Organizations with Collected Archives) [54]	• Descubre metadatos y datos ocultos en los archivos o imágenes que escanea.

WinHex [55]	• Editor Hexadecimal, inspecciona y edita todo tipo de archivos. • Analiza y compara archivos • Cifrado AES de 256bits
ExifTool [56]	• Admite formatos de metadatos diferentes EXIF , GPS , IPTC , XMP , JFIF , Geo TIFF , ICCProfile , Photoshop IRB , FlashPix , AFCP e ID3 , Lyrics3 • Notas de fabricante de cámaras digitales Canon , Casio , DJI , FLIR , FujiFilm , GE , GoPro , HP , JVC/Victor , Kodak , Leaf , Minolta/KonicaMinolta , Motorola , Nikon , Nintendo , Olympus/Epson , Panasonic/Leica , Pentax/Asahi , Phase One , Reconyx , Ricoh , Samsung , Sanyo , Sigma /Foveon y Sony .

***Tabla** 1 Herramientas para análisis forense*

3.1.2. Herramientas de Software para validar la integridad de imágenes

En la siguiente tabla se muestran las herramientas necesarias para validar la integridad de las imágenes para el proceso de la esteganografía:

Herramienta	Descripción
StegoSuite [57]	• Compatibles con archivos jpge, png, gif, bmp. • Escrito en java, la versión más reciente es 0.8 • Diseñado para sistemas operativos Windows, Linux, Debian o Ubuntu. • Oculta información en archivos de imagen.
OpenStego [58]	• Compatibles con archivos bmp, gif, jpeg, png, tif, tiff, wbmp. • La versión más reciente es 0.8.4, escrita en Java.

	• Sistema Operativo Windows y Ubuntu. • Permite ocultar archivos en otros archivos portadores y extraer los archivos ocultos.
SSuite Picsel [59]	• Versión más reciente es la 2.8.1, escrita en java. • Se ejecuta en todos los sistemas Windows: 32 bits/64 bits. • Tipos de formatos compatibles bmp, jpg, png y wmf. • Permite esconder archivos de texto en una imagen, se carga una imagen original, se ingresa un mensaje dentro del editor de texto o se carga un archivo de texto se guarda la imagen cifrada con su texto secreto dentro con un nombre diferente al de la imagen original.
SteganPEG [60]	• Formato compatible jpge, escrito en java. • Puede ocultar varios archivos en una imagen jpeg. • Muestra una indicación de cuánto espacio queda en la imagen para agregar más archivos. • Comprime los archivos antes de ocultarlos, para que se pueda ocultar una mayor cantidad de archivos.

Tabla 2 *Herramientas comunes para esteganografía*

Para el proceso de estegoanálisis se muestran las herramientas en la siguiente tabla:

Herramienta	Descripción
StegSolve [61]	• Compatibles con archivos gif, png y jpge. • Sistema operativo Windows y Linux • Permite analizar la imagen en diferentes planos, quitando fragmentos de la imagen hasta encontrar si hay algún mensaje incrustado. • Contiene más de 10 planos diferentes como Alpha, Blue, Green, Red, XOR, etc.
StegoSuite [57]	• Compatibles con archivos jpge, png, gif, bmp. • Escrito en java, la versión más reciente es 0.8 • Diseñado para sistemas operativos Windows, Linux, Debian o Ubuntu. • Oculta información en archivos de imagen y extrae.

StegHide [62]	• Soporte para archivos jpeg, bmp y audio (wav, au) • La versión actual es de 0.5.1 • Herramienta versátil y madura para encriptar y ocultar datos.

Tabla 3 *Herramientas comunes para estegoanálisis*

3.2. Procedimiento Técnico

Este procedimiento técnico implica planificación, ejecución y documentación de cada fase del proceso, desde la recopilación inicial de la evidencia hasta la presentación de resultados. La preservación de la integridad de la evidencia, la aplicación de herramientas forenses especializadas son elementos esenciales que definen la calidad y la confiabilidad de una investigación forense. Este campo, en constante evolución, exige no solo conocimientos técnicos sólidos, sino también un compromiso inquebrantable con la legalidad, la seguridad de la información y la ética profesional. En este contexto, se explora los pasos fundamentales de la metodología forense, destacando la importancia de la formación continua, la adaptabilidad y la colaboración, elementos clave para el éxito en la aplicación de esta disciplina.

Figura 7 *Procedimiento técnico de la metodología forense*

3.3. Desarrollo y Pruebas

Durante la fase de análisis se implementaron las técnicas esteganográficas y análisis de nivel de Error ELA utilizando las herramientas estegoanalíticas. En este apartado se proporcionará el desarrollo de las pruebas como se muestran a continuación:

En la **Tabla 4** Reporte de evidencia digital A01 Esteganografía detalla el desarrollo de la prueba de esteganográfica realizada a la imagen con formato jpg.

En la **Tabla 5** Reporte de evidencia digital A-02 Estegoanálisis se detalla el desarrollo de la prueba de estegoanálisis realizada a la imagen formato png.

METOLOGÍA FORENSE DIGITAL

REPORTE DE ANÁLISIS DE EVIDENCIA DIGITAL

DATOS DEL ANÁLISIS			
Título del análisis:	Esteganografía	**Realizado por:**	Angie Carvajal S.
No. Prueba:	A-01	**Fecha inicio:**	23/11/2023
Formato de la Imagen:	**JPGE**	**Fecha fin:**	23/11/2023
DETALLES DEL ANÁLISIS			
Objetivo del experimento:	Embeber un archivo en una imagen.	**Fase:**	Análisis de la evidencia
Nivel complejidad prueba:	Medio	**Tiempo ejecución:**	10 minutos
HERRAMIENTAS APLICADAS			
Software:	QuickHash Stegosuite AccessData Ftk imager MD5&SHA Autopsy WinHex	**Virtualización:**	Caine
Software en línea:	FotoForensics		
DISEÑO DEL EXPERIMENTO			

Procedimientos:	**Descripción del procedimiento:**
1. Imagen adquirida desde un USB y creación de imagen forense 2. Visualización de la información de la Copia Forense y creación del Hash. 3. Realización de la esteganografía a imagen jpg con la herramienta StegoSuite de Caine. 4. Visualización de la metadata de la imagen embebida tomada desde FotoForensics. 5. Imagen tomada desde un USB y creación de imagen forense	Anexo 1. Fase de adquisición Anexo 2. Fase de Preservación Anexo 3. Fase de Análisis Anexo 4. Fase de Documentación
Resultados esperados: 1. Incrustar un archivo .docx a la imagen jpg. 2. El tamaño de la imagen esteganografiada sea menor que la imagen original. 3. El valor hash de la imagen sea diferente al de la original.	**Resultados obtenidos:** 1. Incrustación exitosa sin afectar su apariencia visual de la imagen original. 2. Compresión de datos al examinar la metadata. 3. Variación del hash por la incrustación
Conclusiones: Se realizó la esteganografía a la imagen jpg sin afectar significativamente la apariencia original de la imagen.	**Validado** ■ Invalidado ☐ No concluyente ☐

Tabla 4 *Reporte de evidencia digital A01 Esteganografía*

METOLOGÍA FORENSE DIGITAL

REPORTE DE ANÁLISIS DE EVIDENCIA DIGITAL

DATOS DEL ANÁLISIS			
Título del análisis:	Estegoanálisis	**Realizado por:**	Angie Carvajal S.
No. Prueba:	A-02	**Fecha inicio:**	23/11/2023
Formato de la Imagen:	**PNG**	**Fecha fin:**	23/11/2023
DETALLES DEL ANÁLISIS			
Objetivo del experimento:	Extraer un archivo de una imagen.	**Fase:**	Análisis de la evidencia
Nivel complejidad prueba:	Medio	**Tiempo ejecución:**	10 minutos
HERRAMIENTAS APLICADAS			
Software: **Software en linea:**	AccessData Ftk imager MD5&SHA Autopsy OpenStego	**Virtualización :**	
DISEÑO DEL EXPERIMENTO			
Procedimientos: 1. Imagen adquirida desde un disco duro y creación de imagen forense. 2. Visualización de la información de la Copia Forense y creación del Hash. 3. Realización del estegoanálisis a imagen png con la herramienta OpenStego.		**Descripción del procedimiento:** Anexo 1. Fase de adquisición Anexo 2. Fase de Preservación Anexo 3. Fase de Análisis Anexo 4. Fase de Documentación	
Resultados esperados:		**Resultados obtenidos:**	

1. Analizar la imagen en busca de posibles datos ocultos. 2. Extraer la información con la herramienta.	Con Extract Data la herramienta intentará detectar la presencia de los datos en la imagen png.
Conclusiones: Se realizó el estegoanálisis a la imagen png ya que OpenStego detecta información oculta.	**Validado** ☑ Invalidado ☐ No concluyente ☐

Tabla 5 *Reporte de evidencia digital A-02 Estegoanálisis*

REPORTE DE ANÁLISIS DE EVIDENCIA DIGITAL

DATOS DEL ANÁLISIS			
Título del análisis:	Nivel de error ELA	**Realizado por:**	Angie Carvajal S.
No. Prueba:	A-03	**Fecha inicio:**	23/11/2023
Formato de la Imagen:	**JPGE**	**Fecha fin:**	23/11/2023
DETALLES DEL ANÁLISIS			
Objetivo del experimento:	Detectar regiones afectadas en la imagen.	**Fase:**	Análisis de la evidencia
Nivel complejidad prueba:	Medio	**Tiempo ejecución:**	10 minutos
HERRAMIENTAS APLICADAS			
Software:	AccessData Ftk imager MD5&SHA Autopsy	**Virtualización:**	
Software en línea:	FotoForensics		
DISEÑO DEL EXPERIMENTO			
Procedimientos:		**Descripción del procedimiento:**	

1. Imagen adquirida desde un USB y creación de imagen forense. 2. Visualización de la información de la Copia Forense y creación del Hash. 3. Se calcula el ELA con la herramienta en línea. 4. Diferenciar entre los niveles de error de las imágenes original y modificada. 5. Visualizar las áreas más afectadas, las regiones que más resaltan.	Anexo 1. Fase de adquisición Anexo 2. Fase de Preservación Anexo 3. Fase de Análisis Anexo 4. Fase de Documentación
Resultados esperados: Se visualice las regiones resaltadas por la herramienta ya que suele indicar posibles áreas de manipulación o edición en la imagen.	**Resultados obtenidos:** Las pruebas realizadas con ELA se pudieron identificar a simple vista las regiones o áreas donde los niveles de error son significativamente diferentes.
Conclusiones: cuando la imagen original se comprime a un cierto nivel de calidad utilizando el algoritmo de compresión específico, ELA compara esta imagen original con la misma imagen después de haber sido modificada.	**Validado** ■ Invalidado ☐ No concluyente ☐

Tabla 6 *Reporte de evidencia digital A-03 Análisis de Nivel de Error ELA*

3.4. Reporte de resultados

A continuación, se detallan los resultados obtenidos en la fase de análisis (**Anexo 3**: Fase de Análisis**)** donde se describe las posibles evidencias de manipulación o presencia de información oculta. Para entender los resultados se sugiere ver los apartados APLICANDO ESTEGANOGRAFÍA A LAS IMÁGENES, APLICANDO ESTEGOANÁLISIS A LAS IMÁGENES y APLICANDO NIVEL DE ERROR ELA que muestran ejemplos muchos más detallados, esto facilitará la comprensión de los resultados obtenidos.

- **Esteganografía con la herramienta Stegosuite de CAINE a una imagen jpg.**

Inicialmente, se creó el archivo encuesta.docx que es el mensaje oculto a embeber a la imagen. Cabe mencionar que la imagen original a utilizar ocupa 4,45 MB y su hash es 3DD55B084743A10FF47ECEB8D195B64E.

Posteriormente, utilizando la herramienta StegoSuite se oculta el archivo encuesta.docx a la imagen original y utilizando o no la opción de password que ofrece la herramienta, se obtiene como salida una imagen idéntica a la original a simple vista, pero en tamaño la imagen baja a 2,4MB siendo menor que la imagen original debido a la compresión de datos que la herramienta ejecuta durante el proceso donde comprime y oculta los datos en la imagen.

Y esta herramienta además optimiza el espacio de almacenamiento eliminando redundancias o aplicando procedimientos específicos para minimizar el tamaño de la imagen sin exponer la calidad visual de la misma ya que el objetivo es ocultar información sin afectar significativamente la percepción visual de la imagen. Inclusive esta herramienta elimina ciertos metadatos o información adicional de la imagen original durante el proceso de incrustación como se muestra en la **Figura 42** Metadata de la imagen incrustada utilizando FotoForensics donde solo se puede visualizar algunos de los metadatos de la imagen original.

Se compara el hash de la imagen original y con el hash de la imagen incrustada que en este caso es 347A49E75218A20313E5CF84D4EB7D87, como se puede apreciar el valor numérico se ha modificado ya que cualquier cambio mínimo que

sea este, hace que el hash sea diferente ya que el objetivo principal de estos algoritmos es que sea como una huella digital única para cada imagen así sean dos imágenes idénticas.

Mediante el editor WinHex se presenta los datos que se pueden extraer a través de esta herramienta. Solo se presentarán los datos a partir de la cabecera de los archivos jpg que consisten en los bytes FFD8 (en hexadecimal), ya que cuando se realiza el proceso de incrustación la información se oculta desde la cabecera hasta final del archivo.

- **Estegoanálisis con la herramienta OpenStego de una imagen png**.

La herramienta OpenStego nos permite analizar una imagen en busca de posibles datos ocultos. A la imagen png incrustada se analiza la metadata como las dimensiones, resolución, y otros detalles técnicos, ya que muchos de ellos suelen ser comprimidos por la imagen y estas características dan indicio a presencia de datos ocultos.

Al seleccionar Extract Data la herramienta intentará detectar la presencia de esos datos en la imagen png especificada ya que OpenStego detecta información oculta mediante análisis de firmas de imágenes para identificar formatos específicos como en la búsqueda de patrones específicos en la cabecera o el pie de una imagen, para así obtener como salida dicho archivo embebido para este ejemplo se obtuvo encuesta.docx.

- **Análisis de Nivel de Error ELA a imagen jpg**

Se realiza el análisis de error ELA, se compara el nivel de error en diferentes secciones de la imagen. Si una sección de la imagen muestra un nivel de error significativamente diferente en comparación con el resto de la imagen, es una indicación de que esa sección podría haber sido modificada o editada digitalmente.

Utilizando la herramienta en línea FotoForensisc se calcula el ELA a la imagen generalmente con formatos JPEG, cuando la imagen original se comprime a un cierto nivel de calidad utilizando el algoritmo de compresión específico, ELA compara esta imagen original con la misma imagen después de haber sido modificada, calcula la diferencia entre los niveles de error de las imágenes original

y modificada. Esta diferencia se representa como una imagen que resalta las áreas donde los niveles de error son significativamente diferentes.

FotoForensisc crea un mapa de diferencias que muestra visualmente las áreas donde se han detectado cambios en los niveles de error. Las regiones resaltadas en este mapa suelen indicar posibles áreas de manipulación o edición en la imagen como se muestra en la **Figura 66** Imagen con ELA regiones sospechosas que muestran grandes diferencias en los nivele de error.

CONCLUSIONES

Desde la antigüedad la humanidad ha buscado maneras de enviar mensajes de forma oculta, asegurándose que estos permanezcan encubiertos incluso si son interceptados. Esa técnica se la denomina esteganografía que consiste en incrustar un archivo en una imagen y pasar completamente desapercibido ante el ojo humano.

A diferencia de la criptografía que consiste en enviar información cifrada donde la información debe protegerse de terceros, la esteganografía va más allá de eso ya que este pretende esconder información dentro de otro objeto sustituyendo los bits menos significativos para lograr la incrustación ya que las alteraciones deben ser mínimas evitando así levantar sospechas haciendo que la información oculta sea difícil de detectar.

El estegoanálisis por otro lado, se centra en detectar y analizar la presencia de información oculta mediante las técnicas esteganográficas y ha sido evaluado en este contexto para determinar su capacidad para detectar manipulaciones en imágenes. Las herramientas especializadas diseñadas para automatizar el análisis de información oculta pueden utilizar algoritmos avanzados para detectar patrones o cambios específicos que son invisibles a simple vista.

Con respecto, al Análisis de Nivel de Error (ELA) se basa en mostrar el nivel de compresión de cada píxel, aplicando diferentes colores a las zonas con mayores errores. FotoForensics es una herramienta en línea que emplea esta técnica ELA la cual permite examinar y revelar posibles áreas o regiones manipuladas en una imagen, esta da como resultado imágenes que difieren del blanco, negro, azul y rojo. Una imagen no editada el ELA se mostrará uniforme con una intensidad muy baja (negro), pero a medida que se realizan ediciones o manipulaciones a la imagen este muestra las inconsistencias de forma que ELA toma más intensidad (blanco), las áreas modificadas tienen niveles de error distintos en comparación con la imagen ya que compara y resalta las áreas que han sido alteradas.

Con el arribo de la digitalización asociada a las tecnologías de la información, las posibilidades de la esteganografía se han aumentado drásticamente, las imágenes, los videos hasta los archivos de audios se han identificados como portadores ideales

para ocultar mensajes secretos, siendo así los más dables para este tipo de aplicación ya que debido a la gran cantidad de información que contiene y su amplia disponibilidad en internet y el tipo de archivo que puede intercambiarse libremente entre usuarios sin despertar sospecha son el medio idóneo para este tipo de aplicaciones. Además, no solo se usan los contenidos multimedia sino también archivos de textos, código fuente, o hasta incluso los mismos protocolos de internet ya que estos permiten establecer canales esteganográficos ocultos para tener comunicaciones privadas sin que nadie se dé cuenta. Expertos de todo el mundo centran su trabajo en el desarrollo de nuevas técnicas de esteganografía y de sistemas de detección de anomalías que se puedan emplear para discriminar si un objeto digital es lo que parece o deberá examinarse a fondo para determinar si esconde alguna información.

La identificación de una imagen estenografiada puede ser desafiante, por los métodos específicos de esteganografía utilizados y las técnicas de ocultamiento de información. La efectividad de los Firewalls (firewire), Sistemas de Detección de Intrusiones (IDS) y Dispositivos de Gestión Unificada de Amenazas (UTM) deben mantenerse al día para ser seguras ya que la dificultad de detección aumenta con la complejidad de las técnicas utilizadas y tener capacidad para adaptarse a nuevas técnicas de ocultamiento de información. Estos son componentes de seguridad informática diseñados para identificar y prevenir amenazas, pero su capacidad para detectar esteganografía puede ser limitada, sin embargo, si una técnica esteganográfica está dentro de las bases de datos de firmas y patrones hay una gran probabilidad que sea detectada.

Es posible que se pueda infectar un teléfono móvil a través de un archivo ejecutable en una imagen o una imagen incrustada con algún archivo, aunque estos ataques no suelan ser comunes, las empresas cuentan con parches a estos fallos de seguridad. En el 2019 WhatsApp y Google emitieron una alerta. Google tuvo que solucionar un problema de vulnerabilidad en su sistema operativo Android ya que estaba expuesto a que un atacante pudiera ejecutar algún código malicioso arbitrariamente en el dispositivo a través de una imagen con formato png y este pudiese infectar el móvil. La vulnerabilidad de WhatsApp proporcionaba a los ciberatacantes añadir

código malicioso en un móvil con el simple hecho de realizar una descarga de un GIF cuando este abriera la galería desde la app, y se ejecutara permitiera que la otra parte acceda a otras aplicaciones del teléfono. Los métodos de protección más desarrollados disponen de sistemas de detección de malware basado en el comportamiento del código.

RECOMENDACIONES

- Desarrollar un algoritmo para la detección de esteganografía para abordar amenazas digitales, proteger la integridad y seguridad de la información en un entorno digital en constante cambio.
- Fomentar la investigación de nuevos estilos de esteganografía, como la incrustación de información en formatos emergentes, en dispositivos y plataformas específicos.
- Antes de abordar o realizar algún tipo de análisis de integridad de imágenes se debe tener en cuenta los aspectos éticos y legales relacionados con la manipulación de datos.

REFERENCIAS

[1] D. ALEJANDRO CÁCERES, B. E. VACA BARAHONA y M. F. GONZÁLEZ PUENTE, «ANÁLISIS METODOLÓGICO DE EXTRACIÓN DE EVIDENCIA CON HERRAMIENTAS CYBER FORENSES EN DISPOSITIVOS DE ALMACENAMIENTO,» *Revista de Ciencias de Seguridad y Defensa*, vol. IV, nº 8, pp. 126-141, 2019.

[2] S. Roatta, M. E. Casco y M. Fogliato, «EL TRATAMIENTO DE LA EVIDENCIA DIGITAL Y LAS NORMAS ISO/IEC 27037:2012,» 2016. [En línea]. Available: https://core.ac.uk/reader/76489970.

[3] D. F. De Carvhalo, «ESTEGANOGRAFÍA EN VIDEOS COMPRIMIDOS MPEG-4,» OCTUBRE 2008. [En línea]. Available: https://teses.usp.br/teses/disponiveis/55/55134/tde-08062009-143448/publico/DissertacaoDiegoFiorideCarvalho.pdf.

[4] R. D. Muñóz Ardila, «APLICACIÓN MÓVIL PARA LA PROTECCIÓN DE LA PRIVACIDAD DE LA INFORMACIÓN DIGITAL UTILIZANDO TÉCNICAS ESTEGANOGRÁFICAS Y DE ENCRIPTACIÓN.,» 2020. [En línea]. Available: https://repository.unab.edu.co/handle/20.500.12749/14330.

[5] J. D. Coronel Ventimilla, «APLICACIÓN DE LA TÉCNICA DE ESTEGANOGRAFÍA PARA EL MEJORAMIENTO DE LA INTEGRIDAD DE LA INFORMACIÓN EN SISTEMAS ACADÉMICOS BASADOS EN LA WEB, CASO PRÁCTICO https://sisepec.espoch.edu.ec,» 2021. [En línea]. Available: http://dspace.espoch.edu.ec/handle/123456789/18312.

[6] E. Chicano Tejada, GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA. IFCT0109, MÁLAGA: ic editorial, 2014.

[7] S. DR. ACURIO DEL PINO, «MANUAL DE EVIDENCIAS DIGITALES Y ENTORNOS INFORMÁTIICOS. VERSIÓN 2.0,» 7 JULIO 2009. [En línea]. Available: https://www.oas.org/juridico/english/cyb_pan_manual.pdf.

[8] S. N. D. PLANIFICACIÓN, «PLAN DE CREACIÓN DE OPORTUNIDADES 2021 - 2025,» 5 OCTUBRE 2022. [En línea]. Available: https://www.planificacion.gob.ec/wp-content/uploads/2021/09/Plan-de-Creacio%CC%81n-de-Oportunidades-2021-2025-Aprobado.pdf.

[9] linkedin, «Seguridad infórmatica: Informática Forense,» 2023. [En línea]. Available: https://es.linkedin.com/learning/seguridad-informatica-informatica-forense/hashing-como-metodo-de-preservacion-de-evidencias#:~:text=El%20%22hashing%22%20es%20una%20herramienta,n%C3%BAmero%20hexadecimal%20de%20longitud%20fija..

[10] B. Donohue, «Kaspersky daily,» 14 Abril 2014. [En línea]. Available: https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/.

[11] KeepCoding, «¿Qué es una suma de verificacion o checksum?,» 25 Octubre 2023. [En línea]. Available: https://keepcoding.io/blog/suma-de-verificacion-checksum/#:~:text=Una%20suma%20de%20verificaci%C3%B3n%20o%20cheksum%20%2C%20tambi%C3%A9n%20conocida%20como%20suma,la%20integridad%20de%20la%20informaci%C3%B3n..

[12] A. López, «Criptografía: Qué son los algoritmos hash y para qué se utilizan,» RZ redes zones, 12 Abril 2023. [En línea]. Available: https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-hash/.

[13] J. I. De la Rosa, A. Moreno, J. Villa, E. García y M. Araiza, «Comparacion de Tres Codificadores para Imagenes Fijas e implementacion en Lenguaje de Alto Nivel,» *Centro de investigacion y desarroollo de tecnología digital*, pp. 213-219, 2014.

[14] R. Din y A. Samsudin, «Digital Steganalysis: Computational Intelligence Approach,» *INTERNATIONAL JOURNAL OF COMPUTERS*, vol. III, nº I, pp. 161-170, 2009.

[15] F. Sánchez, «Análisis forense sobre imagenes digitales, un ejemplo de su aplicabilidad,» *Revista científica Diálogo Forense*, vol. II, nº IV, pp. 1-10, 2021.

[16] F. L. Domínguez, INTRODUCCIÓN A LA INFORMÁTICA FORENSE, MADRID: RA-MA, 2014.

[17] M. Guerra Soto, Análisis forense informático, Madrid: RA-MA, 2021, p. 15.

[18] S. A. Elneser Mesa, M. V. E y J. G. Lalinde Pulido, Aproximacion a la informática forense y el derecho informatico: Ámbito Colombiano, Medellín: FUNLAM, 2013, p. 97.

[19] J. E. Bonilla O, Computación Forense, Bogotá, 2009.

[20] R. D. Varela Velasco, «CRIPTOGRAFÍA, UNA NECESIDAD MODERNA,» *Revista Digital Universitaria*, vol. 7, nº 7, pp. 2-9, 2006.

[21] Merriam-webster.com, «Definition of STEGANOGRAPHY,» 2018. [En línea]. Available: https://www.merriam-webster.com/dictionary/steganography#word-history.

[22] T. Fernández y E. Tamaro, «Biografia de Histieo, Biografías y Vidas LA ENCICLOPEDIA BIOGRÁFICA EN LÍNEA,» 2004. [En línea]. Available: https://www.biografiasyvidas.com/biografia/h/histieo.htm.

[23] P. Wayner, Disappearing Cryptography: Information Hiding: Steganography and Watermarking, 2da. ed., San Francisco, CA, United States: Publishers Inc., 2002.

[24] G. A, I. E, C. A. Espinoza A, S. M y O. C, «Análisis de técnicas esteganográficas y estegoanálisis en canales encubiertos, imágenes y archivos de sonido,» *Vector*, vol. I, nº I, pp. 29-38, 2006.

[25] R. A. Española, «Diccionario histórico de la lengua española,» Equipo Real Academia Española, 31 Agosto 2019. [En línea]. Available: https://www.rae.es/dhle/estegoan%C3%A1lisis.

[26] B. T. Ahmed, «A systematic overview of secure image steganography,» *International Journal of Advances in Applied Sciences (IJAAS)*, vol. 10, nº 2, pp. 178-187, 2021.

[27] J. Pereira, «Análisis forense de fotogrfías digitales,» DIGITALHERITAGE, 2015. [En línea]. Available: http://www.jpereira.net/apuntes-breves/analisis-forense-de-fotografias-digitales.

[28] W. Jonás, «Imagen Forense- Análisis de nivel de error,» [En línea]. Available: https://forensics.map-base.info/report_2/index_en.shtml#:~:text=considered%20very%20carefully.-,ELA%20Analysis,has%20different%20degrees%20of%20compression..

[29] C. A. Ordoñez Santiago, «FORMATOS DE IMAGEN DIGITAL,» *Revista Digital Universitaria*, vol. 5, nº 7, pp. 2-10, 10 Mayo 2005.

[30] Wikipedia, «Formatos de archivos de imagen,» 6 Octubre 2022. [En línea]. Available: https://es.wikipedia.org/wiki/Formatos_de_archivos_de_imagen.

[31] F. D. Barzola Tobar y R. D. Cabrera Velasco, «Comparación entre compresión de audio en diferentes formatos de imágenes equivalentes y el formato de compresión MP3,» 2009. [En línea]. Available: https://www.dspace.espol.edu.ec/bitstream/123456789/21613/1/D-42727.pdf.

[32] M. Pascual Martinez, «Software inteligente de codificación de imagen y vídeo adaptativa a requerimientos de hardware,» 2017-2018. [En línea]. Available: https://repositori.upf.edu/bitstream/handle/10230/33730/TFG_Marc_Pascual.pdf?sequence=1&isAllowed=y.

[33] IONOS, «JPG o PNG: diferencias e idoneidad de los formatos de imagen,» 15 Octubre 2020. [En línea]. Available: https://www.ionos.es/digitalguide/paginas-web/diseno-web/jpg-o-png/.

[34] H. Kaschel C., F. Watkins y E. San Juan U., «COMPRESIÓN DE VOZ MEDIANTE TÉCNICAS DIGITALES PARA EL PROCESAMIENTO DE SEÑALES Y APLICACIÓN DE FORMATOS DE COMPRESIÓN DE IMÁGENES,» *Rev. Fac. Ing. - Univ. Tarapacá,* vol. 13, nº 3, pp. 4-10, 2005.

[35] Interpol, «Análisis Forense Digital,» 2022. [En línea]. Available: https://www.interpol.int/es/Como-trabajamos/Innovacion/Analisis-forense-digital#:~:text=El%20objetivo%20principal%20del%20an%C3%A1lisis,miras%20a%20la%20persecuci%C3%B3n%20penal..

[36] M. López Delgado, «Análisis Forense Digital,» *Hackers & Seguridad,* vol. II, nº I, pp. 1-32, 2007.

[37] M. Sheetz, Computer Forensics an Essentiall Guide for Accountants, Lawyers, and Manager, Canadá: acid-free, 2007.

[38] P. A. Ochoa Arévalo, «THE TREATMENT OF DIGITAL EVIDENCE, A GUIDE TO ITS ACQUISITION AND/OR COLLECTION,» *Economía Política,* nº 28, pp. 35-44, 2018.

[39] IONOS, «¿Qué son los metadatos?,» Digital Guide IONOS, 3 ENERO 2023. [En línea]. Available: https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/que-son-los-metadatos/.

[40] E. Morocho, A. Zambrano, J. Carvajal y G. López, «Análisis del Algoritmo Esteganográfico F5 para Imágenes JPEG a Color,» *Revista Politécnica,* vol. 36, nº 3, pp. 1-7, 2015.

[41] M. Ruiz Tejeida, «Ocultamiento de información en documentos de formato abierto,» Noviembre 2013. [En línea].

[42] «Ataque práctico a F5,» [En línea]. Available: https://daniellerch.me/stego/aletheia/f5-attack-es/.

[43] G. E. ONOFRE CONCHA, «DESARROLLO Y ANÁLISIS DE UNA TÉCNICA ESTEGANOGRÁFICA EN ZONAS RUIDOSAS DE LA IMAGEN MEDIANTE TRANSFORMACIONES DE COLOR REVERSIBLES,» Octubre 2016. [En línea]. Available: https://repositorio.espe.edu.ec/bitstream/21000/12249/1/T-ESPE-053515.pdf.

[44] R. HERNÁNDEZ SAMPIERI, C. FERNÁNDEZ COLLADO y M. D. P. BAPTISTA LUCIO, METODOLOGÍA DE LA INVESTIGACIÓN, 6TA. ed., MÉXICO: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V, 2014.

[45] IOCE, «Guidelines for Best Practice in the Forensic Examination Of Digital Technology,» 2002. [En línea]. Available: https://archive.ph/rct16.

[46] S. G. Patiño Rosado, J. M. Rojas Rosado y H. A. Sacon Klinger, «Methodology for the forensic analysis of images of storage units,» *Revista de Investigación, Formación y Desarrollo: Generando Productividad Institucional*, vol. 11, nº 1, pp. 8-16, 2023.

[47] Oracle, «Virtual Box,» 2023. [En línea]. Available: https://www.virtualbox.org/.

[48] kali, «Kali,» OffSec Services Limited 2023, 2023. [En línea]. Available: https://www.kali.org/.

[49] J. Boucher, «CAINE Computer Forensics Linux Live Distro,» Creative Commons, Octubre 2022. [En línea]. Available: https://www.caine-live.net/.

[50] AUTOPSY, «AUTOPSY DIGITAL FORENSICS,» LABORATORIOS DEL KIT DE SLEUTH, 2023. [En línea]. Available: https://www.autopsy.com/.

[51] Exterro, «exterro Plataforma de software legal GRC,» Exterro, Inc., 2023. [En línea]. Available: https://www.exterro.com/ftk-imager.

[52] F. Cheng, «Utilidad de suma de comprobación MD5 y SHA,» LO4D.COM, 2023. [En línea]. Available: https://md5-sha-checksum-utility.en.lo4d.com/windows.

[53] FotoForensics, «FotoForensics,» Hacker Factor, 2023. [En línea]. Available: https://fotoforensics.com/.

[54] I. W. Hat, «FOCA - Toma de huella organizacional,» Instituto White Hat, 2023. [En línea]. Available: https://whitehatinstitute.com/foca-fingerprinting-organizations-with-collected-

archives/#:~:text=FOCA%20(Fingerprinting%20Organizations%20with%20Collected,in%20the%20documents%20it%20scans..

[55] X.-W. S. T. AG, «WinHex: software de informática forense y recuperación de datos,editor hexadecimal y editor de discos,» 26 Julio 2023. [En línea]. Available: https://www.x-ways.net/winhex/.

[56] ExifTool, «ExifTool de Phil Harvey,» Noviembre 2023. [En línea]. Available: https://exiftool.org/.

[57] GeeksforGeeks, «Image Steganography using Stegosuite in Linux,» 28 Septiembre 2021. [En línea]. Available: https://www.geeksforgeeks.org/image-steganography-using-stegosuite-in-linux/.

[58] V. S, «OpenStego,» [En línea]. Available: https://www.openstego.com/.

[59] G. Software, «SSuite Picsel Security,» Go Green Software , 2003. [En línea]. Available: https://www.ssuiteoffice.com/software/ssuitepicselsecurity.htm.

[60] K. Abhiram, «SteganPEG,» apponic, 2023. [En línea]. Available: https://steganpeg.apponic.com/.

[61] C. Bios, «StegSolve,» MkDocs, 2021. [En línea]. Available: https://wiki.bi0s.in/steganography/stegsolve/.

[62] SOURCEFORGE, «Steghide,» 2003. [En línea]. Available: https://steghide.sourceforge.net/.

ANEXOS

Anexo 1: Fase de Adquisición

La adquisición de las imágenes será tomada desde las unidades de almacenamiento de datos tales como USB, Disco duro y memoria Ram de un ordenador, se adquirirán imágenes originales e imágenes ya manipuladas o editadas para la realización de este proyecto.

Para la hacer la copia forense de las unidades de almacenamientos utilizaremos la herramienta **AccessData FTK Imager 3.4.3.3** que hará la copia bit a bit de los dispositivos. Se procede a realizar el paso a paso de las unidades de almacenamiento.

- **Adquisición de una imagen con formato png desde una unidad de almacenamiento disco duro.**

Se realiza la copia bit a bit de la unidad de almacenamiento y seleccionamos la unidad que se le realizará la copia en este caso es MyPassport como se muestra a continuación.

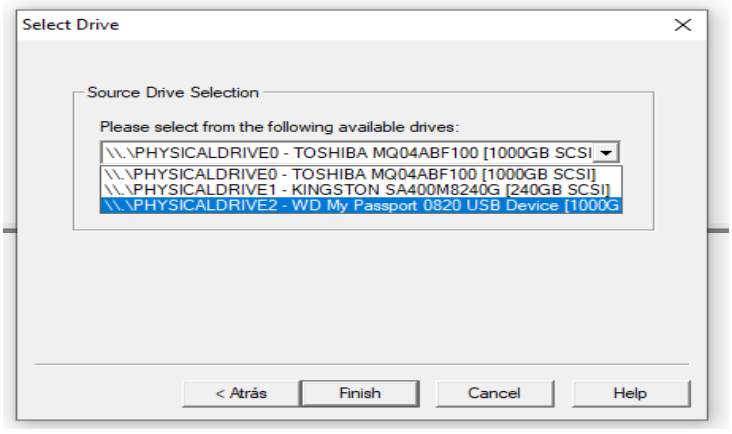

Figura 8 *Cuadro de diálogo de Access Data*

Aparece una nueva ventana de diálogo donde se llenará los siguientes campos como número del caso, nombre, descripción y quien lo realiza.

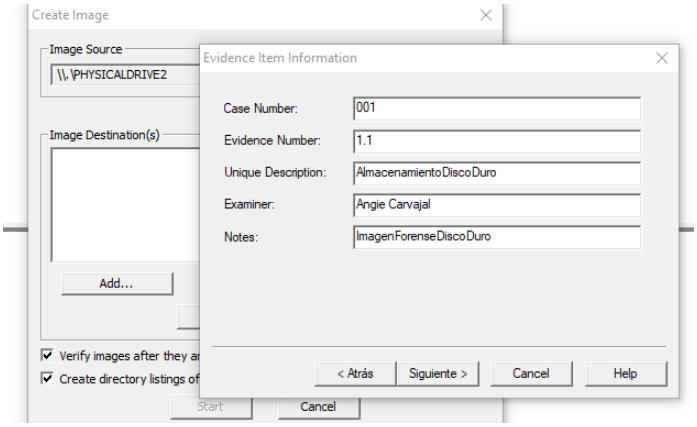

Figura 9 *Ingreso de datos*

Luego se coloca la ruta donde se guardará la copia y se agrega el nombre como se muestra en la imagen.

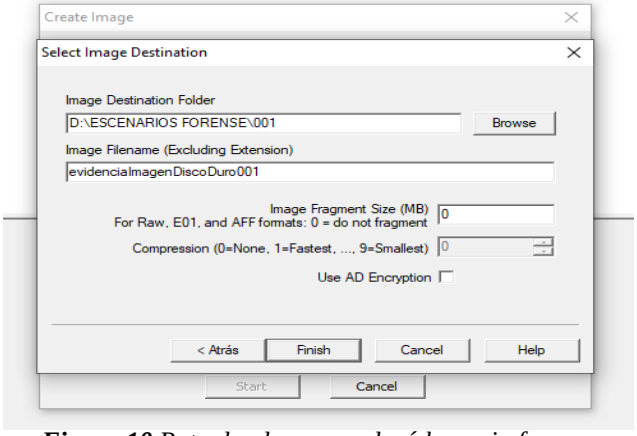

Figura 10 *Ruta donde se guardará la copia forense*

Automáticamente empieza el proceso de creación de imágenes y Accsess Data además de realizar la copia bit a bit genera el código Hash de la imagen que crea.

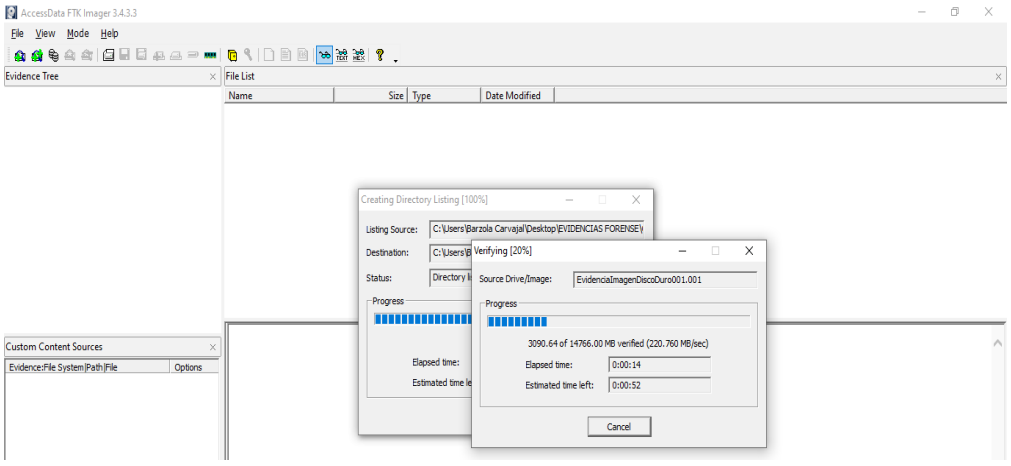

Figura 11 *Creación de la imagen forense*

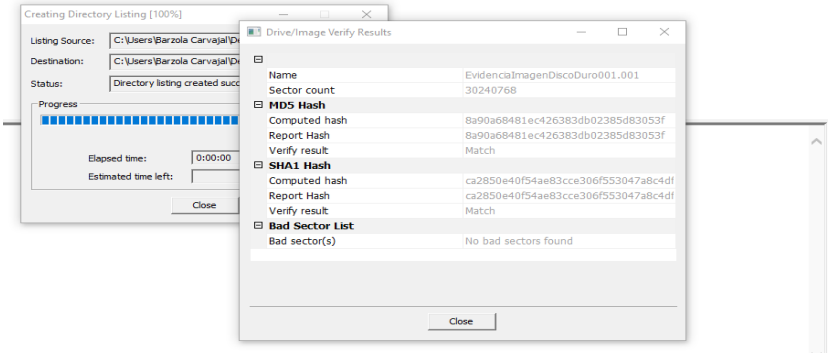

Figura 12 *Generación del Hash automático*

Una vez terminado el proceso se puede acceder a los archivos que se generaron con la copia de la imagen y se pueden visualizar ciertos datos.

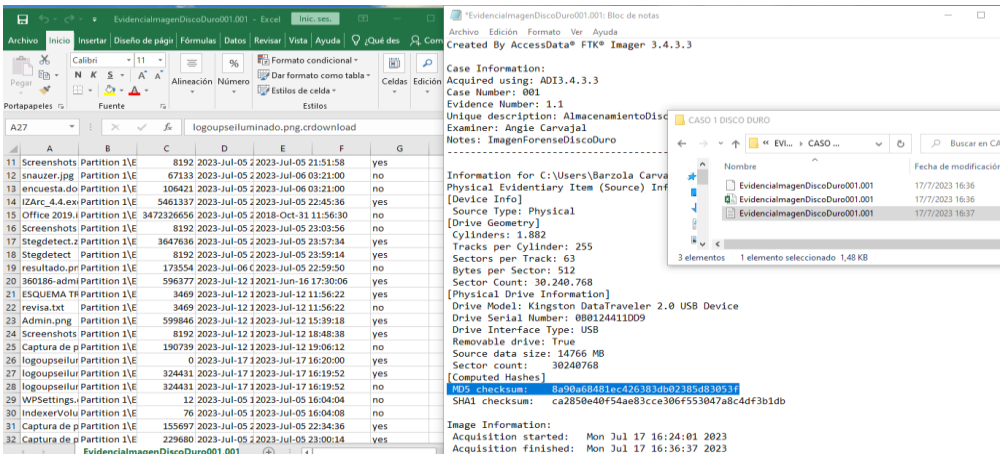

Figura 13 *Accesos a los archivos*

Se procede a generar el hash a la copia forense creada para realizar la verificación y tener en cuenta que la evidencia no ha sido alterada, se usa la herramienta MD5 & SHA Checksum Utility para este proceso.

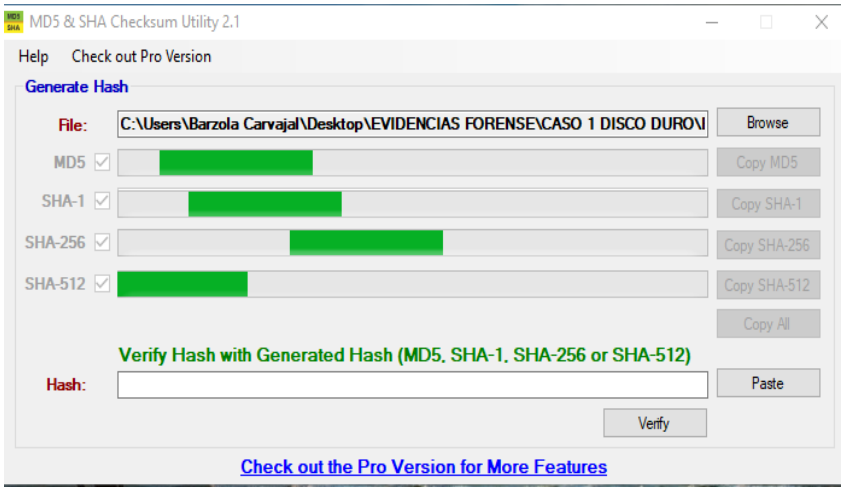

Figura 14 *MD5 & SHA Checksum Utility*

- **Adquisición de una imagen con formato jpg desde una unidad de almacenamiento USB.**

Se crea una copia exacta y completa (una copia bit a bit) de las imágenes seleccionadas utilizando la herramienta AccessData FTK Imager, se elige el nombre del USB donde se va a adquirir la imagen.

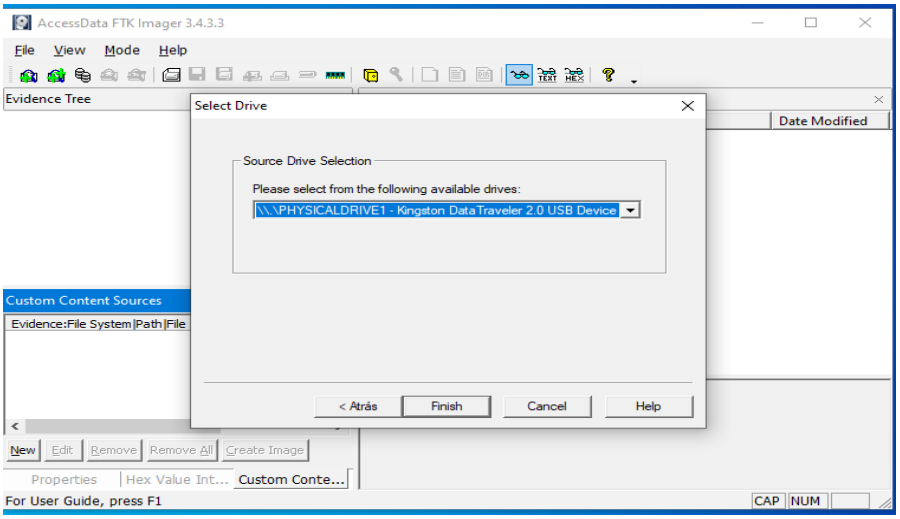

Figura 15 *Cuadro de diálogo Access Data*

Luego se procede a ingresar el número, nombre, descripción y quien realiza el caso.

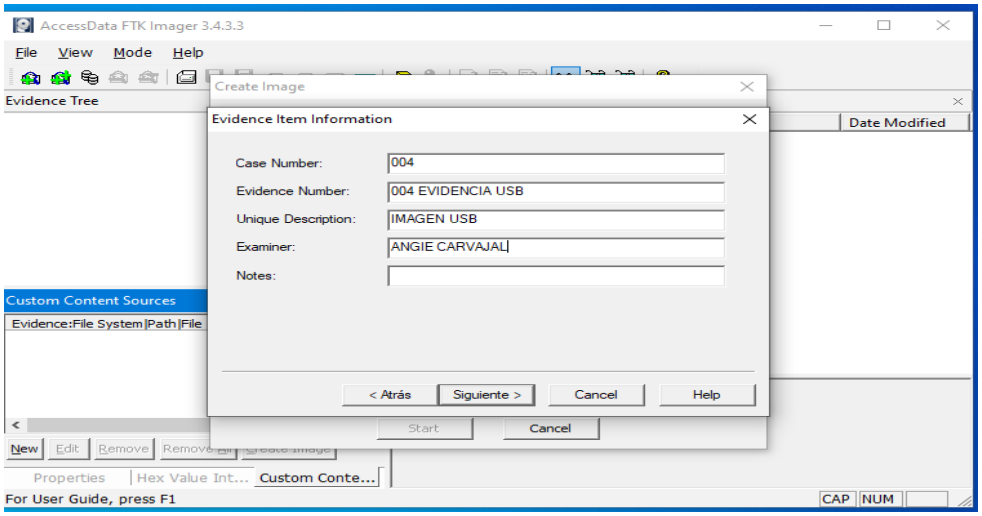

Figura 16 *Ingreso de datos*

Se selecciona la carpeta donde se guardará la imagen que se creará y se le asigna un nombre.

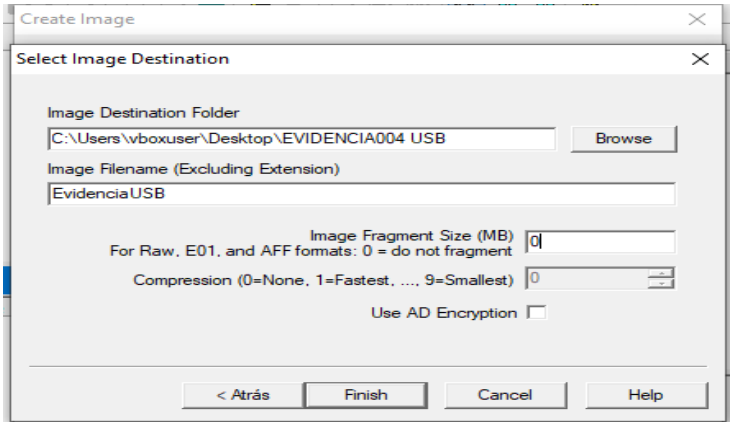

Figura 17 *Ruta de la carpeta para guardar la imagen forense*

Automáticamente empieza el proceso de creación de imágenes y se genera el código Hash de la imagen.

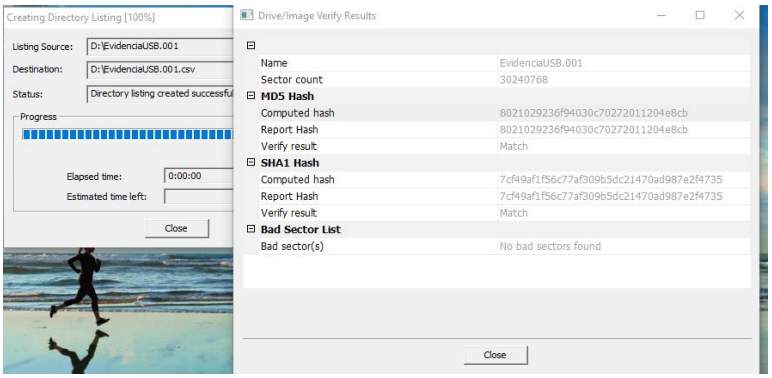

Figura 18 *Creación del Hash*

Una vez creada se puede acceder a los archivos que se generaron con la copia de la imagen y se procede a verificar los datos, cabe mencionar que Access Data Ftk Imager genera automáticamente el código Hash a la evidencia como se muestra en la imagen MD5 Checksum.

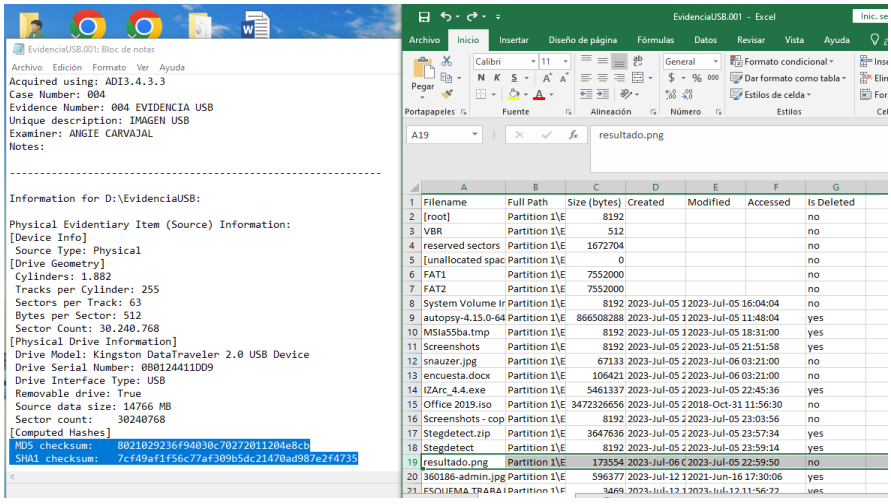

Figura 19 *Acceso a las imágenes*

Anexo 2: Fase de Preservación

- **Preservación de una imagen con formato png desde una unidad de almacenamiento disco duro.**

Para preservar la información adquirida en la fase anterior se procede a extraer la información de la copia forense que se realizó inicialmente, utilizando la herramienta **Autopsy 4.15.0** se creará un nuevo caso llenando los casilleros donde pide los códigos hash obtenidos anteriormente para una mejor autenticidad.

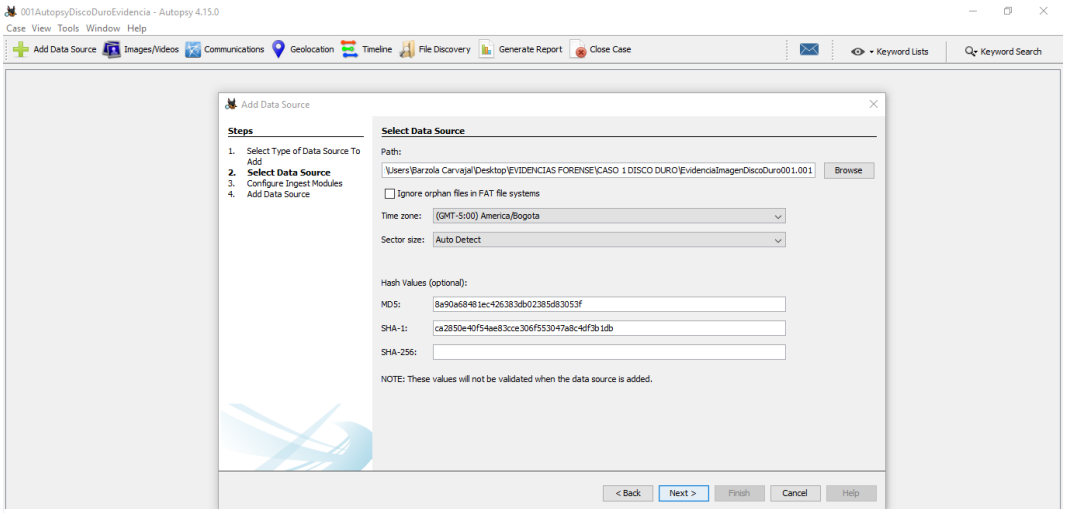

Figura 20 *Cuadro de diálogo de Autopsy*

Se genera el caso y solo queda esperar a que se carguen los datos para poder acceder a la información.

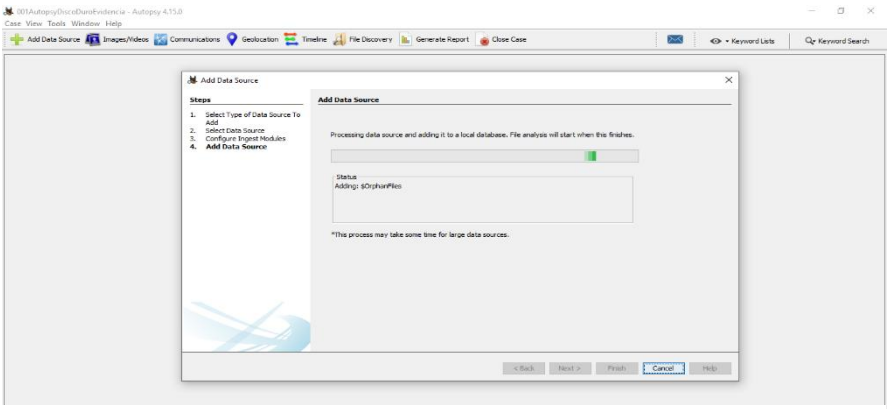

Figura 21 *Generación del caso*

Una vez terminado la carga de datos se podrá visualizar el contenido como se muestra en la imagen, para extraer la imagen y poder usarla, se da clic derecho encima del nombre de la imagen elegimos Extract File(s) y de esta forma obtenemos la imagen y luego procedemos a guardar la imagen según corresponda.

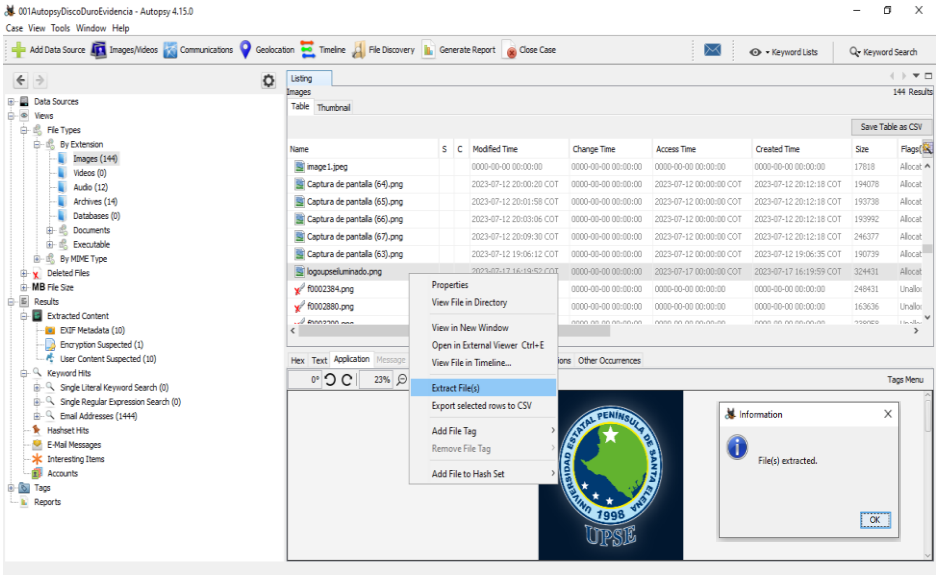

Figura 22 *Visualización de la imagen png*

Se selecciona una de las imágenes para generar el código hash para preservarla y no sea alterada o modificada con la herramienta MD5 & SHA Checksum Utility.

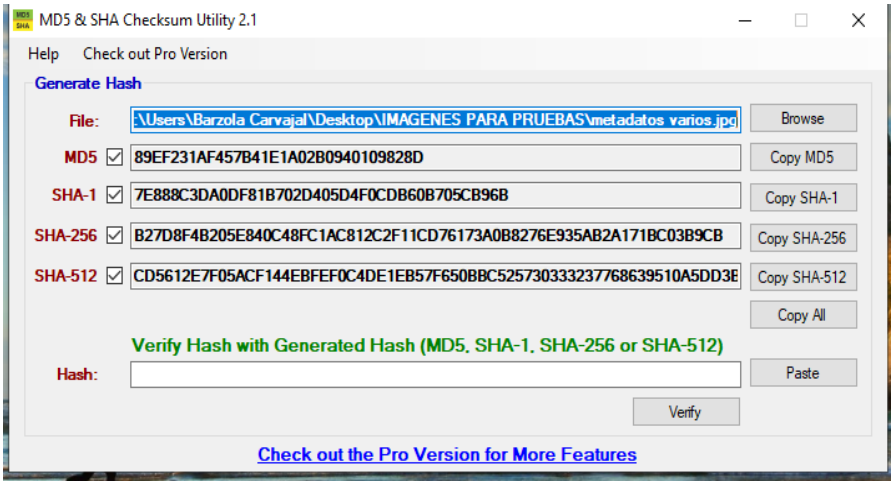

Figura 23 *Hash de la imagen png*

- **Preservación de una imagen con formato jpg desde una unidad de almacenamiento USB.**

Para preservar la información adquirida en la fase anterior se procede a extraer la información de la copia forense que se realizó inicialmente, utilizando la herramienta **Autopsy 4.15.0** se creará un nuevo caso llenando los casilleros donde pide los códigos hash obtenidos anteriormente para el resguardo de la imagen.

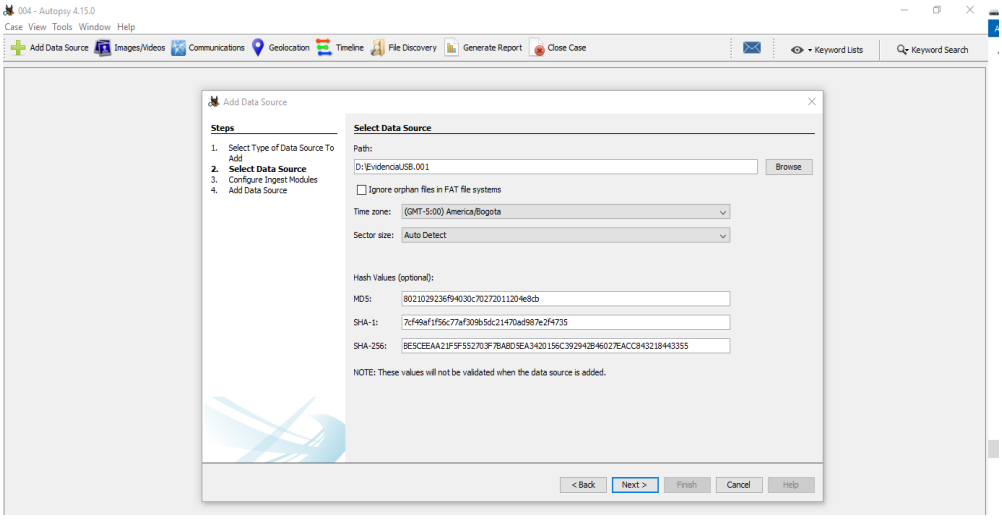

Figura 24 *Cuadro de diálogo de Autopsy*

Se genera el caso y solo queda esperar a que se carguen los datos para poder acceder a la información.

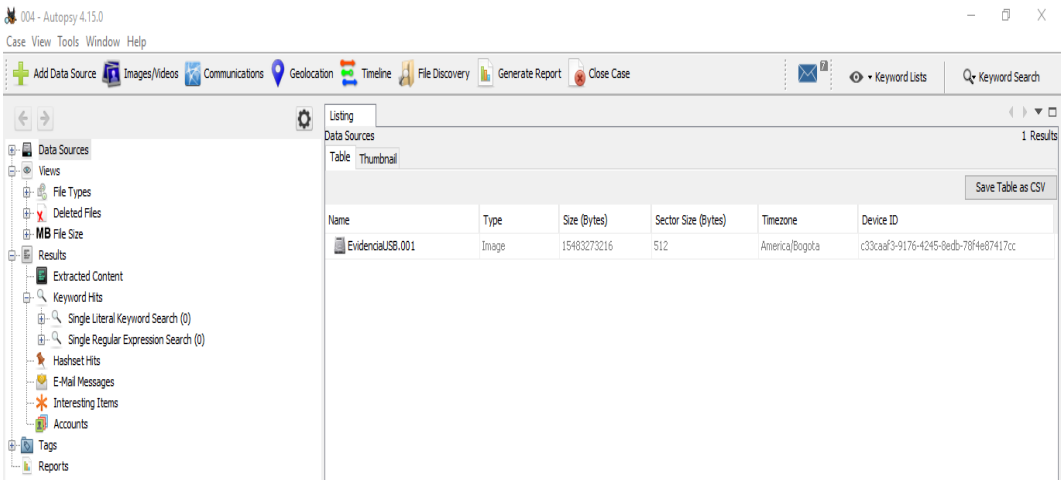

Figura 25 *Generación del caso*

Una vez cargado podemos acceder a toda la información q contiene en este caso se buscará la imagen resultado.png y la extraeremos para realizar el análisis de los metadatos en la fase de análisis.

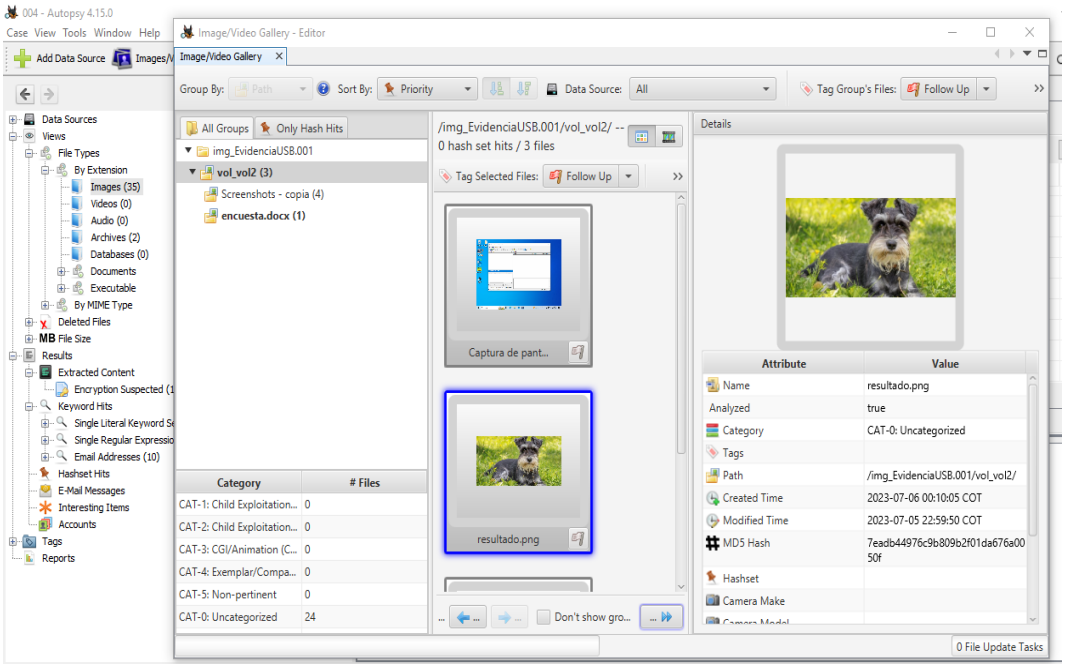

Figura 26 Acceso a la información

Se selecciona una de las imágenes para generar el código hash para preservarla y no sea alterada o modificada con la herramienta MD5 & SHA Checksum Utility.

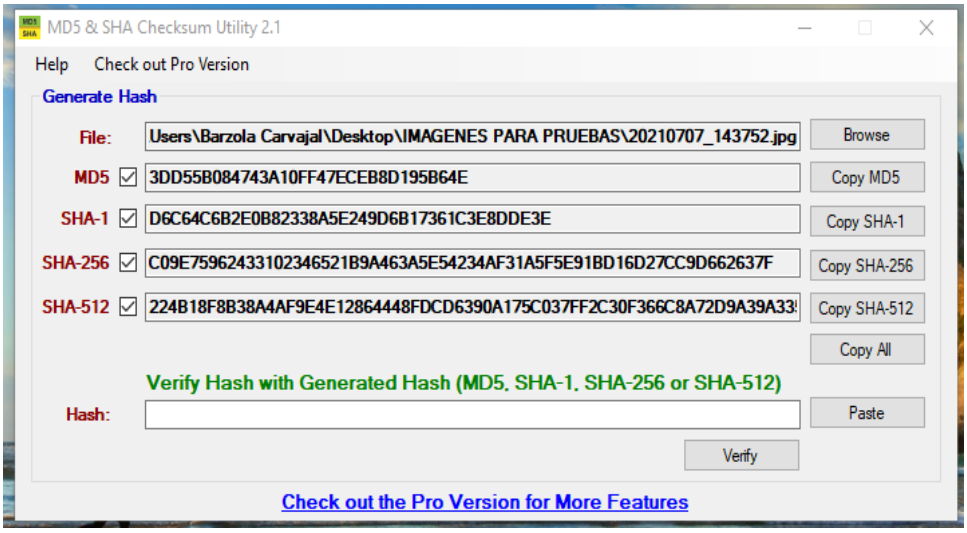

Figura 27 *MD5 & SHA Checksum Utility*

Anexo 3: Fase de Análisis

Se aplican herramientas y enfoques forenses como esteganografía, estegoanálisis y nivel de error ELA, que permitirán examinar la evidencia digital desde múltiples perspectivas, identificando posibles manipulaciones.

Para la realización de esta fase utilizaremos las herramientas OpenStego, SteganPEG, StegoSuite de Caine, stegsolve y StegHide de Kali Linux, FotoForensics, FOCA, MD5 SHA y Exiftool.

APLICANDO ESTEGANOGRAFÍA A LAS IMÁGENES

- **Esteganografía a imagen con formato jpg:**

Esteganografía a través de líneas de comando Windows. Para la realización de la esteganografía se tomará una imagen original la cual se manipulará; a esta imagen se le copiará un archivo .docx y como resultado se obtendrá una imagen con formato .png, además se deberá realizar la respectiva generación del hash de la imagen antes y después de ser manipulada como se muestra a continuación:

Hash de la imagen original: 3DD55B084743A10FF47ECEB8D195B64E

Metada de la imagen original: Tomada de la herramienta FOCA.

Exif Makernote:	
Anchura de la imagen en miniatura	512 pixels
Altura de la imagen en miniatura	384 pixels
Marca	samsung
Modelo	SM-A325M
Orientación	Top, left side (Horizontal / normal)
Resolución X	72 dots per inches
Resolución Y	72 dots per inches
Resolución Unidad	Inches
Software	A325MUBU1AUD2
Fecha/Hora	2021:07:07 14:37:52
Posicionamiento YCbCr	Center of pixel array
Tiempo de exposición	1/49 sec
Número F	F 1,8
Programa de exposición	Program normal
Velocidad ISO	8000
Versión Exif	2.20
Fecha/Hora Original	2021:07:07 14:37:52
Fecha/Hora Digitalizada	2021:07:07 14:37:52
Velocidad de obturación	1 sec
Valor de apertura	F 1,8
Valor de luminosidad	742/50

Valor de sesgo de exposición	0
Valor de apertura máxima	F 1,8
Modo de medición	Center weighted average
Flash	Flash did not fire
Distancia focal	4,6 mm
Espacio de color	sRGB
Anchura de imagen Exif	4624 pixels
Altura de imagen Exif	3468 pixels
Modo de exposición	Auto exposure
Modo de balance de blancos	Auto white balance
Relación de zoom digital	1
Longitud focal en película de 35 mm	25 mm
Tipo de Captura de Escena	Standard
Compresión	JPEG (old-style)
Desplazamiento de miniaturas	778 bytes
Longitud de la miniatura	49966 bytes
Datos en miniatura	[49966 bytes of thumbnail data]
Miniatura	
Imagen	
	

Tabla 7 *Metadata de la imagen con formato jpg***.**

En el equipo Windows se ejecutará en modo administrador la línea de comandos CMD donde ubicaremos la ruta que contiene la imagen.jpg y el archivo.doc. Se ejecuta la instrucción cd Prueba. Luego, la instrucción **copy /v /B 20210707_143752.jpg+encuesta.docx resultado.png** esta instrucción indica que copiará el archivo **encuesta.docx** dentro de la imagen **20210707_143752.jpg** y la imagen con el resultado final se llamará **resultado.png** como se muestra a continuación.

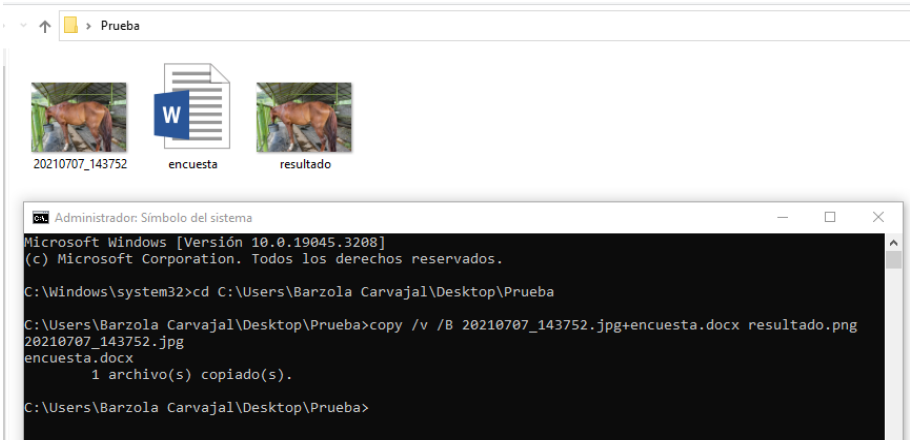

Figura 28 Cmd Windows

En la siguiente imagen se muestra el hash de la imagen original antes de ser manipulada y el hash de la imagen que ha sido modificada.

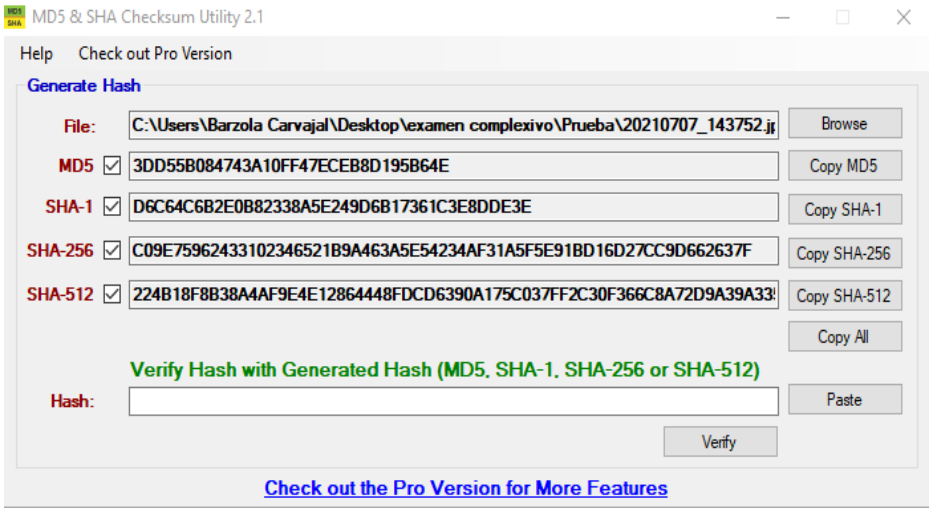

Figura 29 *Hash de la imagen editada*

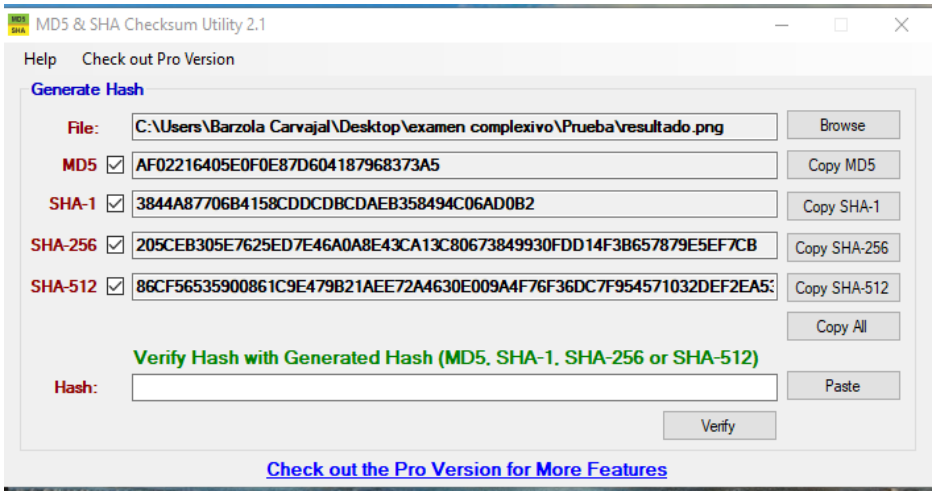

Figura 30 *Hash de la imagen original*

Figura 31 *Metada de Imagen con esteganografía*

Esteganografía con la herramienta Stegosuite de CAINE. Antes de la realizacion de la esteganografía a la imagen se debe relizar la respectiva generación del hash de la imagen antes de ser manipulada y luego realizar el mismo proceso cuando la imagen halla siso incrustada como se muestra a continuación. Para la ejecución del hash de la imagen se emplea la herramienta QuickHash v3.1.0 de Caine.

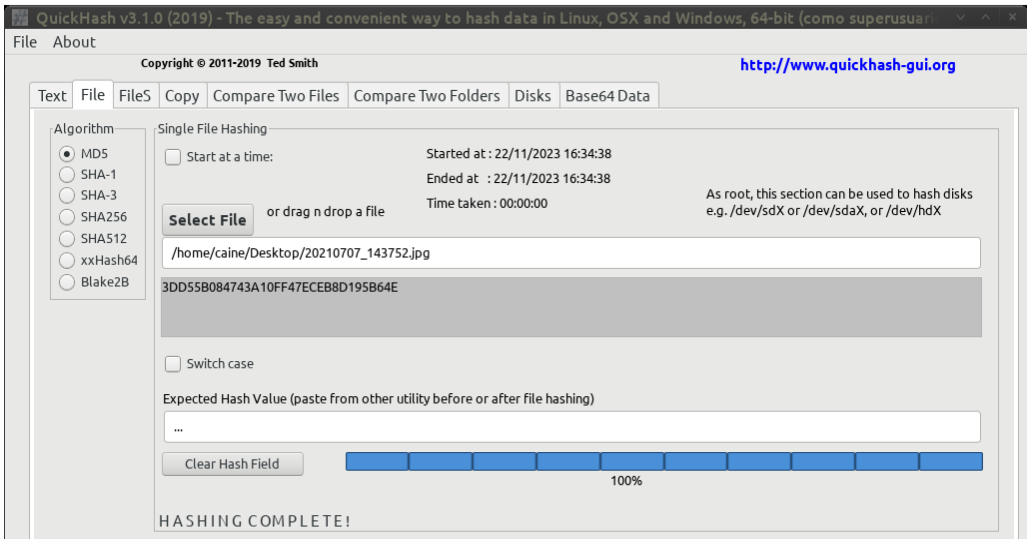

Figura 32 Hash de la imagen original

En la siguiente gráfica se muestra la metadata de la imagen original desde FotoForensics y propiedades de la imagen.

File	
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Exif Byte Order	Little-endian (Intel, II)
Image Width	4624
Image Height	3468
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)

EXIF	
Make	samsung
Camera Model Name	SM-A325M
Orientation	Horizontal (normal)
X Resolution	72
Y Resolution	72
Resolution Unit	inches
Software	A325MUBU1AUD2
Modify Date	2021:07:07 14:37:52
Y Cb Cr Positioning	Centered
Exposure Time	1/49
F Number	1.8
Exposure Program	Program AE
ISO	40
Exif Version	0220
Date/Time Original	2021:07:07 14:37:52
Create Date	2021:07:07 14:37:52
Offset Time	-05:00
Offset Time Original	-05:00
Shutter Speed Value	1

Figura 33 *Metadata de la imagen original tomada desde FotoForensics*

Aperture Value	1.8
Brightness Value	14.84
Exposure Compensation	0
Max Aperture Value	1.8
Metering Mode	Center-weighted average
Flash	No Flash
Focal Length	4.6 mm
Color Space	sRGB
Exif Image Width	4624
Exif Image Height	3468
Exposure Mode	Auto
White Balance	Auto
Digital Zoom Ratio	1
Focal Length In 35mm Format	25 mm
Scene Capture Type	Standard
Compression	JPEG (old-style)
Thumbnail Offset	790
MakerNotes	
Time Stamp	2021:07:07 19:37:52.627+00:00
MCC Data	Ecuador (740)
Composite	
Aperture	1.8
Shutter Speed	1/49
Date/Time Original	2021:07:07 14:37:52-05:00
Modify Date	2021:07:07 14:37:52-05:00
Image Size	4624x3468
Light Value	8.6
Megapixels	16.0
Scale Factor To 35 mm Equivalent	5.4
Circle Of Confusion	0.006 mm
Field Of View	71.5 deg
Focal Length	4.6 mm (35 mm equivalent: 25.0 mm)
Hyperfocal Distance	2.13 m

Figura 35 *Metadata de la imagen original tomada desde FotoForensics*

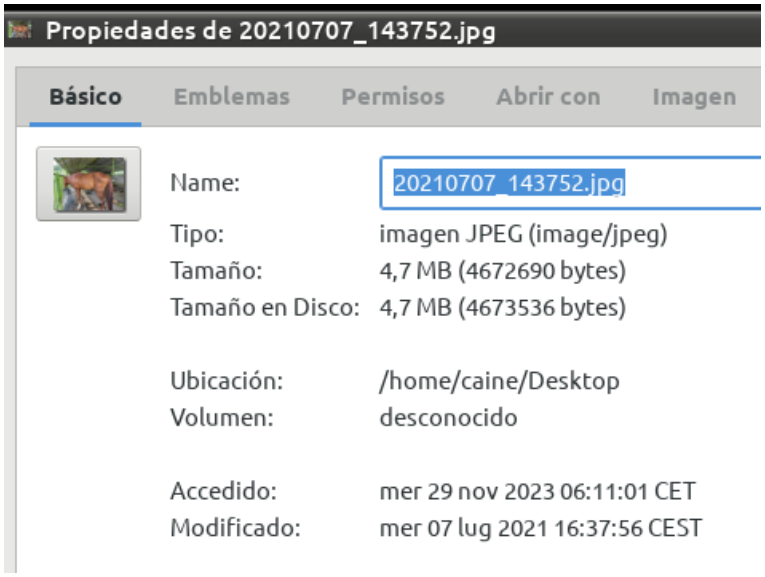

Figura 34 *Propiedades de la imagen original*

En el cuadro de texto se escribe un mensaje si se desea, se añade el archivo a embeber que en este caso es encuesta.docx y luego hacemos clic en Embed y esperamos que cargue.

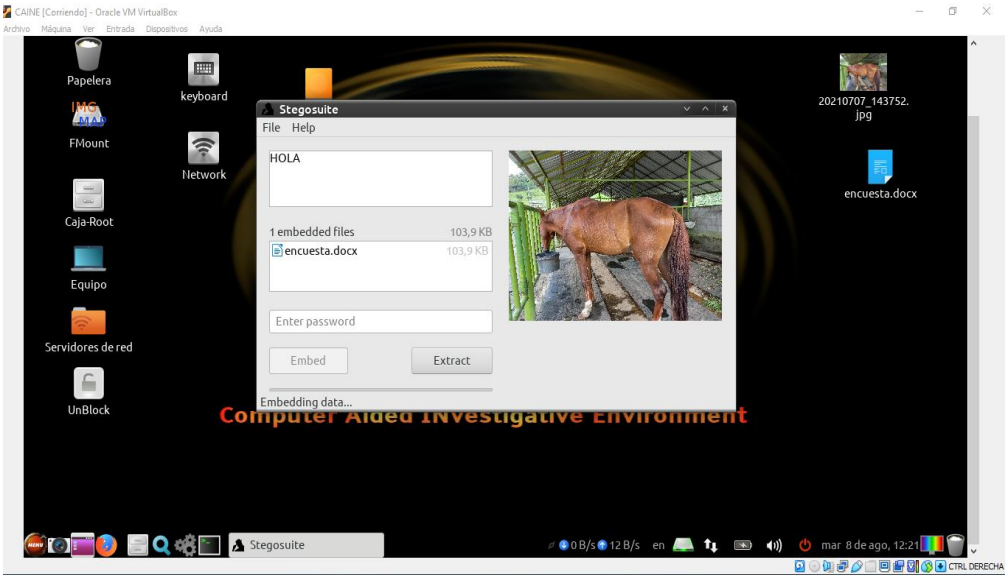

Figura 36 *Incrustando archivo*

Una vez finalizado el proceso se mostrará un mensaje Embedding completed como se muestra a continuación.

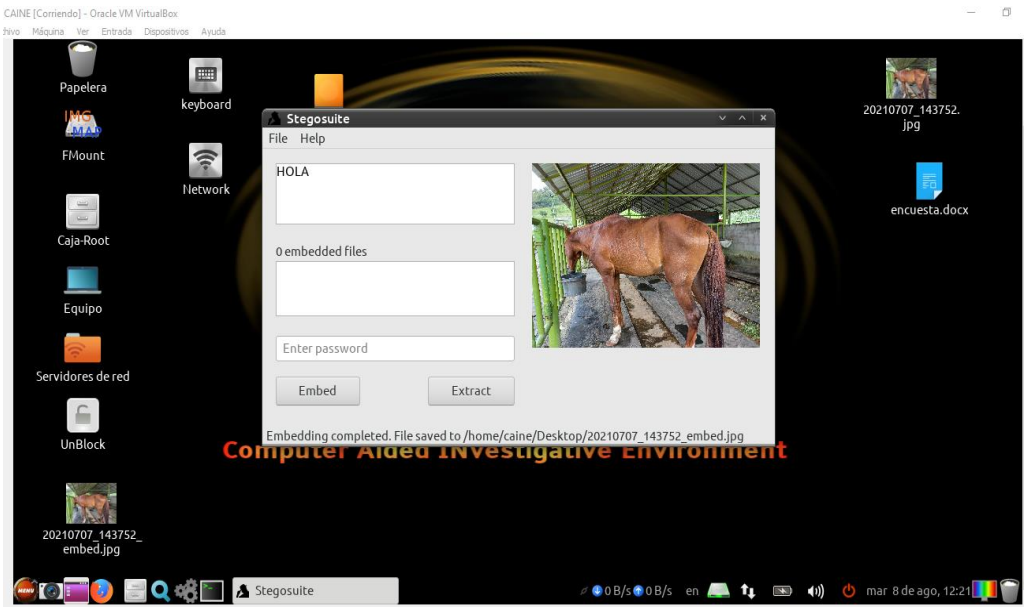

Figura 37 *Incrustación completada*

En la siguiente imagen se muestra el hash de la imagen incrustada.

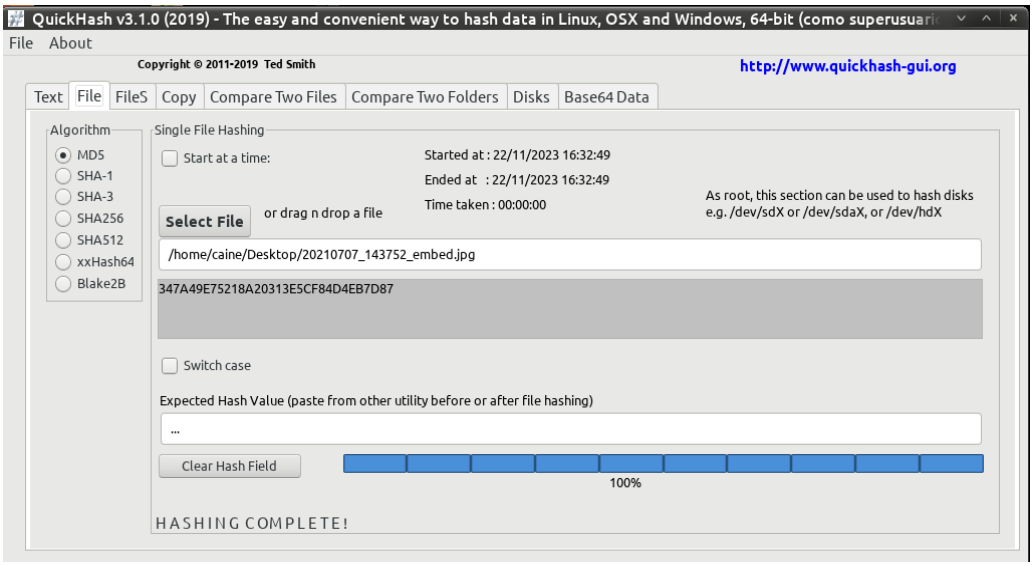

Figura 38 *Hash de la imagen incrustada*

Ahora se considera la opción contraseña que ofrece la herramienta para embeber el archivo a la imagen original.

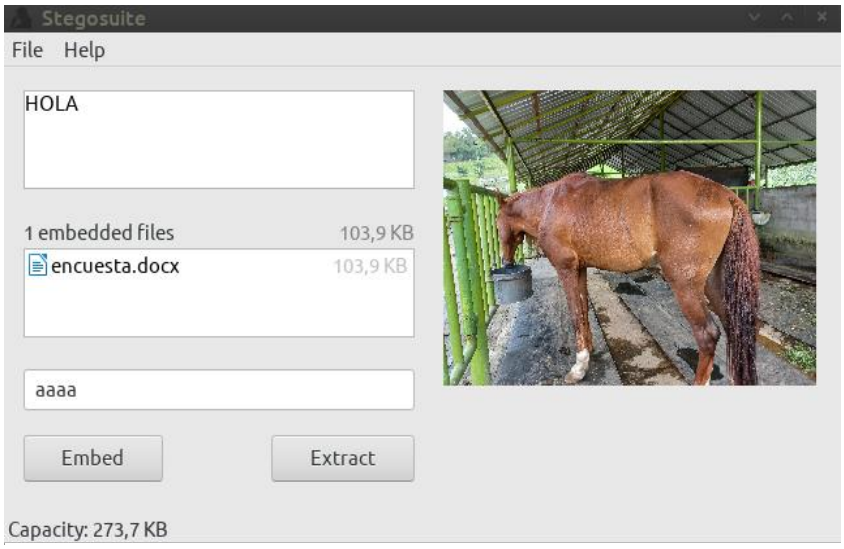

Figura 39 *Imagen con contraseña*

En la siguiente gráfica se muestra la incrustación del archivo encuesta.docx a la imagen original a diferencia del paso anterior ingresamos una contraseña.

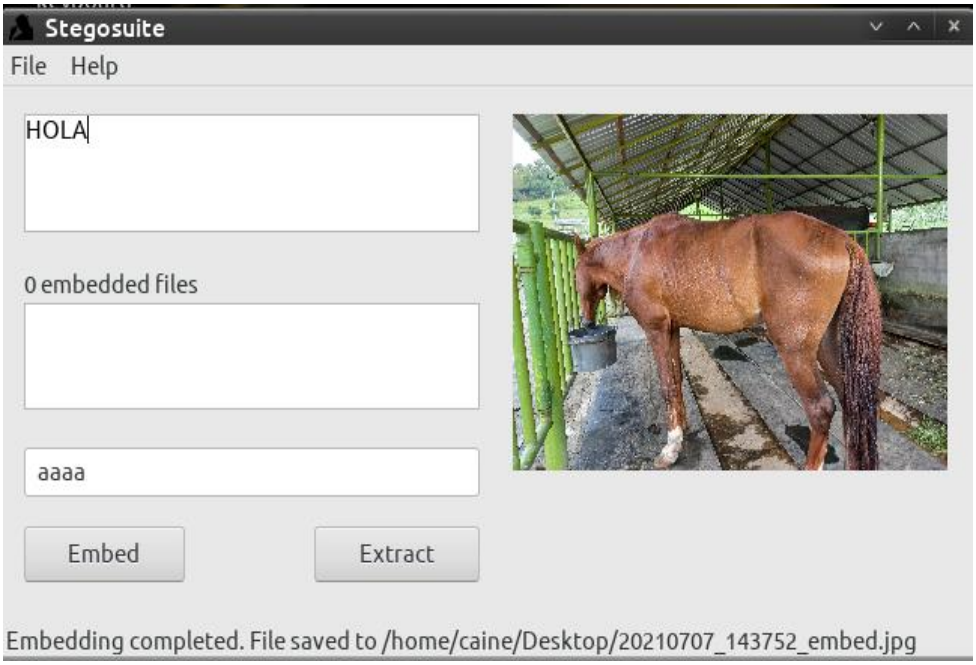

Figura 40 *Incrustación completa*

A continuación, se muestra la metadata de la imagen incrustada con contraseña mediante FotoForensics y propiedades de la imagen.

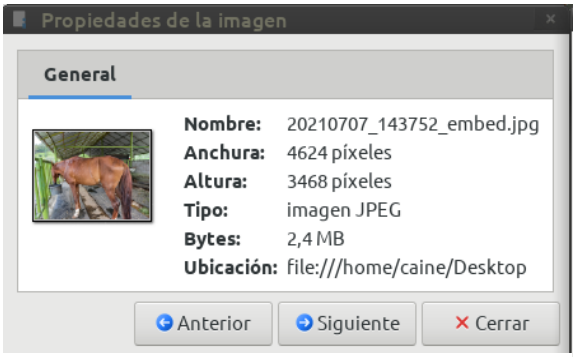

Figura 41 *Propiedades de la imagen incrustada*

File	
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Comment	JPEG Encoder Copyright 1998, James R. Weeks and BioElectroMech.
Image Width	4624
Image Height	3468
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)

JFIF	
JFIF Version	1.00
Resolution Unit	None
X Resolution	1
Y Resolution	1

Composite	
Image Size	4624x3468
Megapixels	16.0

Figura 42 *Metadata de la imagen incrustada utilizando FotoForensics*

Información hexadecimal del contenido de la imagen jpg mediante la herramienta WinHex.

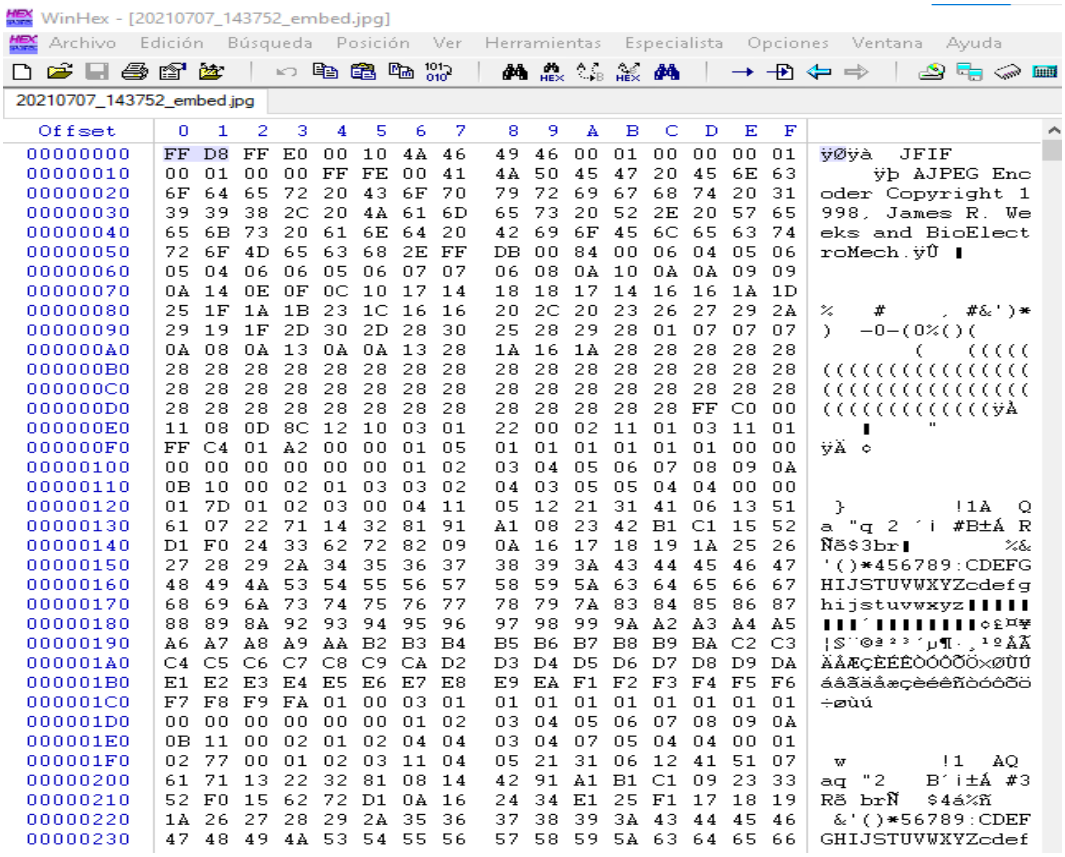

Figura 43 *Información extraída de WinHex*

Esteganografía con la herramienta Steghide de Kali Linux. Se ingresa a la Shell de Kali y se crea un archivo de texto plano .txt con el mensaje a ocultar como se muestra a continuación en el escritorio de kali:

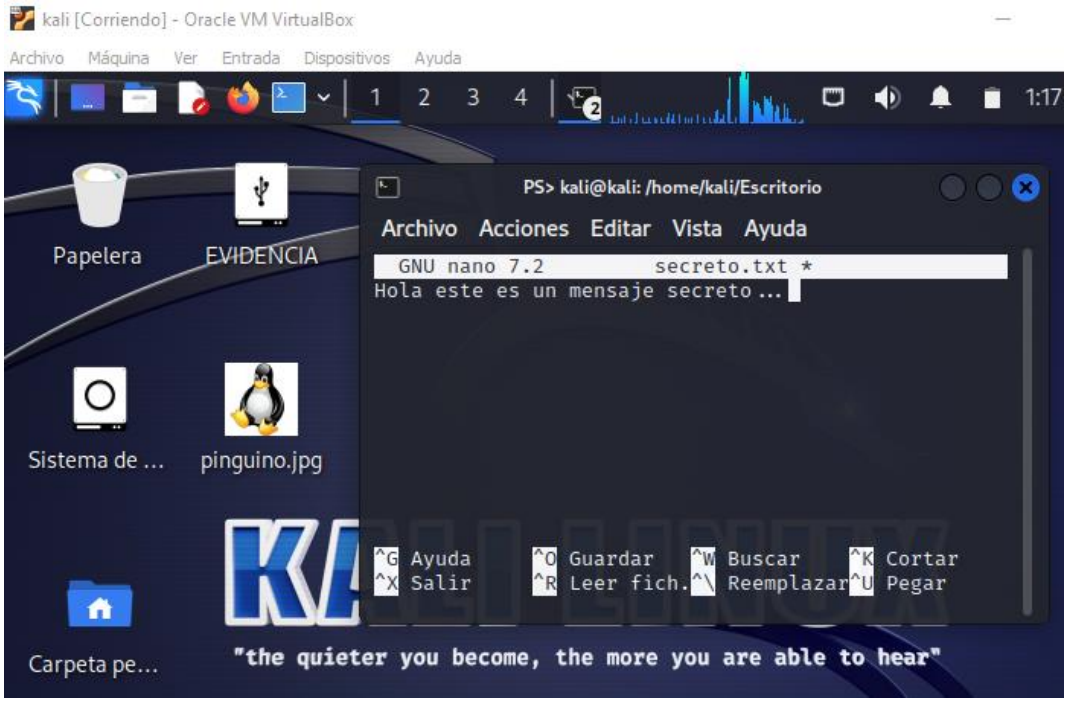

Figura 44 *Creación de texto plano*

Con la siguiente línea de comando **steghide embed -ef secreto.txt -cf pingüino.jpg -sf imagen_con_secreto.jpg** se incrustará el archivo plano a la imagen jpg, una vez embebido se pide ingresar contraseña, solo la persona q contenga la contraseña podrá abrir la imagen.

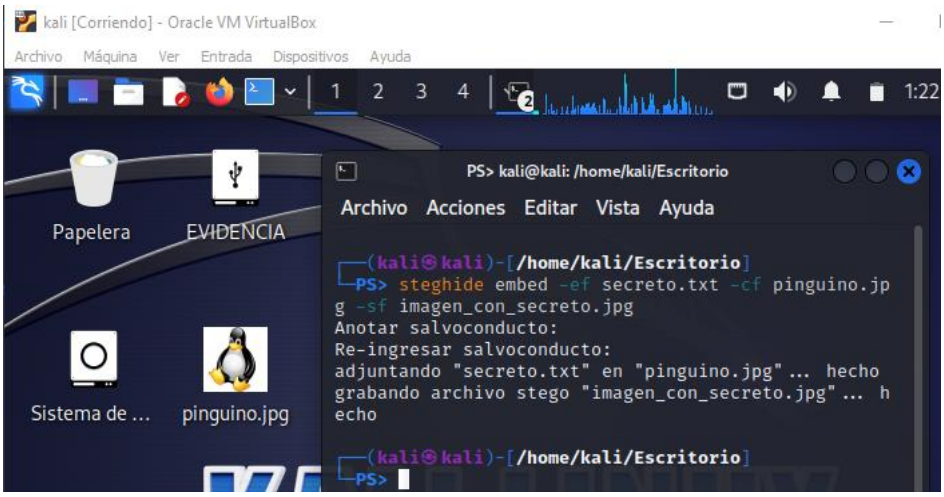

Figura 45 *Archivo .txt incrustado.*

Las siguientes imágenes muestran el Hash de la imagen original y el hash de la imagen incrustada.

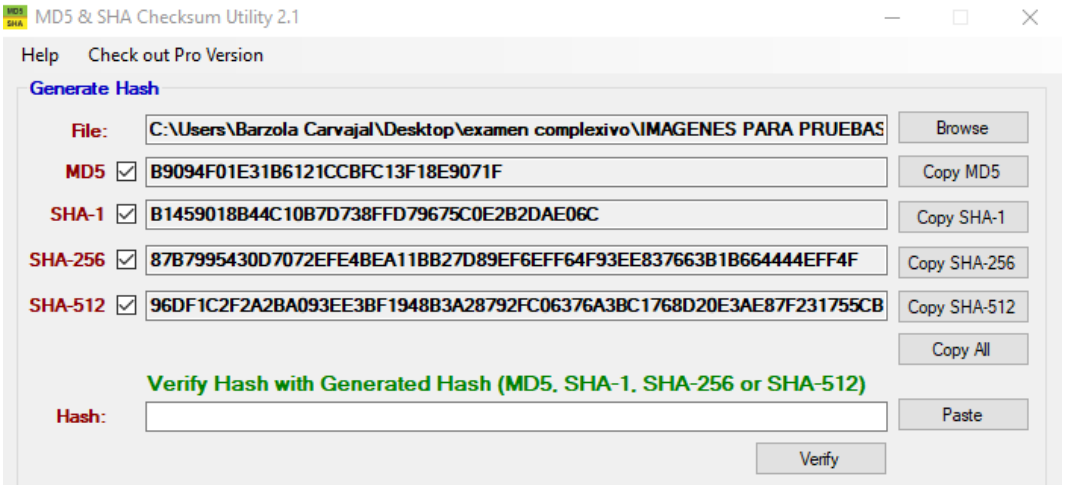

Figura 46 *Hash de la imagen incrustada*

- **Esteganografía con la herramienta SteganPEG:** se muestra el hash de la imagen antes de ser manipulada.

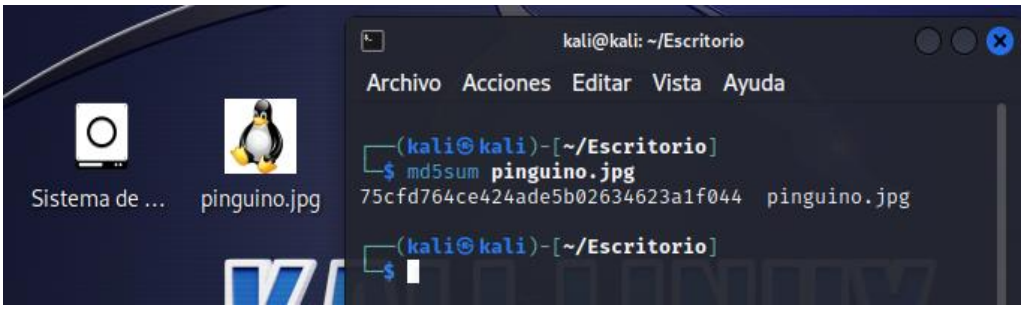

Figura 48 *Hash de la imagen original pingüino,jpg*

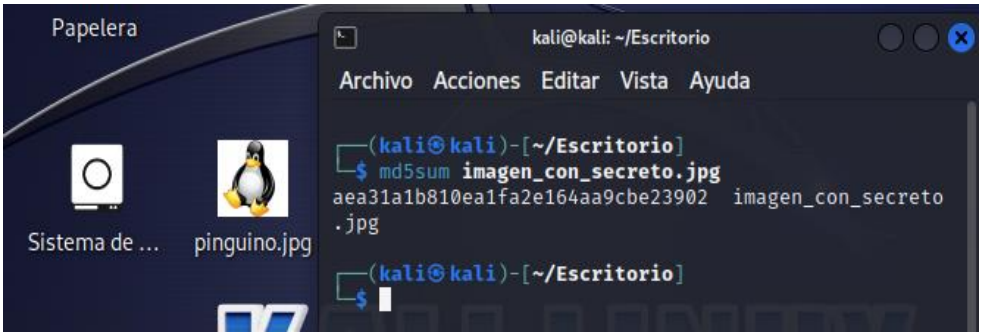

Figura 47 *Hash de la imagen incrustada imagen_con_secreto*

- **Metadata de la imagen original usando https://fotoforensics.com/**

Archivo	
Tipo de archivo	JPEG
Extensión de tipo de archivo	jpg
Tipo de Mimica	imagen/jpeg
Orden de bytes Exif	Little-endian (Intel, II)
ancho de la imagen	4000
Altura de imagen	2992
Proceso de codificación	DCT de referencia, codificación de Huffman
Bits por muestra	8
Componentes de color	3
Y Cb Cr Submuestreo	YCbCr4:2:0 (2 2)
EXIF	
Unidad de resolución	pulgadas
Descripción de la imagen	
Hacer	Xiaomi
Nombre del modelo de cámara	M2003J15SC
Software	Aplicación de cámara MediaTek
Orientación	Horizontales (normales)
Modificar fecha	2022:07:04 14:03:33
Posicionamiento Y Cb Cr	Coubicado
Índice de exposición recomendado	0
Tipo de sensibilidad	Desconocido
YO ASI	107
Programa de exposición	No definida
Número F	1.8
Tiempo de exposición	1/3300
Hora subseg. digitalizada	29
Tiempo subseg. Original	29
Tiempo subseg.	29

Longitud focal	4,7 milímetros
Destello	Apagado, no disparó
Fuente de luz	Otro
Modo de medición	Promedio ponderado al centro
Tipo de captura de escena	Estándar
Índice de interoperabilidad	R98 - Archivo básico DCF (sRGB)
Versión de interoperabilidad	0100
Distancia focal en formato de 35 mm	28mm
Fecha de Creación	2022:07:04 14:03:33
Compensación de exposición	0
Relación de zoom digital	1
Altura de la imagen Exif	2992
Balance de blancos	Auto
Fecha/Hora Original	2022:07:04 14:03:33
Valor de brillo	0
Ancho de imagen Exif	4000
Modo de exposición	Auto
Configuración de componentes	Y, Cb, Cr, -
Espacio de color	sRGB
Versión Exif	0220
Versión Flashpix	0100
ID de versión de GPS	2.2.0.0
Referencia de latitud GPS	Sur
Referencia de longitud GPS	Oeste
Referencia de altitud GPS	Sobre el nivel del mar
Marca de tiempo GPS	19:03:32
Método de procesamiento GPS	GPS
Sello de fecha GPS	2022:07:04
Resolución X	72
Resolución Y	72
Desplazamiento de miniaturas	4038

Longitud de la miniatura	49792
Compresión	JPEG (estilo antiguo)
Imagen en miniatura	(Datos binarios 49792 bytes)
Compuesto	
Abertura	1.8
Velocidad de obturación	1/3300
Fecha de Creación	2022:07:04 14:03:33.29
Fecha/Hora Original	2022:07:04 14:03:33.29
Modificar fecha	2022:07:04 14:03:33.29
Altitud GPS	25 m sobre el nivel del mar
Fecha/Hora GPS	2022:07:04 19:03:32Z
Latitud GPS	2 grados 11' 32,74" S
Longitud GPS	79 grados 52' 44.31" W
Posición GPS	2 grados 11' 32,74" S, 79 grados 52' 44,31" W
Tamaño de la imagen	4000x2992
Valor de luz	13.3
Megapíxeles	12.0
Factor de escala equivalente a 35 mm	5.9
Círculo de confusión	0,005 milímetros
Campo de visión	65,5 grados
Longitud focal	4,7 mm (equivalente a 35 mm: 28,0 mm)
Distancia hiperfocal	2,47 metros
Ubicación GPS aproximada	
Esta información se interpreta a partir de los metadatos del GPS. **Las ubicaciones son aproximadas.** Aunque las coordenadas parecen precisas, los dispositivos móviles suelen tener poca precisión.	
Coordenadas aproximadas	-2.192428,-79.878975
Ubicación aproximada	Guayaquil, CE
Rango aproximado	No especificado; supongamos +/- 3218 metros (2 millas)

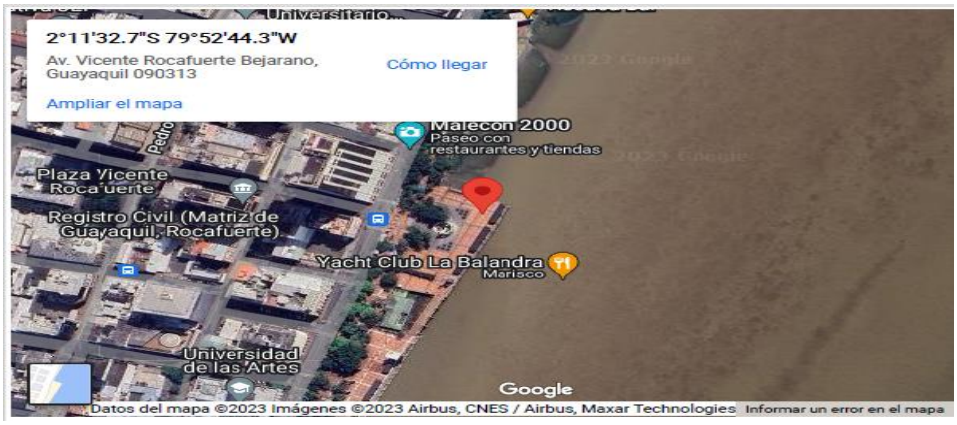

Tabla 8 *Datos de la Metadata de la imagen*

En la pantalla principal de SteganPEG se selecciona embed ya que se va a embeber archivos a la imagen, se agrega password a la imagen y se llena el campo donde se encuentra la ruta de la imagen a incrustar.

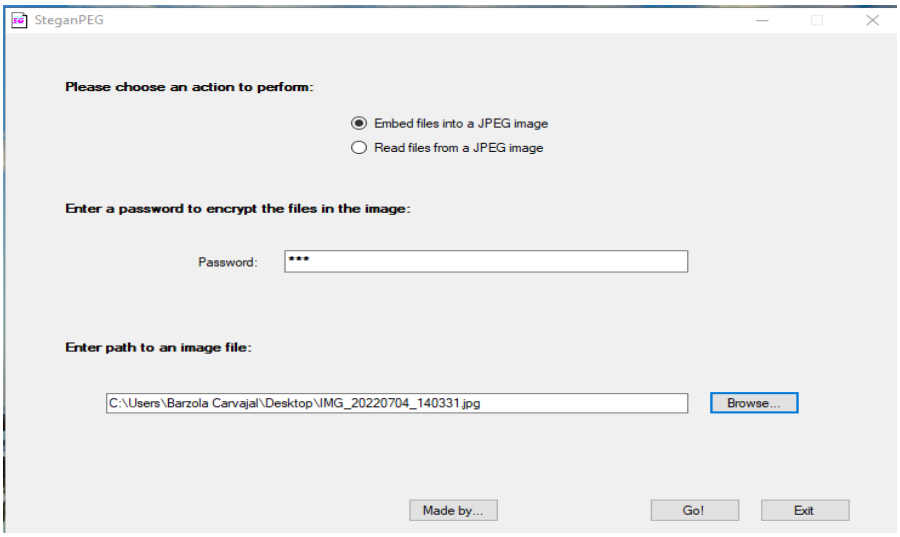

Figura 49 *Pantalla principal de SteganPEG*

En la siguiente grafica se muestra la barra de estado de la imagen indicando así el espacio disponible para seguir añadiendo archivos a la imagen, una vez cargado todos los archivos se procede con la carga.

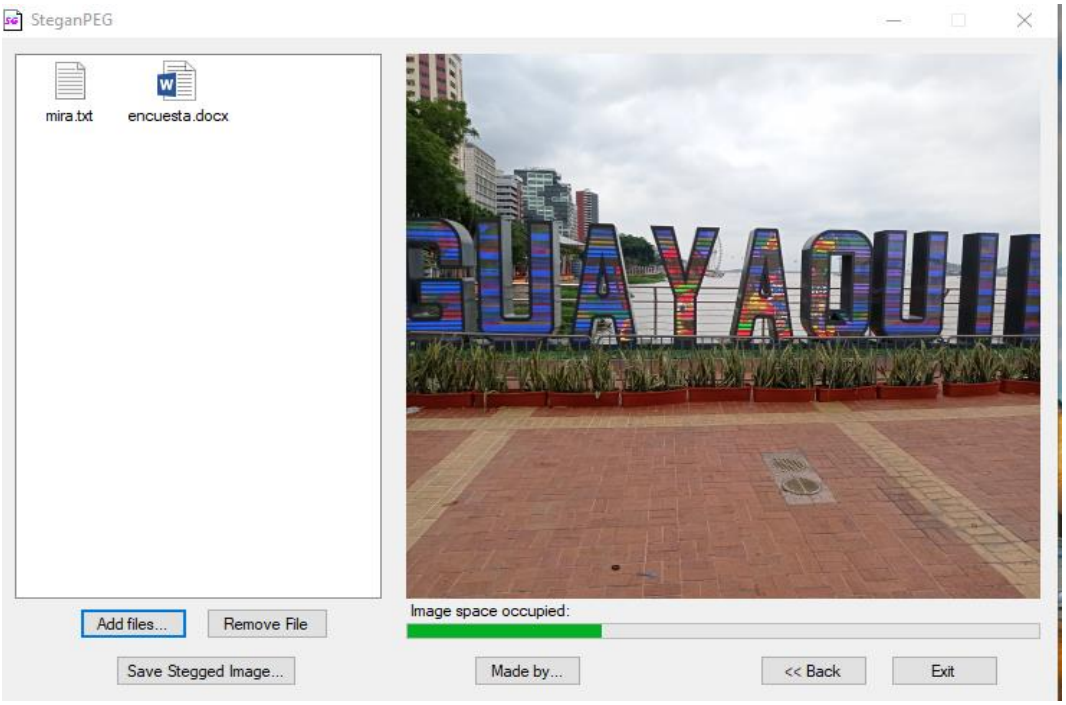

Figura 51 *Esteganografía a imagen jpg*

Antes de eso se debe colocar la ruta donde se guardará la nueva imagen y el proceso esteganográfico termina.

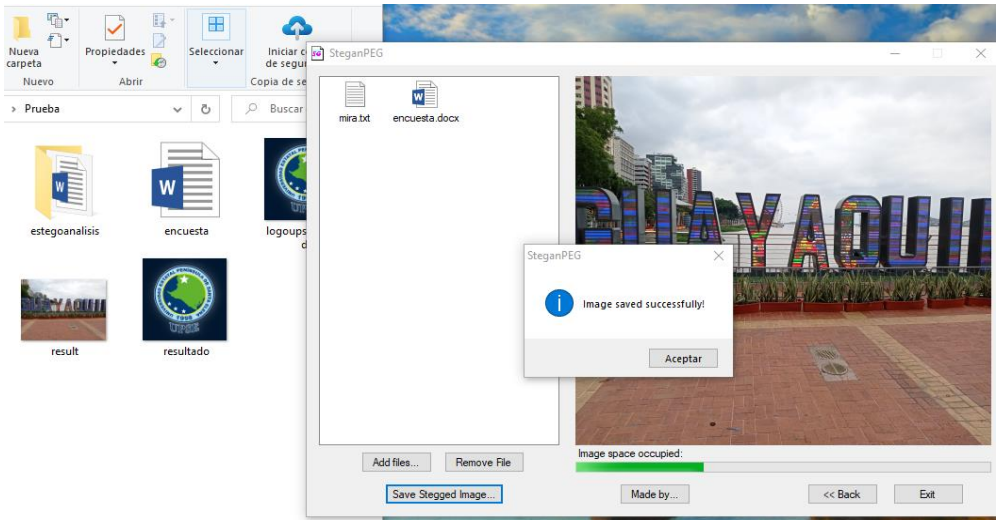

Figura 50 *Imagen guardada*

En la siguiente grafica se muestra el Hash de la imagen incrustada.

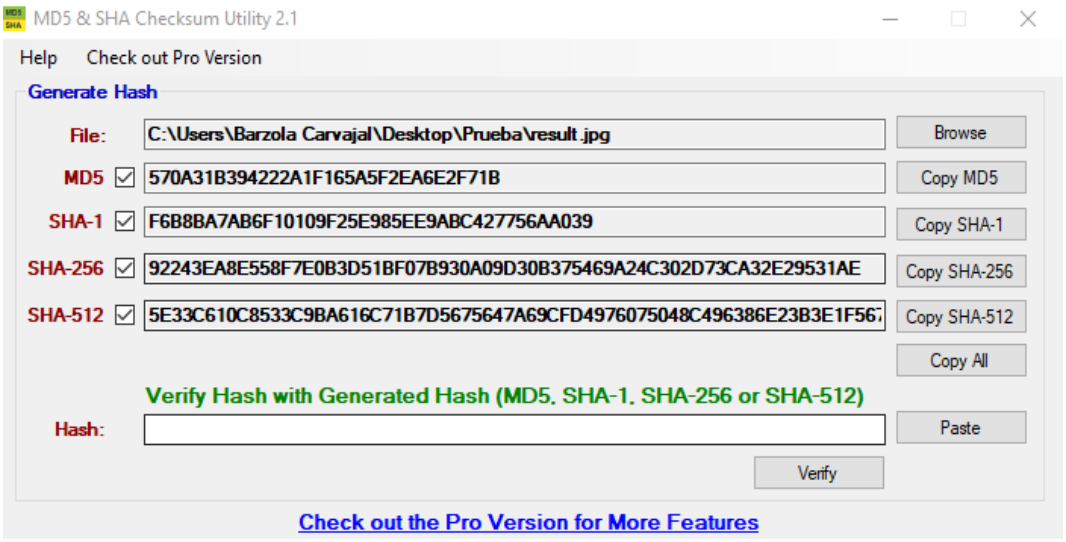

Figura 52 *Hash de la imagen incrustada*

- **Esteganografía a imagen con formato png:**

Esteganografía a través de líneas de comando Windows. Se tomará una imagen con formato png para la realización de la esteganografía, se incrustará un archivo .docx y como resultado de aquello se obtendrá una imagen con el mismo formato .png, además se deberá realizar la respectiva generación del hash de la imagen antes y después de ser manipulada como se muestra a continuación:

- **Hash de la imagen original**: 8FC5D1F649429B5DD32F6FFED0072441

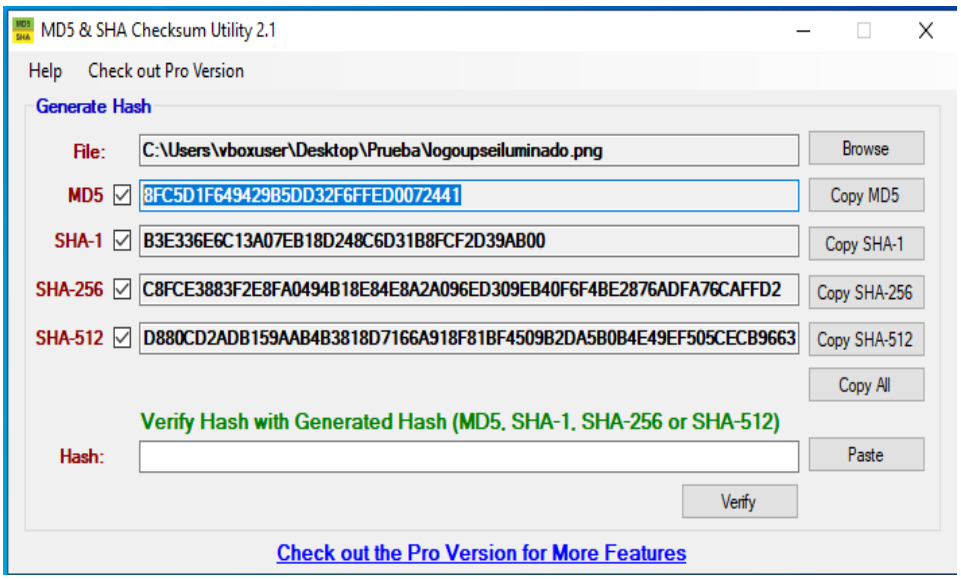

Figura 53 *Hash de la imagen*

- **Metadata de la imagen original:** Fuente tomada de la herramienta FOCA.

	
Archivo	
Nombre:	**logoupseiluminadoE.png**
Tipo de elemento:	Archivo PNG
Ruta de acceso a la carpeta:	C:\Users\Barzola Carvajal\Desktop\IMAGENES PARA PRUEBAS
Fecha de creación:	19/7/2023 20:56
Fecha de modificación:	19/7/2023 20:58
Tamaño:	324 MB
Atributos:	A
Hash:	8FC5D1F649429B5DD32F6FFED0072441
Propietario:	DESKTOP
Equipo:	DESKTOP
Origen	
Fecha de captura	-
Nombre del programa:	-
Imagen	
Id de imagen:	-
Dimensiones:	930x944
Ancho:	930 pixeles
Alto:	944 pixeles
Resolución H/V	-
Profundidad en bits:	32
Unidad de resolución:	-
Representación del color:	-
Cámara	
Fabricante:	-
Modelo:	-
Punto F:	-
Tiempo de exposición:	-
Velocidad ISO:	-
Compensación de exposición:	-
Distancia focal:	-
Apertura máx	-

Modo de medición:	-
Modelo de flash:	-
Long focal de 35 mm:	-
Fotografía avanzada	
Brillo:	-
Programación de exposición:	-
Balance de Blanco:	-
Zoom digital:	-
Versión EXIF:	-

Tabla 9 *Metadata de la imagen con formato png*

En Windows se ejecutará en modo administrador la línea de comandos CMD donde ubicaremos la ruta que contiene la imagen.png y el archivo.doc. Se ejecuta la instrucción cd Prueba. Luego, la instrucción **copy /v /B logoupseiluminado.png+encuesta.docx resultado.png** esta instrucción indica que copiará el archivo **encuesta.docx** dentro de la imagen **logoupseiluminado.png** y la imagen con el resultado final se llamará **resultado.png** como se muestra a continuación.

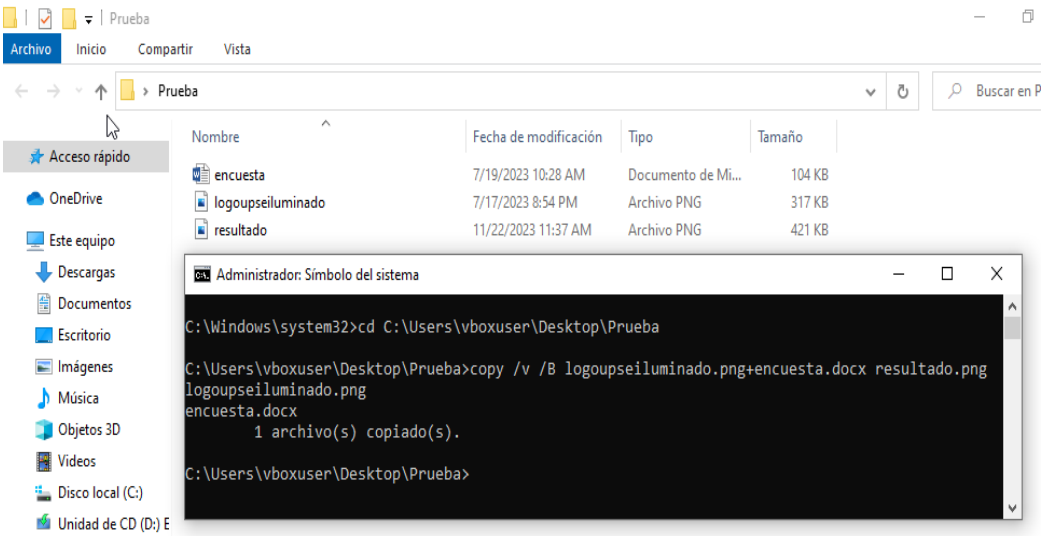

Figura 54 *Incrustación a la imagen con formato png*

En la siguiente imagen se muestra el hash de la imagen incrustada.

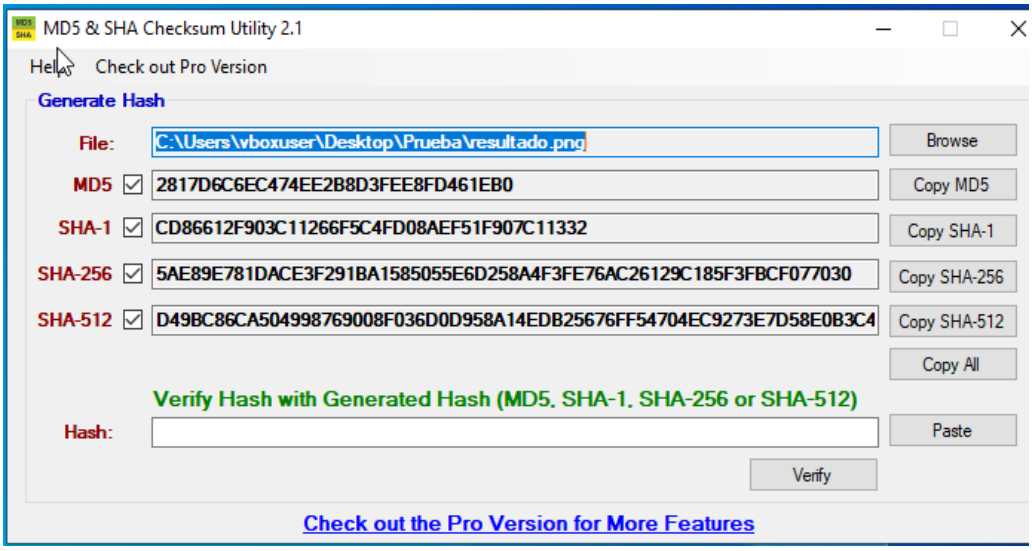

Figura 56 *Imagen incrustada*

– **Esteganografía con la herramienta OpenStego:** En el cuadro de dialogo que se muestra en la imagen se llenan los campos, se elige el archivo encuesta.docx que será el archivo a incrustar, se selecciona la ruta donde se encuentra la imagen original para que sea embebida y como imagen de salida se deberá colocar un nombre y la ruta donde se desee guardar dicha imagen además, se pide que se llene el campo de password que será de suma importancia para la extracción del archivo.

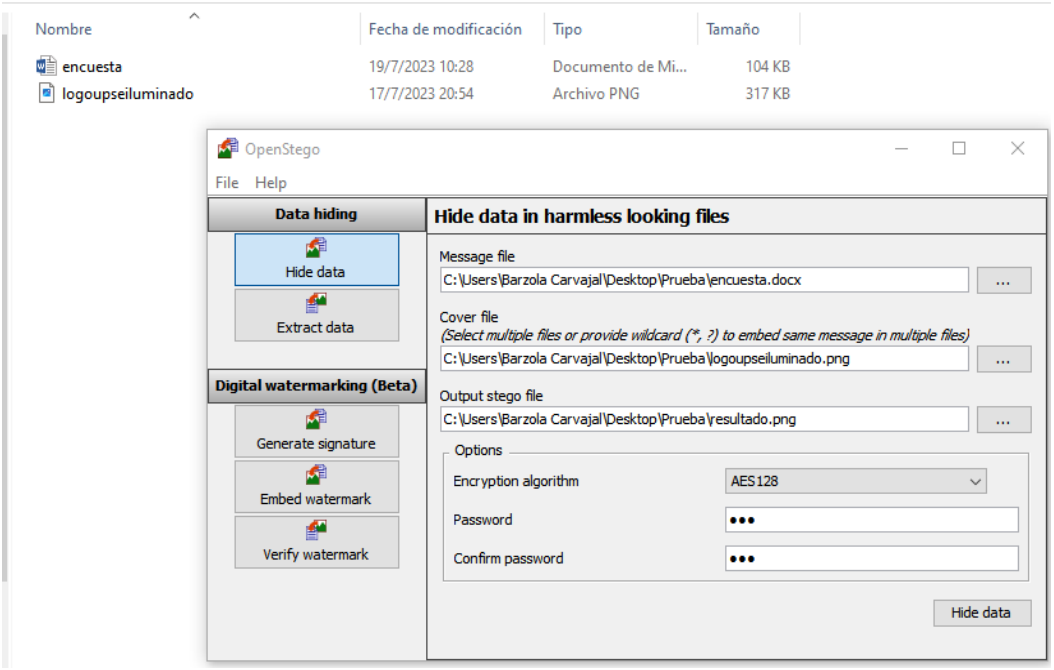

Figura 55 *Esteganografía con OpenStego*

Al hacer clic en Hide data empieza el proceso de incrustación a la imagen, una vez terminada la ejecución se muestra un mensaje como se muestra en la gráfica.

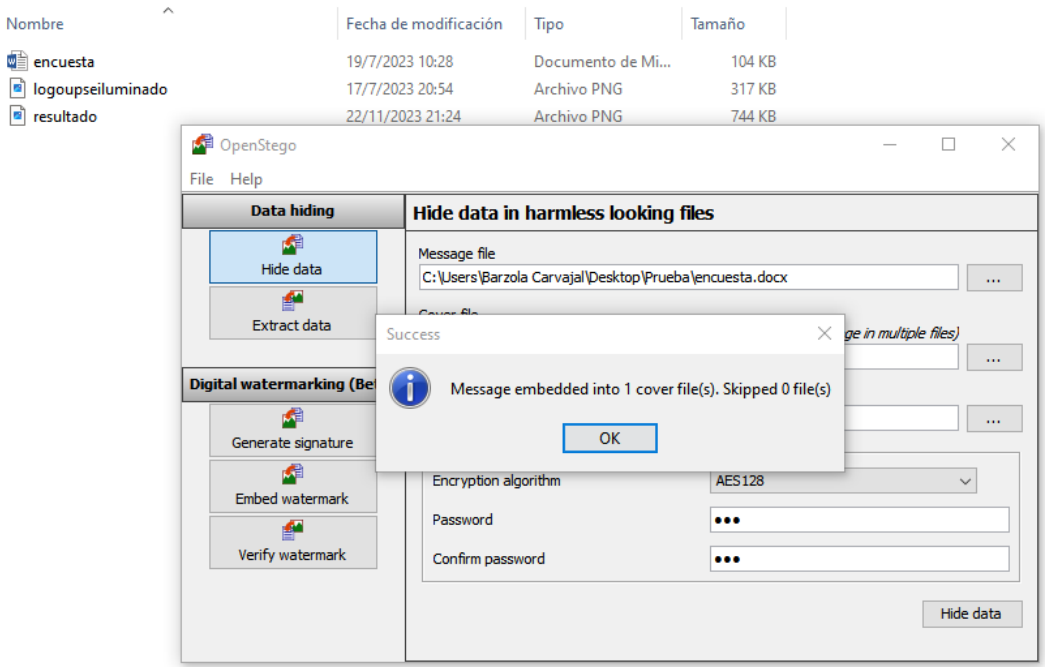

Figura 57 *Proceso de incrustación terminado*

En la siguiente gráfica se muestran los resultados con el archivo ya embebido.

Figura 58 *Resultado de la esteganogrfía*

APLICANDO ESTEGOANÁLISIS A LAS IMÁGENES

Estegoanálisis a imagen con formato png: Se tomará una imagen anteriormente editada para detectar los mensajes o los archivos ocultos por la esteganografía. Con la herramienta OpenStego se extraerá la información embebida de la imagen para ello se debe llenar los campos del archivo a analizar y colocar la ruta de la carpeta donde se desee guardar los archivos detectados por la herramienta, además de agregar la contraseña que debe ser la misma que se proporcionó a la hora de hacer la esteganografía en el paso Hidedata como se muestra en la gráfica.

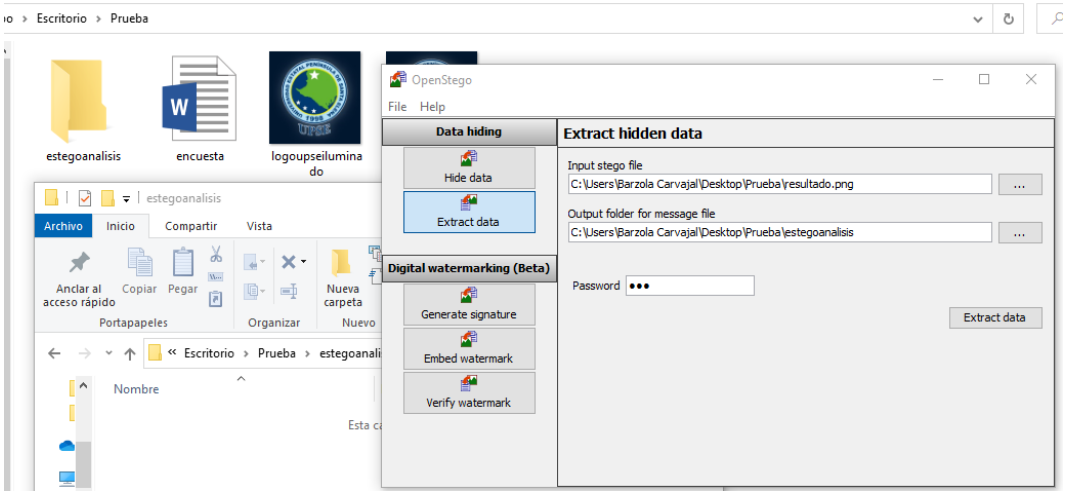

Figura 60 *Proceso de extracción de archivos*

Una vez llenado todos los campos comienza el proceso de extracción, y en la ruta que seleccionamos se guardará el archivo oculto en la imagen como se muestra en la siguiente gráfica.

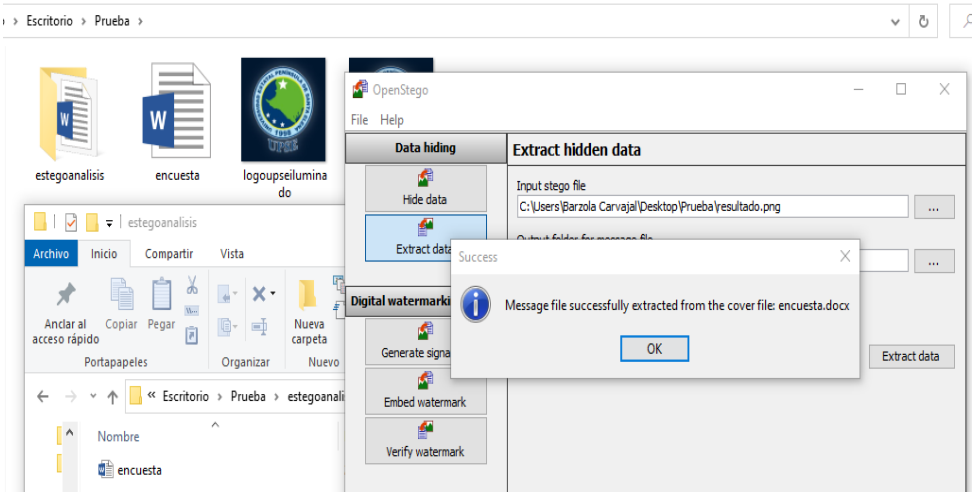

Figura 59 *Proceso de extracción resultado.png*

Estegoanálisis a imagen con formato jpg: En Kali Linux con la herramienta steghide realizamos el estegoanalisis de la imagen como se muestra en la gráfica digitando la contraseña para la extracción del archivo embebido

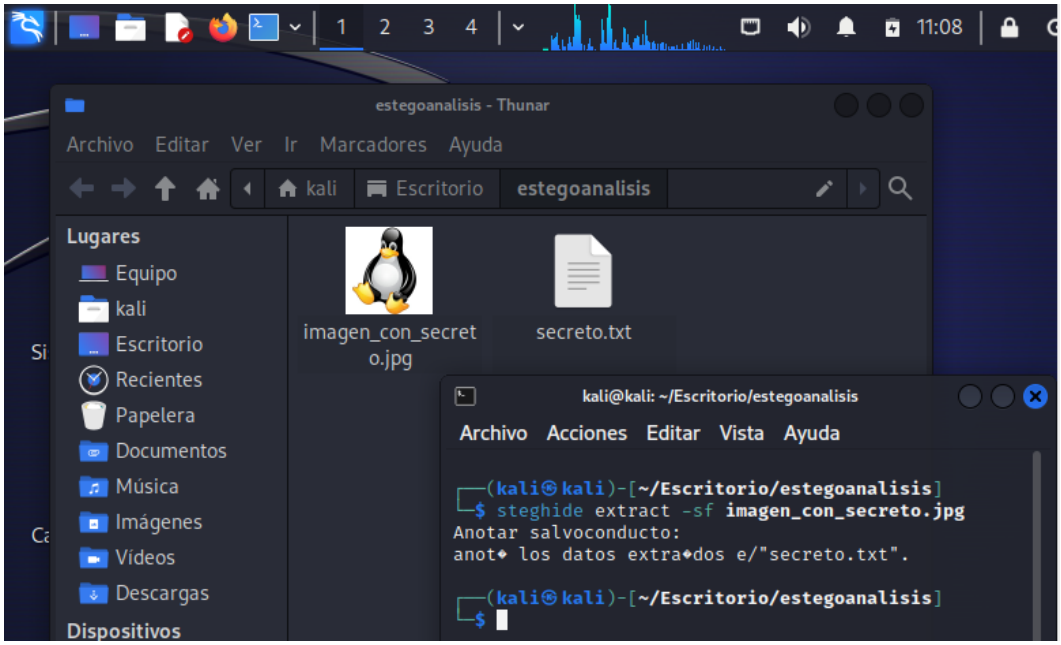

Figura 62 *Extracción de datos*

Como otro ejemplo podemos mencionar la herramienta SteganPEG se procede a la extracción de los archivos embebidos a la imagen, seleccionando la opción Read files from a JPGE image y añadiendo el password como se muestra a continuación.

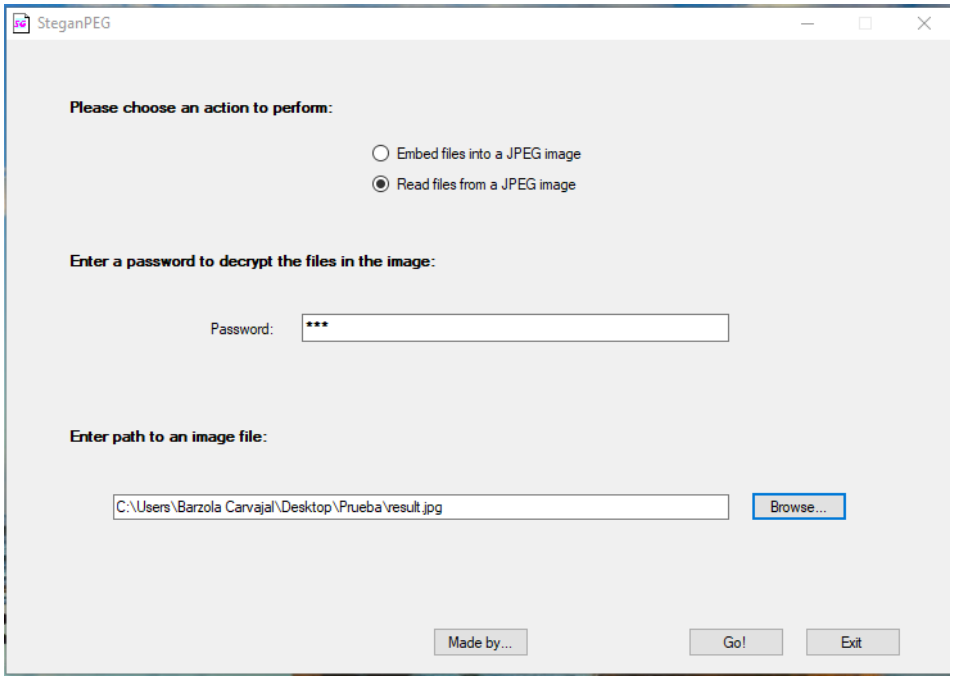

Figura 61 *Proceso de extracción de archivos*

Y automáticamente se visualizan los archivos incrustados como se muestra en la gráfica.

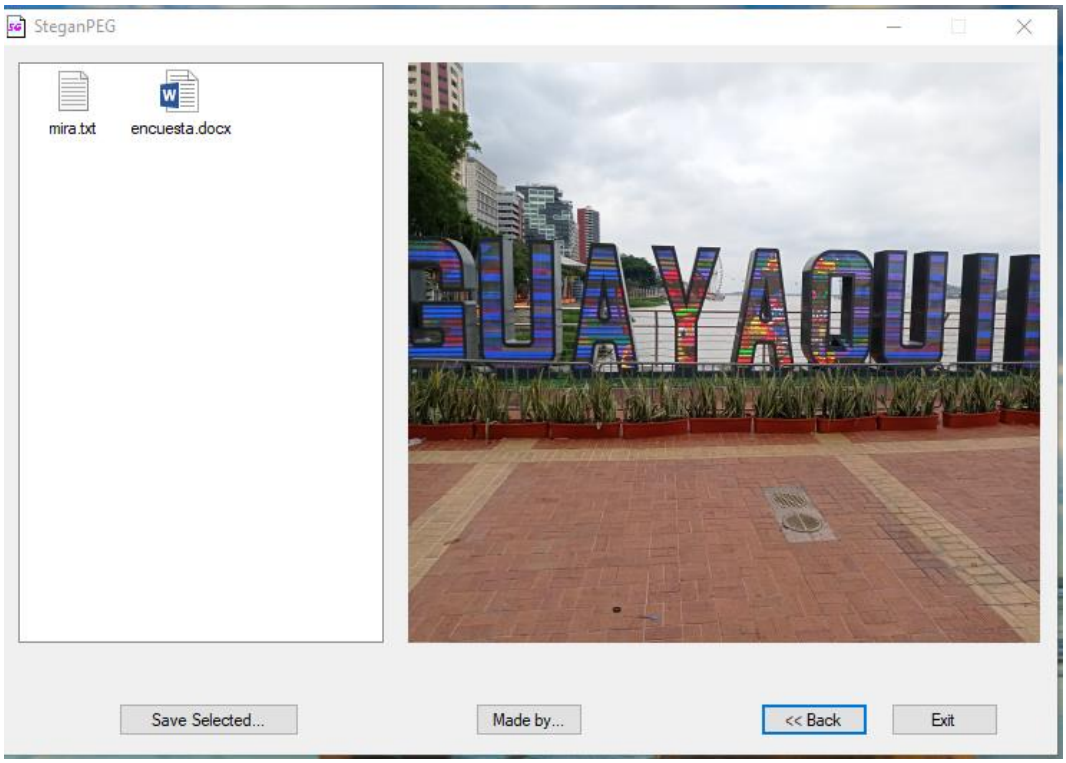

Figura 63 *Extracción de archivos completada*

APLICANDO NIVEL DE ERROR ELA

El análisis de nivel de error (ELA) permite identificar áreas dentro de una imagen que se encuentran en diferentes niveles de compresión. Con las imágenes JPEG, la imagen completa debe estar aproximadamente al mismo nivel.

Cuando se realiza el análisis de error ELA, se compara el nivel de error en diferentes secciones de la imagen. Si una sección de la imagen muestra un nivel de error significativamente diferente en comparación con el resto de la imagen, es una indicación de que esa sección podría haber sido modificada o editada digitalmente.

Se muestra la imagen original y la imagen editada para realizar el análisis de nivel de error ELA.

Figura 65 *Imagen Original*

Figura 64 *Imagen Editada*

Para realizar el análisis de nivel de error ELA ingresamos a https://fotoforensics.com/ que es una herramienta en línea que implementa un algoritmo ELA. Al usarlo, es posible descubrir rápidamente la manipulación de imágenes. La técnica ELA compara los diferentes niveles de error que contienen las regiones de una imagen lo que hace posible identificar áreas donde se ha realizado una edición o donde se ha agregado o quitado elementos de la imagen.

Al aplicar la técnica de error ELA a la imagen original, se podrán observar diferencias en los niveles de error entre el pasto y las áreas donde se encuentran los bigotes del perro. Los cambios en la edición del pasto y los bigotes podrán manifestarse como áreas con niveles de error más altos en comparación con las regiones inalteradas.

Figura 66 *Imagen con ELA*

La edición en el pasto puede mostrar un incremento en los niveles de error en las áreas editadas, en comparación con el pasto original que no ha sido modificado. La diferencia en la textura, el color y los detalles del pasto editado podría resultar en una variación en los niveles de error.

De manera similar, los bigotes del perro que han sido editados mostrarán una discrepancia en los niveles de error en comparación con los bigotes originales. La edición en los bigotes, ya sea para agregar, quitar o alterarlos, generará diferencias notables en los niveles de error. Las áreas que muestran un contraste significativo en los niveles de error serán las zonas de interés donde se han llevado a cabo modificaciones.

Anexo 4: Fase de Documentación

INFORME TÉCNICO

Análisis de la integridad de imágenes usando métodos estegoanalíticos y análisis de nivel de error (ELA).

Introducción:

El análisis de la integridad de imágenes mediante métodos estegoanalíticos y el análisis de nivel de error (ELA) son enfoques que se utilizan para detectar posibles manipulaciones o incrustaciones de información oculta en una imagen.

En este proyecto se llevaron a cabo las 4 primeras fases de la metodología forense detalladas en los anexos 1,2,3 y 4, las técnicas empleadas fueron Esteganografía, Estegoanalisis y Análisis de Nivel de Error (ELA). Para la implementación de la parte práctica se utilizaron herramientas especializadas como OpenStego, SteganPEG, StegoSuite de Caine, stegsolve y StegHide de Kali Linux, FotoForensics, FOCA, MD5 SHA y Exiftool.

Análisis:

En la Anexo 1: Fase de Adquisición (**Anexo 1**: Fase de Adquisición**)** detalla que las imágenes fueron adquiridas desde las unidades de almacenamiento como Disco Duro, USB y memoria Ram enfatizando que los formatos de las imágenes son jpg y png, además, que las imágenes obtenidas algunas de ellas han sido manipuladas casi arbitrariamente sin afectar visualmente la imagen para la realización de la parte práctica de este proyecto.

En la fase de Preservación **(Anexo 2**: Fase de Preservación**)** se utilizan herramientas para el resguardo de la imagen antes de ser manipulada creando copias forenses para la realización de la práctica.

En la Anexo 3: Fase de Análisis **(Anexo 3**: Fase de Análisis**)** se detallan los paso a paso de cada una de las técnicas empleadas en este proyecto.

Se empleo técnica esteganográfica en las imágenes con formato jpg y png con el objetivo de incrustar información dentro de un archivo de imagen obteniendo así una nueva imagen, pero ya no íntegra. Se detalló la metadata y el hash de la imagen

antes de ser manipulada, luego se realizó el proceso de incrustación, finalizado dicho proceso se obtuvo la metadata y el hash de la nueva imagen para luego ser analizada y detallar los cambios de una imagen íntegra y una no íntegra.

La pericia de detectar la esteganografía se denomina estegoanálisis, con las herramientas **Herramientas de Software para validar la integridad de** imágenes mencionadas en el capítulo 3 se realizó la práctica del estegoanálisis, con dichas herramientas se detectó la presencia de datos ocultos en las imágenes. Los algoritmos con las que generalmente trabajan estas herramientas son las del **LSB** y **F5.**

Para analizar el nivel de error ELA se utilizó la herramienta FotoForensics que permite visualizar las regiones afectas en una imagen mostrando así que esta imagen ha sido manipulada teniendo un potencial de nivel de error más alto que el resto de la imagen.

Resultados:

A continuación, se detallan los resultados obtenidos en la fase de análisis **(Anexo 3**: Fase de Análisis**)** donde se describe las posibles evidencias de manipulación o presencia de información oculta. Para entender los resultados se sugiere ver los apartados **APLICANDO ESTEGANOGRAFÍA A LAS IMÁGENES**, APLICANDO ESTEGOANÁLISIS A LAS IMÁGENES y APLICANDO NIVEL DE ERROR ELA que muestran ejemplos muchos más detallados, esto facilitará la comprensión de los resultados obtenidos.

- **Esteganografía con la herramienta Stegosuite de CAINE a una imagen jpg.**

Inicialmente, se creó el archivo encuesta.docx que es el mensaje oculto a embeber a la imagen. Cabe mencionar que la imagen original a utilizar ocupa 4,45 MB y su hash es 3DD55B084743A10FF47ECEB8D195B64E.

Posteriormente, utilizando la herramienta StegoSuite se oculta el archivo encuesta.docx a la imagen original y utilizando o no la opción de password que ofrece la herramienta, se obtiene como salida una imagen idéntica a la original a simple vista, pero en tamaño la imagen baja a 2,4MB siendo menor que la imagen

original debido a la compresión de datos que la herramienta ejecuta durante el proceso donde comprime y oculta los datos en la imagen.

Y esta herramienta además optimiza el espacio de almacenamiento eliminando redundancias o aplicando procedimientos específicos para minimizar el tamaño de la imagen sin exponer la calidad visual de la misma ya que el objetivo es ocultar información sin afectar significativamente la percepción visual de la imagen. Inclusive esta herramienta elimina ciertos metadatos o información adicional de la imagen original durante el proceso de incrustación como se muestra en la **Figura 42** Metadata de la imagen incrustada utilizando FotoForensics donde solo se puede visualizar algunos de los metadatos de la imagen original.

Se compara el hash de la imagen original y con el hash de la imagen incrustada que en este caso es 347A49E75218A20313E5CF84D4EB7D87, como se puede apreciar el valor numérico se ha modificado ya que cualquier cambio mínimo que sea este, hace que el hash sea diferente ya que el objetivo principal de estos algoritmos es que sea como una huella digital única para cada imagen así sean dos imágenes idénticas.

Mediante el editor WinHex se presenta los datos que se pueden extraer a través de esta herramienta. Solo se presentarán los datos a partir de la cabecera de los archivos jpg que consisten en los bytes FFD8 (en hexadecimal), ya que cuando se realiza el proceso de incrustación la información se oculta desde la cabecera hasta final del archivo.

- **Estegoanálisis con la herramienta OpenStego de una imagen png**.

La herramienta OpenStego nos permite analizar una imagen en busca de posibles datos ocultos. A la imagen png incrustada se analiza la metadata como las dimensiones, resolución, y otros detalles técnicos, ya que muchos de ellos suelen ser comprimidos por la imagen y estas características dan indicio a presencia de datos ocultos.

Al seleccionar Extract Data la herramienta intentará detectar la presencia de esos datos en la imagen png especificada ya que OpenStego detecta información oculta mediante análisis de firmas de imágenes para identificar formatos específicos como

en la búsqueda de patrones específicos en la cabecera o el pie de una imagen, para así obtener como salida dicho archivo embebido para este ejemplo se obtuvo encuesta.docx.

– **Análisis de Nivel de Error ELA a imagen jpg**

Se realiza el análisis de error ELA, se compara el nivel de error en diferentes secciones de la imagen. Si una sección de la imagen muestra un nivel de error significativamente diferente en comparación con el resto de la imagen, es una indicación de que esa sección podría haber sido modificada o editada digitalmente.

Utilizando la herramienta en línea FotoForensisc se calcula el ELA a la imagen generalmente con formatos JPEG, cuando la imagen original se comprime a un cierto nivel de calidad utilizando el algoritmo de compresión específico, ELA compara esta imagen original con la misma imagen después de haber sido modificada, calcula la diferencia entre los niveles de error de las imágenes original y modificada. Esta diferencia se representa como una imagen que resalta las áreas donde los niveles de error son significativamente diferentes.

FotoForensisc crea un mapa de diferencias que muestra visualmente las áreas donde se han detectado cambios en los niveles de error. Las regiones resaltadas en este mapa suelen indicar posibles áreas de manipulación o edición en la imagen como se muestra en la **Figura 66** Imagen con ELA regiones sospechosas que muestran grandes diferencias en los nivele de error.

Conclusiones:

- La capacidad de ocultar información en imágenes se demostró mediante la incrustación de un archivo en una imagen sin afectar significativamente su apariencia visual.
- La detección de datos ocultos en las imágenes demuestra la capacidad de estas herramientas para identificar patrones esteganográficos y revelar la presencia de información oculta.
- La identificación de áreas con niveles de error significativamente diferentes proporciona evidencia visual de posibles manipulaciones en las imágenes,

respaldando así la detección de alteraciones digitales usando el algoritmo ELA.

- La combinación de herramientas especializadas y metodologías forenses permitió detectar y analizar posibles manipulaciones en imágenes, lo cual es esencial para la preservación de la integridad y autenticidad de la evidencia digital.