TITULO

MANUAL DE BUENAS PRÁCTICAS UTILIZANDO HERRAMIENTAS DE ANALISIS FORENSE DIGITAL EN UNIDADES DE ALMACENAMIENTO

Adrián José Barrios Vergara

MONOGRAFIA DE INVESTIGACION PRESENTADO PARA OPTAR POR EL TITULO DE:
ESPECIALISTA DE CIBERSEGURIDAD

DIRECTOR:
JUAN FERNANDO HURTADO RIVERA

LINEA DE INVESTIGACION:
ANALISIS FORENSE Y CRIPTOGRAFIA EN UNIDADES DE ALMACENAMIENTO.

INSTITUTO TECNOLOGICO METROPOLITANO
FACULTAD INGENIERIA
MEDELLIN – COLOMBIA

2023

TABLA DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCION.

En el campo de la ciberseguridad el análisis forense es un pilar fundamental para encontrar evidencias digitales que ayuden a determinar la causa de un delito cibernético o violación de la seguridad en el sistema de información de una empresa, permitiendo identificar las vulnerabilidades y evaluar las contramedidas necesarias para prevenir futuros ataques. Es fundamental la recopilación de toda la evidencia digital cumpliendo con la cadena de custodia para poder posteriormente identificar los ataques los cuales continúan en constante crecimiento. Sumado a lo anterior, la ausencia de monitoreo y la falta de capacitación están ampliando la brecha de seguridad que deriva en malas prácticas, fuga o secuestro de información, entre otras, las cuales afectan gravemente el funcionamiento de las empresas.

En esta monografía se plantea un manual de buenas prácticas para implementar herramientas de análisis forense digital buscando compensar las falencias identificadas en el tratamiento de imágenes forenses en las organizaciones tanto privadas como públicas. Como consideración en la parte legal se tendrán en cuenta las leyes, normas o entidades que cobijan estos aspectos fundamentales de la ciberseguridad, para que áreas internas o generales dentro de las empresas respalden y contribuyan con investigaciones, sirviendo de guía cuando se presenten casos de vulneraciones en dispositivos o unidades de almacenamiento.

1. RESUMEN

El tratamiento de evidencia digital bien procesada puede aprovecharse al máximo por un perito forense aplicando técnicas y metodologías de extracción de información muy sofisticadas sin perder la cadena de custodia y dependiendo de los escenarios donde se plantea la problemática a tratar [1]. En cada proceso existen diversas orientaciones muy definidas con respecto a lo que se desea obtener: ya sea calidad probatoria, análisis muy precisos, restauración de servicios interrumpidos o recolección de evidencia digitales. Como componente claves que proporcionarán credibilidad a la monografía descrita son las metodologías aplicadas en todo el proceso, desde el análisis, la clasificación y obtención de resultados y el desarrollo de actividades específicas de cada metodología. En la siguiente monografía se presentarán pautas para el manejo de evidencia digital con herramientas ya definidas, sistematizando la identificación, adquisición, análisis y preservación de esta.

Estos procesos están diseñados para mantener la integridad de la evidencia, con una metodología aceptable para contribuir a su admisibilidad en procesos legales y en sintonía con las normas ISO/IEC 27037:2012 en concordancia con la anterior norma la ISO – NTC-ISO-TR 15801 [2] (tiene por objeto la gestión de los documentos físicos a formato digital, el tipo información almacenada electrónicamente, y sus respectivas recomendaciones para mantener la integridad y fiabilidad de estas), además como objetivo adicional también definen las mejoras prácticas para el correcto almacenamiento electrónico y como los protocolos de otras normas se evalúan y comparan entre ellas mismas. Finalmente, se muestran los resultados del análisis y la valoración de algunas herramientas.

PALABRAS CLAVES: Análisis forense Digital, Cadena de custodia, Criptografía, Ciberataques, Evidencia digital, Preservación Digital, Sistemas de particiones, Fuente de datos.

2. ESTADO DEL ARTE

De acuerdo con los conceptos planteados en la propuesta de monografía se identifican conceptos y teorías que deben ser desarrolladas para mayor comprensión de la problemática planteada.
Es así como en este apartado se desarrollarán 3 temas relacionados con Marco Teórico, Marco Conceptual y Marco Referencial, donde se sustentarán las teorías que apoyan la propuesta de monografía.

La norma ISO/IEC 27037:2012 [3], define la informática forense como un proceso que utiliza la ciencia y la tecnología con el propósito de desarrollar y demostrar hipótesis que permitan responder preguntas sobre lo ocurrido en un incidente de seguridad o delito informático a través de la evidencia digital por un software. La informática forense es un término que tiene varias definiciones y también aplicabilidad en el entorno donde se desarrolle, así como también en muchos procesos informáticos donde se busca analizar información no visible y con los resultados obtenidos desde estas herramientas se busca como solucionar estas brechas de seguridad que pueden ser accedidas por hacker o criminales que vulneren el software del dispositivo o también en sistemas informáticos como no dejar una ruta o huella visible la cual estas herramientas facilitan para hacer estos procesos [4].

Asimismo, la Guía para la Integración de técnicas forenses en la respuesta a incidentes NIST SP 800-86 considera y apropia la definición del análisis forense digital como la aplicación, la identificación y análisis de datos mientras se preservan la integridad de la información que requiere mantener una estricta cadena de custodia de los datos [5]. De la misma manera, la Organización Internacional de Policía Criminal INTERPOL reconoce que el análisis forense digital es fundamental para las investigaciones de incidentes, ataques y delitos informáticos en las organizaciones que implementan esta disciplina, ya que el análisis forense digital se encarga de la detección, adquisición, tratamiento, análisis y comunicación de datos almacenados en medios electrónicos [6, p. 17] . A continuación, hago un breve relato de como la informática forense inicio hasta la actualidad en entidades públicas como privadas además de técnicas utilizadas para cometer estos delitos.

En el año 1978, la informática forense dio un punto de partida donde reconocieron por primera vez que existían los delitos informáticos “Sabotaje, Copyright, alteraciones de datos o sistemas informáticos” implementados en los sistemas del momento [7]. Ya para los años 80`s donde salió al mercado las computadoras portátiles y PC de escritorios las cuales tuvieron una gran acogida y se posicionaron como medios indispensables de comunicación y automatización de procesos para la

realización de trabajos cotidianos lo que llevo a una revolución tecnológica donde día a día a evolucionado desde Portátiles APPLE , con sistema operativo MAC OS Classic basado en UNIX, hasta los desarrolladores del sistema operativo WINDOWS utilizados en la mayor cantidad de portátiles creados por HP, DELL, CORSAIR, ASUS entre otros basando su estructura funcional tanto en Windows y otros sistemas operativos en linux, En los años 1984 el FBI creo un Programa de medios magnéticos el cual llamo CART el cual era un grupo de personas que daban soporte, análisis de información, y asistencia a investigaciones [7].

En el año 1997, se formó un equipo especialista en recoger evidencias de equipos de cómputo, los cuales debían seguir un manifiesto emitido por el G8 en ese mismo año. De esta manera la INTERPOL celebro un simposio de informática forense a los dos años siguientes, el programa CART del FBI abordó más de 2000 casos individuales, con esta meta el FBI vio en aumento los casos lo cual llevo a que el programa analizara 17 TB de datos entre los años 2000 y 2003 y ya para finales del 2003 se llegaron a examinar casi 782 TB de información en 1 año. Debido al avance de nuevas tecnologías, dispositivos más inteligentes y el amplio acceso a Internet, los delincuentes empezaron a tener opciones para romper la ley y vulnerar diferentes sistemas incluyendo bancos [7]. Para el Dr. Acurio [8] existen diferentes tipos de análisis forense que se deben tener en cuenta a la hora de hacer el proceso inicial de obtención de los datos o pruebas electrónicas, ya que es una etapa muy importante donde se debe analizar el entorno y procesos muy descriptivos para formular hipótesis relacionadas con el caso, desde ese punto de partida encontramos lo siguientes tipos 1. Sistemas de computación abierto, 2. Sistemas de comunicación, 3. Sistemas convergentes de comunicación.

Como se ha mencionado anteriormente la ciberdelincuencia a abordado la tecnología para hacer actividades ilícitas desde años atrás, la policía nacional de Colombia aborda con varias entidades gubernamentales la informática forense y varias de sus ramas para investigar delitos en entidades públicas o privadas como también en empresas, implementando estas ramas de defensa en las fuerzas armadas también para combatir la delincuencia [9]. El diario “El Tiempo” destacó que en el año 2004 desde que se creó esta entidad se han detectado más de 7.360 virus un aumento del 32 % [9] con respecto al año anterior, lo cual aumento el ataque a entidades financieras entre otras, por esta razón se generó una pérdida de 666 millones de dólares por estos problemas para lo cual fue necesario investigadores forenses que investigaran estos incidentes como la Dijin, CTI, Cipol, que actualmente brindan herramientas y protegen al país cuando ocurre un incidente.

Las unidades de almacenamiento llamadas HDD y SSD son dispositivos de almacenamiento, pero con diferencias en su formato tanto internas o externas, de forma general un dispositivo funciona en CD magnéticos y la otra unidad por memorias Flash Nand que actúan como bloques en un mismo espacio muy delgado haciendo que sean más volátiles y se ahorre espacio donde se instale. Los dispositivos de almacenamiento magnéticos son no volátiles, donde se encuentran instalados todos los programas e información personal de los usuarios para que puedan interactuar con el hardware y el dispositivo está compuesto por platos o discos unidos bajo un mismo eje que gira a una velocidad reprogramada en un microchip el cual esta sellado internamente, estos dispositivos dependiendo del tipo de conexión pueden ser SATA, SAS, SCSI, IDE, a medida que la tecnología ha avanzado estas unidades han evolucionado en formatos desde gigas hasta teras [10]. En estas unidades de almacenamiento se ha avanzado en las herramientas de análisis forense en la fase de recuperación de información, restauración, y borrado seguro de datos, el realizado de copias y la clonación de estas mismas copias, sin alterar los datos originales, entre otras funciones especializadas estas técnicas utilizadas por investigadores forenses y una de estas herramientas forenses es el AccesData Toolkit (FTK) [11] .

En unidades de estado sólido la función es diferente en arquitectura ya que tienen componentes electrónicos más comprimidos como memorias Flash Nand, el cual se define que es una memoria no volátil diseñado como almacenamiento secundario o auxiliar. Todo este sistema es gobernado por un controlador que establece unas reglas en un conjunto de bloques de memorias NAND que actúan como arreglo en miniatura, lo que permite aumentar la velocidad de lectura y escritura junto a otras propiedades como el acceso, ya que es posible aumentar o realizar varias lecturas simultaneas tanto de escritura como lectura haciendo que el dispositivo sea más persistente en fallos internos o de software [10]. En estas unidades existen varios formatos lo que optimizan el borrado seguro de información como el de bajo nivel o FAT 32, lo que conlleva a que se vea la problemática de que las unidades de almacenamiento se pongan el formato RAW lo que no hace accesible la información a estas unidades porque no tienen el archivo de registro de la información dañado por una mala conexión, para mejorar esto se recomienda desconectar las unidades de forma segura o expulsarlas por el sistema [12].

El análisis forense digital se define como un conjunto de técnicas de recopilación y exhaustivo peritaje de datos, por lo que sin modificación alguna podría ser utilizada para responder en algún tipo de incidente en un marco legal. Un incidente es un evento en donde las políticas de seguridad de un sistema se ven corrompidas o comprometidas, siendo entonces el objetivo entender la naturaleza del ataque de este modo se debe establecer una serie de cuidados establecidos lo que comúnmente se conoce como cadena de custodia, estos mecanismos nos garantizan la confiabilidad en el manejo de estas evidencias al recolectarlas, analizarlas y entregarlas en un caso judicial [13].

La criptografía consiste en transformar información mediante la implementación de algoritmos y una clave de cifrado y descifrado como en el caso de los sistemas simétricos o el uso de dos claves como en los sistemas asimétricos, buscando que el resultado sea incomprensible a quien acceda a la información sin autorización o la robe, de modo que esta información solo sea descifrada o leída por el destinatario autorizado. En la actualidad muchas empresas o instituciones gubernamentales hacen que sea obligatorio el uso de cifrado de la información en reposo y en tránsito en equipos tecnológicos, además la criptografía tiene 4 pilares que giran en el entorno físico, datos, en proceso y arquitectura de sistemas [14], también existen 3 tipos de criptografía: clave secreta, clave pública y funciones Hash lo que facilita su implementación según sea su necesidad en el entorno utilizado.

Un ciberataque es un conjunto de acciones dirigidas contra sistemas de información, como pueden ser bases de datos o redes computacionales, con el objetivo de perjudicar a personas, instituciones o empresas. Este tipo de acción puede atentar tanto contra los equipos y sistemas que operan en la red, anulando sus servicios, como contra bases que almacenan información, siendo esta espiada, robada o incluso, utilizada para extorsionar [15]. Los ciberataques se clasifican en amenazas internas o externas y sus tipos más comunes en la actualidad son los troyanos, denegación de servicios, DNS tunnel, Ransomware, Phinsing, entre otros.

La evidencia digital “es única, cuando se le compara con otras formas de “evidencia documental”. A comparación de la documentación tradicional (aquella realizada en papel), la evidencia informática o tecnológica es frágil y cuenta con la posibilidad de permitir la copia idéntica al original. Otro aspecto único en la recolección de la evidencia es la posibilidad de obtener copias autorizadas sin dejar rastro de que se realizó una copia” [16]. De acuerdo [17] en el apartado de Proyect Computer Forensic Tool Testing (CFTT) se afirma que hay que tener en cuenta los procedimientos para el análisis de todas las evidencias obtenidas a partir de una copia forense del dispositivo original o sus respectivas copias, lo

que sus clonados deben contener el mismo Hash y no deben ser alteradas dados que estos deben contener la misma evidencia del original y alguna modificación invalidara inmediatamente la evidencia digital, por lo anterior los investigadores forenses deben revisar constante las evidencias digitales sin ningún cambio.

La preservación digital es definida como el proceso o acción que contribuyen a garantizar el acceso continuo o indefinido de evidencia o información en un registro que existe de forma digital. La preservación Digital para Ferreira [18] tiene como objetivo superar la debilidad del soporte físico, la obsolescencia tecnológica y la vulnerabilidad del medio digital para garantizar la autenticidad, fiabilidad, integridad, así como el acceso seguido a la información, siendo esta la única manera de garantizar y promover la memoria colectiva e institucional. En las directrices para la preservación digital se define la preservación como las acciones destinadas a mantener la accesibilidad de los objetos digitales a largo plazo [19].

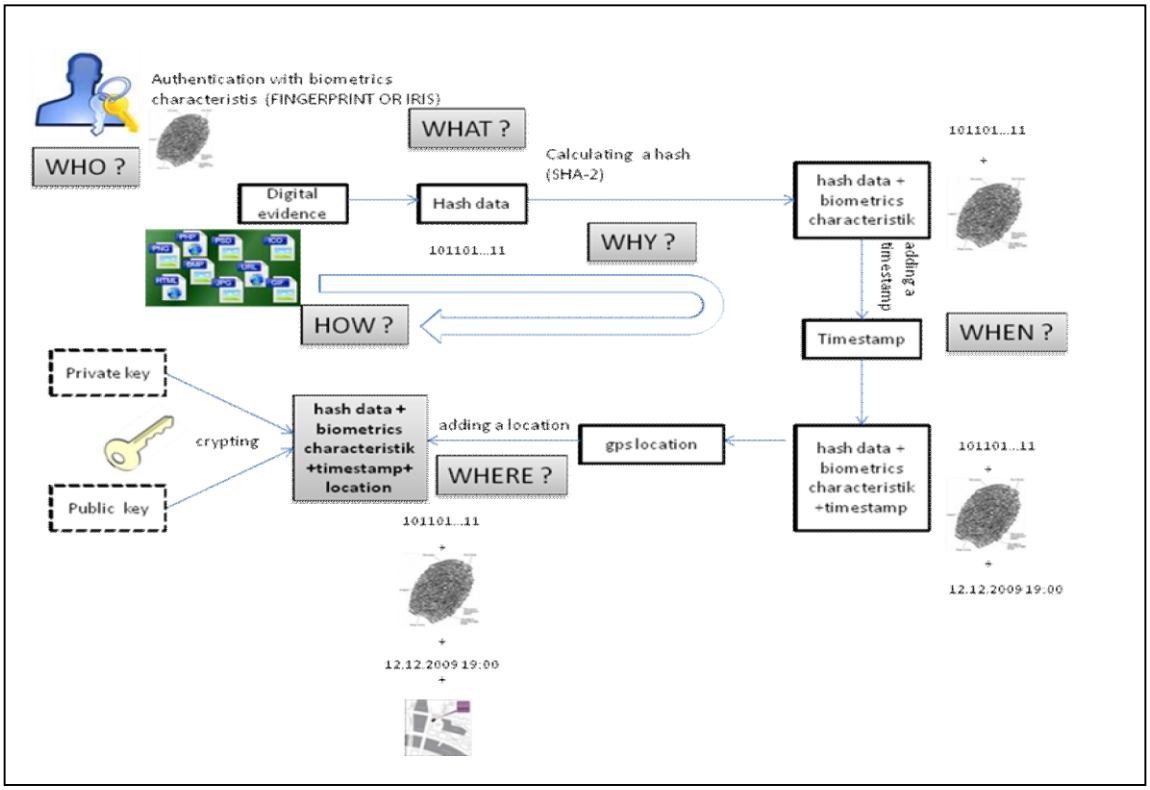
Los sistemas de particiones de un disco duro son una división lógica en una unidad de almacenamiento, un disco duro o unidad flash, en la cual se alojan y organizan los archivos mediante un sistema de archivos. Existen múltiples sistemas de archivos con diferentes capacidades como: FAT, NTFS, FAT32, EXT2, EXT3, EXT4, Btrfs, FedFS, ReiserFS, Reiser4 u otros, una partición de disco, en mantenimiento, es el nombre genérico que recibe cada división presente en una sola unidad física de almacenamiento de datos. Toda partición tiene su propio sistema de archivos (formato); generalmente, casi cualquier sistema operativo interpreta, utiliza y manipula cada partición como un disco físico independiente a pesar de que dichas particiones estén en un solo disco físico [20].

Las fuentes de datos son los tipos de información que pueden ser recolectada, analizada y utilizada y resolver los incidentes de ciberseguridad, estas fuentes de datos pueden incluir registros de eventos de los sistemas, archivos de registro de actividad, registros de red, registros de bases de datos, registro de aplicaciones entre otros además de los registros también se pueden incluir dispositivos físicos de almacenamiento lógico digital como lo son los discos duros, unidades flash, discos ópticos así como los dispositivos de red como los Router, cortafuegos o dispositivos de seguridad en la red, las fuentes de datos en ciberseguridad forense pueden ser variadas y pueden incluir cualquier cosa que proporcione información relevante para investigar un incidente de seguridad cibernética. La selección de las fuentes de datos y su análisis adecuados son fundamentales para la obtención de pruebas sólidas y la resolución de incidentes de seguridad cibernética [21].

Las huellas de evidencia hacen parte fundamental en la reconstrucción de un proceso digital [22] para lo cual se propone no utilizar la evidencia digital original, en su lugar recomiendan que se maneje una huella digital de las pruebas. Para calcular la huella digital se utilizará una función hash SHA-2, en lugar de las funciones SHA-0 o SHA-1. Esto se hace para evitar un ataque criptográfico (colisión y/o ataque preimagen). No hay límite del tamaño del archivo de evidencia digital para el que se desea calcular un hash. Se puede utilizar un archivo (jpg, tiff, txt, etc.), un grupo de archivos o algún tipo de archivo específico (zip, rar, tar, etc.) o incluso una unidad física (disco duro, memoria externa, etc). Al utilizar una función hash SHA-2, se dará un valor de tamaño fijo (224, 256, 384 o 512 bits dependiendo de sí se usa SHA-224, SHA-256, SHA-384 o SHA-512). Las huellas más utilizadas son SHA-256 y SHA-512 en un caso judicial.

Figura 1

Concepto de marcos para garantizar las huellas de una cadena de custodia.



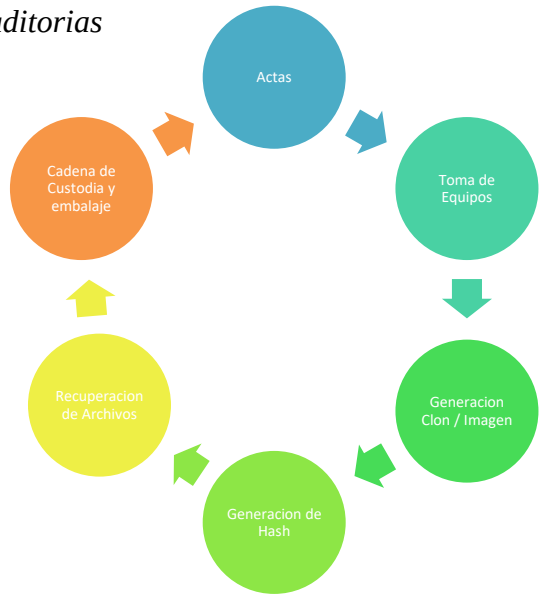
Nota. Marcos de evidencias para la preservación de una buena reconstrucción y toma de evidencias digitales Fuente: [22].

En este apartado se identifican todos los trabajos referenciales que aportan al desarrollo de la problemática planteada. En este sentido, en la investigación [23] de las "herramientas de análisis forense digital orientadas a infraestructuras TI como medio de investigación en delitos informáticos". La aplicación y las recomendaciones de estas guías y mejores prácticas relacionados con el análisis forense digital se encuentran en NIST SP 800-86- Guía para la integración de técnicas forenses en la respuesta a incidentes (2006)" [24]. Esta guía tiene como propósito presentar el análisis forense desde una perspectiva de TI. Describe los procesos para realizar actividades forenses efectivas a sistemas informáticos y redes, informa sobre las tecnologías y forma de uso para actividades de respuesta de incidente. La NIST SP 800-44 versión 2 [25]- Directrices sobre la protección de servidores web públicos (2007), describe las prácticas para la elección de plataformas y software del servidor web, instalación, configuración y mantenimiento de servidores web públicos seguros. Configuraciones de parches y actualizaciones, pruebas de seguridad entre otros.

La RFC 3227 Guidelines for Evidence Collection and Archiving [26] directrices para la recolección de evidencias y su almacenamiento, sirve como estándar para la recolección de información en los incidentes de seguridad debido a que esta incluye los principios a seguir durante la recopilación, adquisición y archivos de pruebas, las consideraciones de factores como la volatilidad de la evidencia, privacidad de la información recopilada, aspectos legales de la evidencia, transparencia en el proceso de recolección de la evidencia y métodos utilizados, aspectos que se ha de tener cuenta al realizar la documentación en el procedimiento de almacenamiento que permita garantizar la cadena de custodia de la evidencia y herramientas necesarias para llevar a cabo la recolección de estas.

Figura 2

Metodología Actual de Auditorias



NOTA. Metodología actual de auditorías forenses implementado en TIC. Fuente. [26]

Esta metodología de auditorías se soporta en el estándar ISO/IEC 27037:2012 [27] cuya directriz está enfocada en la recopilación de evidencias y su correcto almacenamiento brindando las pautas para la identificación, recolección, adquisición y preservación de la evidencia digital, la cual está basada en los principios fundamentales de relevancia, confiabilidad y suficiencia. Este estándar está diseñado para conservar la integridad de la evidencia digital y posee una metodología acorde a los requerimientos de la cadena de custodia permitiendo su admisibilidad en un proceso judicial [28].

También se utiliza la norma británica BS 10008 "Valor probatorio y admisibilidad legal de la información electrónica" [29] que engloba y define las mejores prácticas para le gestión y almacenamiento de la información electrónica la cual ayuda en la verificación y autenticación de la información con el objetivo de evitar perjuicios judiciales o descarte de las evidencias en un evento legal proporcionando relatividad a la parte administrativa legal y el almacenamiento de los datos. Es importante mencionar que esta norma nos muestra las mejores prácticas en la transferencia de datos electrónicos entre sistemas y la migración de registros en papel a lo digital ofreciéndonos la guía incluida de gestión de disponibilidad y accesibilidad de estos mismos que puedan ser necesarios como pruebas legales.

El manual de "ENFSI-BPM-FIT-01 Best Practice Manual for the Forensic Examination of Digital TechnologyÇ (2015)" [30]. (mejores prácticas para el examen Forense de la tecnología digital) tiene como objetivo definir las mejores prácticas europeas en el campo de la informática forense, destaca la importancia de la utilización de una metodología coherente para el análisis forense de equipos informáticos y teléfonos. Este documento incluye la recomendación formal al grupo de trabajo de informática forense para solo considerar la validación de procesos más que las herramientas de validación. La "Good Practice Guide for Computer- Based Electronic Evidence ACPO 2012" [31] (Guía para las buenas prácticas de manipulación adecuada de medios digitales) puede ser aplicada a todo tipo de fuentes de datos informáticos y dispositivos móviles desarrollo por la Asociación de Comisarios de Policía del Reino Unido.

OSForensics, es una herramienta que nos permite realizar un diagnóstico forense a nuestros computadores, trae una versión gratuita y de pago, con múltiples aplicaciones como lo es el algoritmo hash para obtener huellas digitales de cada archivo contenido en el computador (también en la versión gratuita), con ello podemos evidenciar si un archivo fue borrado, modificado o alterado de algún modo, implementando diferentes algoritmos como MD5, SHA1,SHA-256 entre otros, además dispone de rainbow tables, analizando datos de un disco ya montado entre otras funcionalidades más intrincadas a medida que la herramienta se actualiza.

La herramienta "FTKImager es un software de análisis forense que se utiliza para crear archivos de imagen de disco o montar imágenes de disco o dispositivos de almacenamiento y realizar análisis de la estructura del disco, recuperar datos, o información borrada, etc. Este software permite localizar archivos perdidos o buscar datos escaneando la imagen de disco mediante palabras claves." Esta herramienta es muy potente y utilizada por el ámbito forense, debido a la amplia utilidad que tiene y sus nuevas herramientas que permiten desde el volcado de memoria, imágenes forenses, hasta la realización de búsquedas de nivel hexadecimal de metadatos, identificados por un archivo de medios llamado "magic numbers" [32] . Al realizar una copia digital se procede a hacer múltiples duplicados de la imagen para dejar la unidad examinada sin ningún tipo de manipulación para cumplir con las políticas y estándares a nivel internacional de la cadena de custodia, permitiendo que haya una muy organizada estructura de presentación de la información en un caso judicial [33].

3. DESCRIPCION DEL PROYECTO

PLANTEAMIENTO DEL PROBLEMA

Los mayores creadores de hardware de almacenamiento a nivel internacional como Kingston, Seagate, Crucial, Toshiba, entre otros, tienen protocolos a nivel de software y hardware para el correcto funcionamiento de lectura y escritura de estos dispositivos, los cuales pueden extender el tiempo de sustracción de la información o generar bucles al momento de hacer la adquisición de una imagen forense. En unidades magnéticas se evidencia que se ponen lentas y tienden a dar errores e igualmente a quedarse en bucles en ciertas particiones cuando la unidad está dañada, mientras que en unidades de estado sólido es óptimo y genera menos perdida de evidencia al momento de crear la imagen forense. Lo anterior, genera problemas de seguridad a la hora de entregar los resultados por parte de un perito forense causando que los hashes no sean iguales a la hora de compararse los resultados.

De acuerdo con lo anterior se evidencia que existen problemas de confiabilidad en cuanto a la recolección de las pruebas al momento de adquirir las imágenes forenses. En este sentido se propone un manual de buenas prácticas basado en los resultados de las herramientas FTKImager y OSForensics que permita el análisis de unidades de almacenamiento de una forma más confiable, optimizando el tiempo y brindando al perito forense insumos para mejorar los reportes relacionados con los incidentes de ciberseguridad identificados en las empresas.

JUSTIFICACION

La informática forense busca generar resultados e impacto en investigaciones judiciales que se ven reflejadas en procedimientos jurídicos cuando a una parte afectada se le ha vulnerado su seguridad u afectado la información. El proceso de análisis forense se realiza de forma metodológica y sus resultados brindan insumos para la toma de decisiones con respecto a los procedimientos de como las empresas resguardan su información, evidenciando sus debilidades en los dispositivos de almacenamiento en tres tipos de calificaciones alto, medio y bajo.

Uno de los muchos objetivos más sobresalientes de la informática forense es generar evidencias legales, los cuales son analizados, verificados, y autenticados para poder así responder cuestiones técnicas que se plantean en los juzgados con estos resultados de los informes. Para [34] la informática forense permite dar soluciones a problemas relacionados con la seguridad de la información, como principio salvaguardar la información digital, en caso de haber incurrido en delito, utilizando como medio el computador o algún equipo digital de la empresa.

En la ciudad de México se implementa un formulario por los cuerpos de seguridad, y lo llaman cadena de custodia para recolectar información cuando hay un robo de información [35].

Figura 3

Ejemplo de formulario de cadena de custodia.

Anywhere Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _39827649_____ Offense: _ Selling company materials_____
Submitting Officer: (Name/ID#) _Aaron Denning_____
Victim: _Mr. Brown Browns Wholesale_____
Suspect: _Mr. Black_____
Date/Time Seized: _5/14/16_____Location of Seizure: _Mr. Browns Wholesale___

Description of Evidence

Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)
1	1	Thumbdrive, Serial # 489387, Good, normal wear
2	1	Laptop Serial # 7392749, Good, Some scratches

Nota: Cadena de custodia de evidencias digitales en un caso forense Fuente [1].

PREGUNTA DE INVESTIGACIÓN

¿Cómo, mediante la implementación de un manual de buenas prácticas para un proceso de análisis forense basado en la norma ISO 27037 y BS 10008, utilizando las herramientas FTKImager y OSForensics, se puede contribuir a la identificación de falencias en el tratamiento de imágenes forenses?

4. OBJETIVOS

GENERAL

Proponer un manual de buenas prácticas en un proceso de análisis forense basado en la norma ISO 27037 y BS 10008, utilizando las herramientas FTKImager y OSForensics, para compensar las falencias identificadas en el tratamiento de imágenes forenses en las organizaciones.

ESPECÍFICOS

- Definir la importancia y funcionalidad de la informática forense.
- Aplicar las diferentes herramientas de informática forense para crear imágenes digitales en unidades de almacenamiento magnéticas y sólidas.
- Comparar los diferentes procesos y resultados que se llevan a cabo durante las diferentes etapas de levantamientos de requisitos en un caso de análisis forense con la herramienta FTKImager y OSForensics.
- Identificar las mejores prácticas en un proceso de análisis forense a partir de la evaluación y datos obtenidos de nuestro análisis forense con las herramientas FTKImager y OSForensics.

5. METODOLOGÍA

Según la guía Didáctica de Monge existen 3 tipos de metodologías "cualitativa, cuantitativa, y mixta" que se implementan a la hora de hacer un documento de investigación para demostrar resultados o hacer una comparación de eventos, obteniendo a partir de estos y sus resultados, como pueden aportar conocimiento para nuevas investigaciones y aportar al conocimiento científico nuevas soluciones a partir de la problemática descubierta [36]. Dentro de los conceptos estipulados utilizados para desarrollar, se encuentran diferentes metodologías las cuales orientarán los resultados de la propuesta de investigación, es así como en la presente monografía se definió una metodología cuantitativa la cual permitirá lograr todas las metas medibles y alcanzables para resolver la problemática propuesta y de tipo descriptiva la que nos permitirá analizar el tipo de resultado requerido ya sea descriptivo, numérico o mixto [37].

MARCO LÓGICO:

En el siguiente apartado se hace una breve descripción y definición de todos los procesos que componen nuestro documento desde el análisis hasta la descripción de los resultados obtenidos a partir de la aplicación de herramientas de ciberseguridad en extracción de imágenes forenses en unidades de almacenamiento y como con una buena aplicación y análisis de las herramientas, se logra confiabilidad, se optimizan tiempo y se generan buenos resultados. Una vez planteados los objetivos específicos de la presente monografía, se definen en la Tabla 1 fase de los objetivos, con el fin de cumplir oportuna y pertinentemente con los resultados de la presente investigación.

TABLA I

FASE DE OBJETIVOS

FASES	OBJETIVOS ESPECIFICOS	ACTIVIDADES	ENTREGABLES
FASE 1: Importancia de la informática forense.	1 ANALIZAR	• Se identifica la importancia de la informática forense. • Se investigan los diferentes tipos de informática forense y su aplicación. • Búsqueda de referencias del tema.	Descripción e importancia de la informática forense, su aplicabilidad en diferentes casos de investigación.

FASE 2: Identificación de las diferentes herramientas que tienen mayor impacto en investigaciones forenses en unidades de almacenamiento HDD, SSD.	2 DEFINIR	• Se realiza una exhaustiva investigación de las diferentes herramientas de extracción y análisis de datos digitales. • Se seleccionan las herramientas de análisis forense y su aplicabilidad a diferentes unidades de almacenamiento.	Descripción con los diferentes tipos de herramientas de análisis digital para la correcta interpretación de sus datos.
FASE 3: Comparación de los procesos y resultados obtenidos de las herramientas FTKImager y OSForensics Imager durante toda la etapa de levantamiento de requisitos y resultados.	3 COMPARAR	• Se identifican las herramientas para hacer los análisis y validación de los resultados obtenidos. • Se realiza una breve descripción de la etapa de levantamiento de requisitos para un correcto peritaje.	Descripción de los procesos y correcta interpretación de los datos a la hora de utilizar FTKImager y OSForensics.
FASE 4: Evaluar los resultados obtenidos al implementar estas herramientas mejorando prácticas a partir de la comparación y obtención de resultado de estas.	3 DETERMINAR Y EVALUAR	• Se realiza un breve análisis de todo el proceso y las diferencias a la hora de implementar estas herramientas en un peritaje forense. • Búsqueda de referencias de la implementación de un perito forense de ambas herramientas.	Descripción de los resultados obtenidos de la correcta implementación de FTKImager y OSForensics.

Nota: Proceso de descripción de las fases del marco lógico con los objetivos específicos a desarrollar.

DETALLES DEL MARCO LOGICO

Fase 1: La importancia de la informática forense.

Objetivo 1: Se analiza la importancia de la informática forense.

Actividad 1: Que es la informática forense, cuál es su importancia en un caso judicial, los tipos de informática forense y su aplicación a diferentes casos, para ello realizaremos una profunda búsqueda exhaustiva de proyectos y referencias que apoyen el problema planteado.

Entregable 1: Se entrega en la primera fase la descripción e importancia la importancia de la informática forense y su aplicabilidad en diferentes casos de investigación.

FASE 2: Diferentes herramientas que tienen mayor impacto en investigaciones forenses en unidades de almacenamiento HDD y SSD.

Objetivo 2: Se definen las diferentes herramientas de extracción de imágenes forenses.

Actividad 2: Se realiza una investigación exhaustiva de las diferentes herramientas de extracción de imágenes forenses, definiendo como es su proceso de extracción, características, diferencias y errores encontrados a la hora de hacer una extracción bajo las normas ISO27037:2012 y su debido tratamiento en diferentes unidades de almacenamiento.

Entregable 2: Se entrega en la segunda fase la descripción con los diferentes tipos de herramientas de análisis digital que existen y la correcta interpretación de sus datos.

FASE 3: Se describen los procesos y resultados obtenidos de las herramientas FTKImager y OSForensics Imager durante toda la etapa de levantamiento de requisitos y resultados.

Objetivo 3: Se describen los resultados obtenidos de diferentes herramientas de extracción de imagen forense y sus resultados interpretando sus diferencias.

Actividad 3: Se analizan los resultados obtenidos de ambas herramientas describiendo sus diferencias y problemas al utilizarlas en una extracción virtual y clonación de diferentes imágenes en diferentes dispositivos de almacenamiento, dando credibilidad a la cadena de custodia, bajo la norma BS 10008:2008 “Garantía de un almacenamiento correcto de la información digital” [29].

Entregable 3: Se entregará en la tercera fase la descripción de los procesos que se realizan en la implementación de herramientas de análisis y la correcta interpretación de sus datos.

FASE 4: Evaluar los resultados obtenidos al implementar estas herramientas mejorando prácticas y resultados del proceso.

Objetivo 4: Evaluar los datos obtenidos de la aplicación de las herramientas y como sus diferencias pueden inferir en el proceso de análisis forense.

Actividad 4: En esta fase se evaluarán los datos y a partir de sus diferencias se describirán soluciones y mejores prácticas para un caso judicial al utilizar estas herramientas tratadas.

Entregable 4: Se entrega en la cuarta fase la descripción con los resultados obtenidos de las aplicaciones de las herramientas de análisis forense y como sus resultados pueden aportar en la correcta interpretación de los datos obtenidos por un perito forense.

DESARROLLO DEL TRABAJO DE CAMPO.

Fase 1: La importancia de la informática forense.

Objetivo 1: Se analiza la importancia de la informática forense.

Actividad 1: Que es la informática forense

La informática forense es aquella rama de la ciberseguridad que se encarga de investigar cómo, dónde, cuándo o con qué herramientas se vulneraron los sistemas informáticos con el fin de obtener o alterar datos. Cuando se habla de informática forense nos referimos al conjunto de procedimientos y técnicas tanto metodológicas como empíricas para la identificación, recolección, preservación, extracción e interpretación de estas evidencias al utilizar software especializado en el análisis de estas de manera que las evidencias puedan ser aceptadas en procedimientos legales o administrativos en un caso judicial [38].

De esta manera, la informática forense en el ámbito judicial y en el ámbito digital muestra de manera física como fue vulnerado un sistema o robado información mediante técnicas de ingeniería social, entre otras técnicas su focalización es los delitos cibernéticos o utilizando la tecnología para sustraer información o vulnerar sistemas como las redes, los servidores o dispositivos de almacenamiento en aquellos casos donde se involucra la tecnología como fuente principal para cometer un delito [39]. Uno de los principales propósitos donde se aplica esta rama es la informática o TIC, donde hay una mayor repercusión donde se suspende o interfiere en alguna actividad muy importante del Core de cualquier negocio y esto es muy importante para tener en cuenta en la cotidianidad antes de abordar los diferentes tipos de informática forense se debe tener una definición muy explicita de su función.

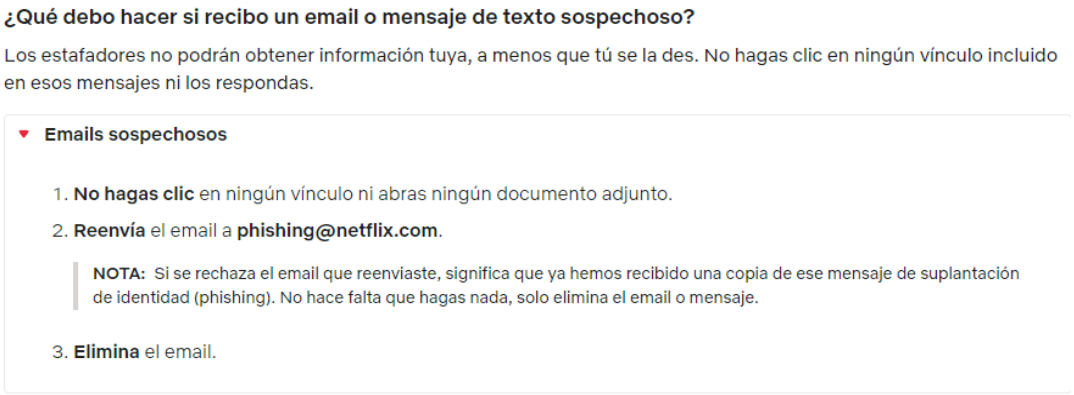
Existen 4 tipos de informática forense, los más relevantes e importantes a la hora de hace un perito forense son las siguientes:

- Sistemas operativos: en esta etapa se enfocan en los procesos de recuperación de información útil de algún sistema operativo infectado de algún dispositivo, con el objetivo de adquirir evidencia contra los ciberdelincuentes.
- Redes: consiste en la recopilación, monitorización y el análisis del tráfico o actividades en la red para descubrir patrones, vectores u orígenes de ataques o violaciones de seguridad. Usualmente se utiliza para identificar el tráfico sospechoso para remediar ataques.
- Dispositivos móviles: el objetivo de este proceso en la informática forense consiste en recuperar evidencia digital o metadatos borrados o sustraídos de los sistemas móviles.
- Nube o cloud: es la combinación de la computación o procesos en la nube y el análisis forense digital.

Un ejemplo práctico fue el 4 agosto de 2023, donde se detectó una campaña de phishing por el instituto nacional de ciberseguridad hacia la organización de entretenimiento y streaming Netflix, donde se pedía a los usuarios cambios en la suscripción de sus cuentas ha expirado y que si quieren extenderla por un periodo de 90 días ingresaran los nuevos datos en un formulario adulterado [40]. De la anterior vulnerabilidad detectada por una brecha de seguridad a la que estamos expuestos las personas es necesario tener los sistemas y personal aplicado en los procesos donde se detecte a tiempo y hacer las correcciones sin interrumpir la utilización del servicio en tiempo real haciendo esto una falla muy crítica a la organización y bajando la credibilidad en la utilización del servicio por consiguiente Netflix tiene una serie de recomendaciones en su sitio oficial como la siguiente.

Figura 4

Email Sospechoso



Nota: Que hacer en caso de un Email sospechosos. Tomado de: [41]

Ante esta problemática Netflix tiene unas sugerencias en su centro de ayuda que pueden ayudar a remediar esta vulnerabilidad y también la tiene como políticas para sus usuarios mantenerse siempre alerta o reportar la llegada de email o mensajes de texto sospechosos que solicite información personal ya que esta no es pedida si no dentro de la cuenta del usuario para validar pagos y otros procesos etc.

- Si tiene dudas nunca hacer clic en su lugar dirigirse directamente al sitio web de la empresa.
- Nunca enviar información confidencial personal o financiera por correo.
- Comprobar siempre la dirección del remitente para su verificación legitima.
- Verificar desde otra computadora la URL antes de hacer clic en ellos.
- nunca instalar software de terceros adjuntos al correo.
- Tener antivirus que detecten estas series de peligro y que ayuden mantener los dispositivos protegidos.

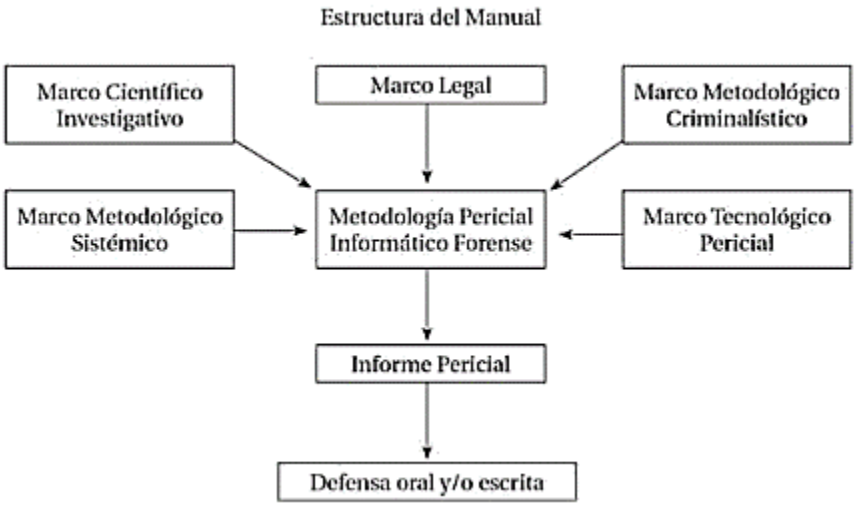
Luego de hacer una investigación exhaustiva sobre importancia de la informática forense y vulnerabilidades descubiertas como el anterior caso que apoyen a describir mejor la funcionalidad de la seguridad informática en cualquier ámbito que apoyen a nuestra problemática plateada [42].

Entregable 1: Se entrega en la primera fase la descripción e importancia de la informática forense, su aplicabilidad en diferentes casos de investigación.

Para [43] todo perito informático debe tener clara una estructura base de partida para armar un caso del cual se componen la estructura o base como apoyo a un caso judicial, Son cuatro marcos y cada marco debe ir direccionado hacia la metodología pericial como eje central teniendo un marco científico investigativo, y un marco metodológico de base que apoye sobre la metodología pericial como núcleo central de todas las partes interesadas para luego armar un informe pericial donde todos los procesos se sustenten en una buena defensa investigativa, oral o escrita. Este tipo de especialidad debe ser constantemente actualizada y justificada por otras ciencias y técnicas, que aporten diferentes entornos específicos entre los que deben destacar de otros.

Figura 5

Estructura de un manual de un perito forense



Nota: Estructura de un manual de un perito informático forense. Fuente: [44].

En la anterior figura 5 podemos observar como la metodología pericial debe estar en constante actualización para ser tomada y referenciada en reconstruir hechos ilícitos en sistema informáticos donde se involucre el sector (Penal, Civil, Contractual o particular), con el único fin de dar solución a una vulnerabilidad detectada o donde se tenga en cuenta el análisis metodológico crítico y constructivo para los resultados obtenidos desde la base de un caso detectado y mostrar su veracidad en un juicio.

De esta forma describimos la importancia de la informática forenses desde cualquier vulnerabilidad o brecha de seguridad en los sistemas tecnológicos mediante la implementación de técnicas o procesos específicos donde se violen las norma ISO 27037 y BS10008, y el correcto trato de la información de cómo debe armarse y apoyarse el armado de un informe pericial haciendo más visible y de vital importancia la aplicación de buenas prácticas en la actualidad debido a nuevas técnicas y la capacidad de investigar ò analizar las evidencias digitales en casos legales delitos informáticos su importante aplicabilidad y como esta se extiende a diversas áreas de investigación desempeñando un papel fundamental en la resolución de casos a nivel técnicos y jurídicos.

FASE 2: Diferentes herramientas que tienen mayor impacto en investigaciones forenses en unidades de almacenamiento HDD y SSD.

Objetivo 2: Se definirán las diferentes herramientas de extracción de imágenes forenses.

Actividad 2: Se realiza una investigación exhaustiva de las diferentes herramientas de extracción de imágenes forenses, definiendo como es su proceso de extracción, características, diferencias y errores encontrados a la hora de hacer una extracción bajo la norma ISO 27037:2012 y su debido tratamiento en diferentes unidades de almacenamiento.

La recuperación de datos forenses es un proceso exclusivo de restauración o recuperación de datos o metadatos que se utilizan en casos legales o judiciales. A diferencias de otras herramientas de extracción o recuperación de datos, estas son más sofisticadas porque ingresan al archivo raíz del log de la unidad de almacenamiento dando más detalles como hora, día, archivo, ubicación y tipo de borrado del archivo recuperado. En este apartado se definen múltiples herramientas de extracción forense consideradas confiables y con menos errores a la hora de hacer una extracción o recuperación de la unidad examinada [43]. De acuerdo con lo anterior, algunas de las herramientas que se utilizan para estas actividades son las siguientes:

- Magnet forensics

El software Magnet AXIOM es una herramienta de gestión forense digital diseñada para ayudar a profesionales en la ciberseguridad y proveedores de servicios jurídicos a obtener información sobre la recolección de pruebas o datos de diversas fuentes, incluyendo detección de datos en la nube, computadores y dispositivos móviles, la plataforma web permite a los administradores acceder al historial de navegación, imágenes, historial de chat y archivos o registros eliminados de un sistema operativo Windows o Android incluyendo también iOS [44]. Además, se puede recopilar información web como en redes sociales capturando archivos guardados en Google o Skype. Magnet AXIOM proporciona una funcionalidad de CBIR (recuperación de imágenes basada en contenido, por sus siglas en inglés), lo que permite a las empresas identificar armas, drogas y otras pruebas potenciales en distintos medios y en contenido.

CARACTERISITCAS PRINCIPALES.

- Permite obtener soporte avanzado para Mac.
- Encuentra rápidamente las pruebas clave.
- Visualiza las conexiones entre archivos, usuarios y dispositivos.
- Interfaz intuitiva y capacidades de revisión.
- Genera puntos de prueba automatizados.

TABLA II

Características del software forense MAGNET AXIOM.

Tipo de software	Clientes habituales	Tipo de Implementación	Idiomas Admitidos
Versión Gratuita ✗	Trabajadores autónomos(1 persona) ✗	Basado en Nube ✗	13
Versión de pago ✓	Empresa Pequeña (2-50) ✓	Local ✓	
	Empresa Mediana (51 - 500) ✓		
	Empresa Grande (500 o más) ✓		

Nota**.** Características fundamentales del software forense MAGNET AXION. Fuente: tomado [44].

- Wondershare Recoverit

La herramienta Wondershare Recoverit es un software de recuperación de datos desarrollado por la empresa de tecnología Wondershare, este programa está diseñado para ayudar a los usuarios a recuperar datos perdidos, eliminados o formateados accidentalmente de discos duros, unidades flash USB, tarjetas de memoria, cámaras digitales y otros dispositivos de almacenamiento. Recoverit utiliza algoritmos avanzados de escaneo y recuperación para buscar archivos perdidos y restaurarlos en su estado original, este software es capaz de recuperar una amplia gama de tipos de archivos, incluyendo fotos, videos, documentos, correos electrónicos y archivos de audios. Además, Recoverit ofrece una interfaz de usuario fácil de usar que permite a los usuarios recuperar datos en solo unos pocos clics, el programa también es compatible con Windows y Mac iOS X, y ofrece una versión gratuita limitada que permite a los usuarios escanear y previsualizar archivos perdidos antes de comprar la versión completa [45].

CARACTERISTICAS PRINCIPALES:

- Cualquier medio de almacenamiento.
- Garantía 100% segura y libre de virus.
- Más de 1000 formatos de archivo.
- Compatible con Windows y Mac.
- Recuperación de fotos, videos, audio, documentos y más.

TABLA III

Características del software WONDERSHARE RECOVERIT.

Tipo de software	Clientes de Equipos	Precio	Tipo de Implementación	Sistemas Operativos	Idiomas Admitidos
Versión Gratuita (30 días)	Para individuos (1 persona) MAX 2 PC ✓	$ 79.95 dòlares $ 375.000 Pesos colombianos ✓	Basado en Nube ✗	11 / 10 / 8 / 7 / Vista / XP ✓	Múltiples ✓
Versión de pago (1 años) (Perpetua)	Empresa Pequeña (2 - 50) MAX 5 PC	$ 899.95 dólares $ 4.213.268 Pesos colombianos ✓	Local ✓	Windows LINUX MAC ✓	Múltiples ✓
Licencia perpetua ✓	Empresa Mediana (51 - 500) MAX 10 - 15 PC ✓	$ 299.95 – 599.95 dòlares ✓ $ 1.405.021- 2.810.277 Pesos colombianos	Basado en nube ✓	11 / 10 / 8 / 7 / Vista / XP Linux ✓	Múltiples ✓
	Empresa Grande (500 o más) MAX 20 PC	899.95 dòlares $ 4.215.533 Pesos colombianos ✓			

Nota**.** Características fundamentales del software forense. Fuente: tomado [45].

- OpenText Encase Forensic: EnCase® Forensic es una poderosa plataforma de investigación que recolecta datos digitales, realiza análisis, informa sobre descubrimientos y los preserva en un formato válido a efectos legales y validados por los tribunales**,** esta herramienta de análisis de datos digitales es una solución que captura con facilidad los datos relevantes para respaldar investigaciones o requisitos de cumplimiento que brinden capacidades de análisis técnico elaboradas para hallar datos ocultos, también produce una duplicación binaria exacta del dispositivo o medio original y luego la verifica generando valores hash de las imágenes y asignando valores de CRC a los datos. Estas verificaciones revelan cuándo la evidencia ha sido alterada o manipulada indebidamente, ayudando a mantener toda la evidencia digital con validez a efectos legales para su uso en procedimientos judiciales [46].

CARACTERISTICAS PRINCIPALES:

- Obtener adquisiciones validas en efectos legales.
- Ahorro de tiempo con funciones de productividad avanzadas.
- Personalización con el tipo de examen a nivel de interno en el dispositivo.
- Proporciona y genera informes con respecto al caso creado.
- Opciones flexibles de elaboración de informes.
- Revisión externa automatizada.
- Adquisición de dispositivos móviles y computadoras.
- Procesamiento potente y personalizable.
- Flujos de trabajo de investigación integrados.

TABLA IV

Características del software ENCASE FORENSIC.

Tipo de software	Clientes habituales	Tipo de Implementación	Idiomas Admitidos
Versión Gratuita ✗	Trabajadores autónomos (1 persona) ✓	Basado en Nube ✓	Ingles
Versión de pago ✗	Empresa Pequeña (2-50) ✓	Local ✗	
Suscripcion ✗	Empresa Mediana (51 - 500) ✓		
	Empresa Grande (500 o más) ✓		

Nota: Características fundamentales del software Encase Forensic. Fuente: tomado [46].

- ACCESS DATA (FTK) IMAGER: Forensic Toolkit (FTK) es un software forense digital diseñado para ayudar a las empresas de los sectores financiero, energético, sanitario, legal y otros a recopilar y procesar datos de diversas fuentes, como unidades de almacenamiento SSD o HDD entre otros dispositivos móviles; además los expertos en ciberseguridad pueden indexar, almacenar y compartir datos con las partes interesadas para identificar evidencia relevante en un perito forense o caso judicial de la cotidianidad [47]. FTK es una solución de investigación digital construida para proporcionar velocidad, estabilidad y facilidad de uso. FTK recopila datos de cualquier dispositivo o sistema digital que produzca, transmita, almacene datos y realiza el análisis forense de los mismos. FTK es conocido por su interfaz intuitiva, su análisis de correo electrónico, las vistas de datos personalizables, su velocidad de procesamiento y su estabilidad [48].

CARACTERISTICAS PRINCIPALES:

- Velocidad y estabilidad inigualables.
- Base de datos.
- Búsqueda más rápida.
- Todos los productos unificados en una sola base de datos.
- Ofrece servicios a medida.

TABLA V

Características del software forense ACCESS DATA (FTK) IMAGER.

Tipo de software	Clientes habituales	Tipo de Implementación	Idiomas Admitidos
Versión Gratuita ✗	Trabajadores autónomos(1 persona) ✓	Basado en Nube ✗	Ingles
Versión de pago ✗	Empresa Pequeña (2-50) ✓	Local ✓	
	Empresa Mediana (51 - 500) ✓		
	Empresa Grande (500 o más) ✓		

Nota: Características fundamentales del software Access Data FTK. Fuente: tomado [48].

- X-WAYS: X-Ways Forensics es una herramienta de análisis forense digital diseñada para ayudar a los investigadores a recuperar y examinar datos de dispositivos electrónicos. Esta herramienta avanzada ofrece una variedad de características como el análisis de discos duros, la recuperación de archivos borrados, la visualización de metadatos y la identificación de patrones y relaciones entre datos. Con X-Ways Forensics los investigadores pueden examinar dispositivos electrónicos con un alto grado de precisión y encontrar pruebas digitales relevantes para sus investigaciones; estas herramientas son ampliamente utilizada por investigadores forenses y agencias gubernamentales en todo el mundo [49].

CARACTERISTICAS PRINCIPALES:

- Capacidad de creación de imágenes de disco.
- Recuperación avanzada de archivos.
- Análisis de metadatos.
- Análisis de línea de tiempo.
- Búsqueda y filtrado de palabras claves.

TABLA VI

Características del software forense X-WAYS FORENSICS.

Tipo de software	Clientes habituales	Tipo de Implementación	Idiomas Admitidos
Versión Gratuita ✗	Trabajadores autónomos(1 persona) ✓	Basado en Nube ✗	Multilenguaje
Versión de pago ✓	Empresa Pequeña (2-50) ✓	Local ✓	
	Empresa Mediana (51 - 500) ✓	Portable ✓	
	Empresa Grande (500 o más) ✓		

Nota: Características fundamentales del software forense X-WAYS FORENSICS. Fuente: tomado [49].

- OSForensics: OSForensics es una herramienta de análisis forense digital diseñada para ayudar a los investigadores a analizar, examinar datos de dispositivos electrónicos y sistemas operativos; esta herramienta avanzada ofrece una amplia gama de características como el análisis de discos duros, la recuperación de archivos borrados, la identificación de contraseñas y la búsqueda de archivos ocultos y eliminados. Con OSForensics los investigadores pueden examinar dispositivos electrónicos, sistemas operativos con alta precisión, encontrar evidencia digital y realizar investigaciones más eficientes. Además, OSForensics puede analizar una amplia variedad de sistemas operativos incluidos Windows, Mac y Linux; lo que la convierte en una herramienta versátil para investigadores de diferentes áreas [50].

CARACTERISTICAS PRINCIPALES:

- Análisis de discos duros.
- Análisis de sistemas operativos.
- Identificadores de contraseñas.
- Análisis de metadatos.
- Búsqueda avanzada.

TABLA VII

Características del software OSForensics.

Tipo de software	Clientes habituales	Tipo de Implementación	Idiomas Admitidos
Versión Prueba ✓	Trabajadores autónomos(1 persona) ✓	Basado en Nube ✗	Multilenguaje
Versión de pago ✓	Empresa Pequeña (2-50) ✓	Local ✓	
	Empresa Mediana (51 - 500) ✓	Portable ✓	
	Empresa Grande (500 o más) ✓		

Nota: Características fundamentales del software forense X-WAYS FORENSICS. Fuente: tomado [50].

En la actuación pericial se define el proceso de extracción característico bajo las normas ISO 27037:2012 y su debido tratamiento a la hora de hacer una extracción en diferentes unidades de almacenamiento, bajo el principio de la triada de seguridad, integridad y disponibilidad de la información; el manejo de la información bajo este estándar es muy estricto en la cadena de custodia, ya que la evidencia digital debe ser adquirida del modo menos intrusivo posible tratando de preservar la originalidad de la prueba y en lo más seguro con prácticas de copias de respaldo de la copia original [51]. En la siguiente norma utilizaremos los principios básicos de la norma ISO 27037:

- Aplicación de métodos y procesos: La evidencia digital debe ser adquirida del modo menos intrusivo posible tratando de preservar la originalidad de la prueba y en la medida de lo posible obteniendo copias de respaldo.
- Proceso Auditable: Los procedimientos seguidos y la documentación generada deben haber sido validados y contrastados por las buenas prácticas profesionales. Se debe proporcionar trazas y evidencias de lo realizado y sus resultados.
- Proceso Reproducible: Los métodos y procedimientos aplicados deben de ser reproducibles, verificables y argumentables al nivel de comprensión de los entendidos en la materia, quienes puedan dar validez y respaldo a las actuaciones realizadas.
- Proceso defendible: Las herramientas utilizadas deben de ser mencionadas y éstas deben de haber sido validadas y contrastadas en su uso para el fin en el cual se utilizan en la actuación.

  Fases ò procesos de la Actuación pericial bajo la norma ISO 27037.

La ISO 27037 es la encargada de proporcionar las pautas o pasos que se deben tener para las actividades específicas en el manejo de la evidencia digital, en los casos de incidentes tecnológicos en los cuales se debe realizar el proceso de identificación, recopilación, adquisición y preservación digital de la información potencialmente probatoria en el incidente. Con la norma 27037 se logra brindar mayor seguridad a los sistemas o entidades con situaciones comunes donde se han encontrado vulnerabilidades en las organizaciones que afectan o comprometen su información crítica o confidencial; permitiendo así definir procesos jurídicos y disciplinarios [27].

Figura 6

Actuación pericial bajo la norma ISO 27037.

Nota. Principios básicos y etapas de la norma 27037 en un caso forense. tomado de : [51].

Para cada tipología de la norma se divide la actuación y el tratamiento en 3 procesos diferentes como modelos genéricos de tratamiento de las evidencias.

- Identificación: Es el proceso de identificación de evidencia que involucra encontrar e identificar la información o evidencia subyacente en sus posibles estados tanto físicos como lógicos dependiendo de las circunstancias de cada evidencia.
- Recolección / Adquisición: Este proceso se define como la recolección de equipos y documentos que puedan contener pruebas coleccionables (Incautación ò secuestro de estos mismos) que puedan contener la evidencia que se desea recopilar o bien la adquisición y copia de la información existente en los dispositivos.
- Conservación / Preservación: La evidencia ha de ser preservada para garantizar su utilidad, es decir, su originalidad para que a posteriori pueda ser ésta admisible como elemento de prueba original e íntegra, por lo tanto, las acciones de este proceso están claramente dirigidas a conservar la cadena de custodia, la integridad y la originalidad de la prueba.

Para la aplicabilidad de practica de la norma en las actuaciones periciales se debe tratar la recopilación y captura de evidencias desde un punto de vista global, abarcando como punto primordial el incidente de seguridad o por una violación de esta en los casos reales de la cotidianidad; no en todos los procesos judiciales es viable ni recomendable por lo que la norma en particular y su aplicabilidad dependen de la circunstancia y de la actividad realizada. Por este motivo a la hora de llevar a cabo una actuación de captura de evidencias se ha de tener en cuenta las características principales de la información que se desea recopilar, es decir, cuál es la naturaleza de la evidencia que se desea recopilar y cuál es la mejor forma o vía de actuación que garantice el éxito de esta, para ello se debería elaborar un protocolo de actuación adecuado para cada caso específico.

ADQUISICION DE IMAGENES FORENSE BAJO EL ESTANDAR ISO 27037

Es de aclarar que para darle solución al problema planteado en esta monografía se identificaron los siguientes estándares ISO 27037 Y norma BS 10008:2008 debido a que se acomodan y orientan perfectamente en la solución de dicho problema.

En este sentido se describen las generalidades de los procesos a seguir:

- Identificación: La fase de identificación consiste en recolección y documentación de forma digital para el análisis forense de esa información extraída de forma digital, en esta etapa de la norma se determina la naturaleza y el alcance del incidente; donde se identifican las fuentes de las evidencias más relevantes y se establecen pautas para su respectiva preservación y adquisición, además de definir los objetivos del análisis forense y evaluando sus riesgos y utilización de recursos necesarios.

- Adquisición: La fase de adquisición se enfoca en la obtención de la evidencia digital de manera forense y confiable, en esta etapa se utilizan técnicas y herramientas especializadas para adquirir copias de datos relevantes, garantizando su integridad y preservando la cadena de custodia, se definen también protocolos y procedimientos para la recolección de dicha evidencia, además de identificar la fuente de la información y realizar copias forenses de los dispositivos afectados y sus sistemas se registran sus metadatos para ser verificados en la etapa de conservación y que se conserve la integridad de una investigación forense.

- Conservación: La fase de conservación se centra en preservar y proteger la evidencia digital adquirida durante el proceso forense, en esta etapa se utilizan técnicas que garantizan la Integridad, Autenticidad, y Confidencialidad de la evidencia, se establecen controles de acceso a dicho almacenamiento seguro para prevenir las alteraciones o manipulaciones no autorizadas y nuestras pruebas forenses conservadas no sean descartada en un caso judicial, implementando técnicas de cifrado y manteniendo los registros detallados de todas las acciones realizadas sobre dicha evidencia, donde se prioriza la cadena de custodia.

A continuación, se va a realizar la adquisición estática en caliente no volátil de 2 unidades de almacenamiento, en concreto de un disco duro SSD y HDD mediante FTK Imager y OSForensic donde se analizarán y verificarán que su estado sea correcto en HASH y no se encuentre vulnerada la cadena de custodia y esta sea preservada y las imágenes virtualizadas estén intactas y no adulteradas con sus respectivas imágenes virtualizadas del sistema operativo Ubuntu.

- Que el equipo pertenece a un sistema critico o vulnerado su sistema que se mantuvo encendido de manera ininterrumpida y se vulnero.

- Que nuestro dispositivo se encuentro no cifrado o algún proceso de encriptación de la información vulnerada, porque si lo esta puede ser una forma imposible de adquirir nuestra imagen forense en frio.

Que el equipo se encuentre expuesto a ataques desde el exterior, lo que hace que nuestras evidencias se alteren durante la adquisición en caliente etc.

6.0 PREPARACIÓN DEL ESCENARIO PARA LA EXTRACCIÓN FORENSE.

En este apartado se mencionarán los requerimientos mínimos de equipos, Hardware y software además de los requerimientos esperados para el funcionamiento de los procedimientos actual y esperados en cuanto a sus resultados.

EQUIPO.

- Sistema operativo Windows 10 pro.
- Procesador AMD ryzen 5 5500 x64 sin gráficos integrados.
- 16 gb de ram ddr4 3200 mhz.
- Tarjeta gráfica gtx 1050 ti.
- Board

HARDWARE:

- Adata nv620s 1tb hdd para almacenamiento de evidencias.
- Hitachi 500 gb hdd
- Kingston 480 gb ssd

SOFTWARE:

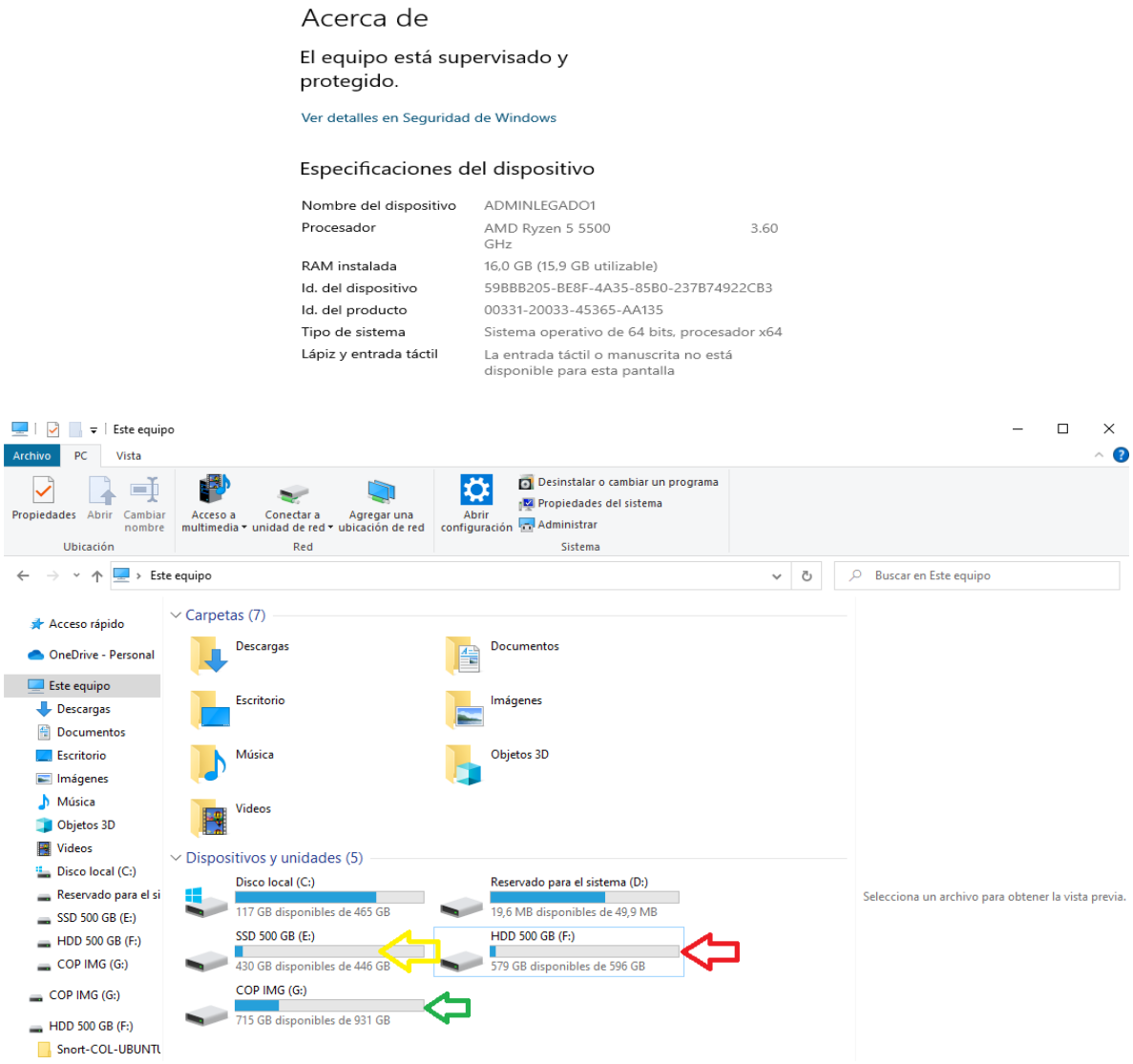
- AccessData FTK Imager
- OSForensic
- MD5_and_SHA_Checksum_Utility
- Quickhash-gui

Al cumplir con los requisitos, se puede realizar el procedimiento de extracción forense bajo las normas internacionales de pericia informática como la ISO 27031 y Bs 10003 de guardado de información digital.

6.1 ESPECIFICACIONES DE EQUIPO

Figura 7

Equipo físico principal de extracción y unidades de almacenamiento forense.



Nota: Equipo físico de extracción forense.

Disco local (C:) Unidad local donde están instalados los softwares FTKimager – OSForensics y nuestro verificador de Hash.

HDD 500GB(F:): Unidad HDD vulnerada donde se clonará y se asegurará una copia de la imagen original - “Flecha Roja”.

SSD 500 GB (E:) Unidad SSD vulnerada donde se clonará y se asegurará una copia de la imagen original - “Flecha Amarrilla”.

COP IMG (G:) Unidad de almacenamiento de imágenes clonadas - “Flecha Verde”.

Dispositivos de Hardware:

Figura 8

SSD Kingston vulnerado.

Nota: Unidad Kingston SSD examinada.

HDD 500 GB (F:) Unidad HDD vulnerada donde se clonará y se asegurará una copia de la imagen original - “Flecha Roja”.

Figura 9

HDD Hitachi vulnerado

Nota: Unidad Hitachi SSD examinada.

COP IMG (G:) Unidad adata donde se guardarán las copias y la copia original de cada imagen forense del SSD y HDD – “Flecha Verde”.

Figura 10

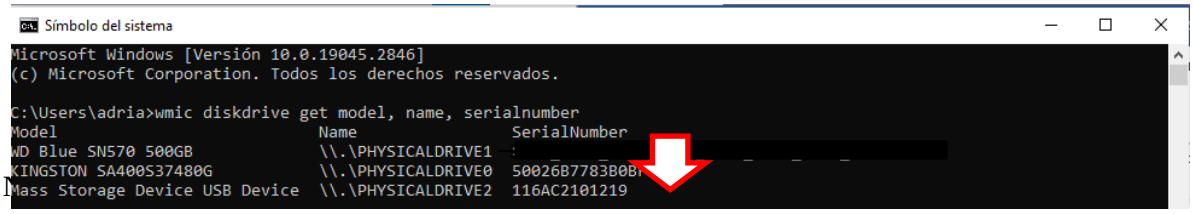
Unidad de copias digitales.

Nota: Unidad de almacenamiento de copias de seguridad del clonado de las imágenes Forenses.

Se procede a hacer un escaneo de los dispositivos conectados por nuestra caja portable para ver los seriales de nuestros dispositivos.

Figura 11

Nombre del dispositivo analizado.

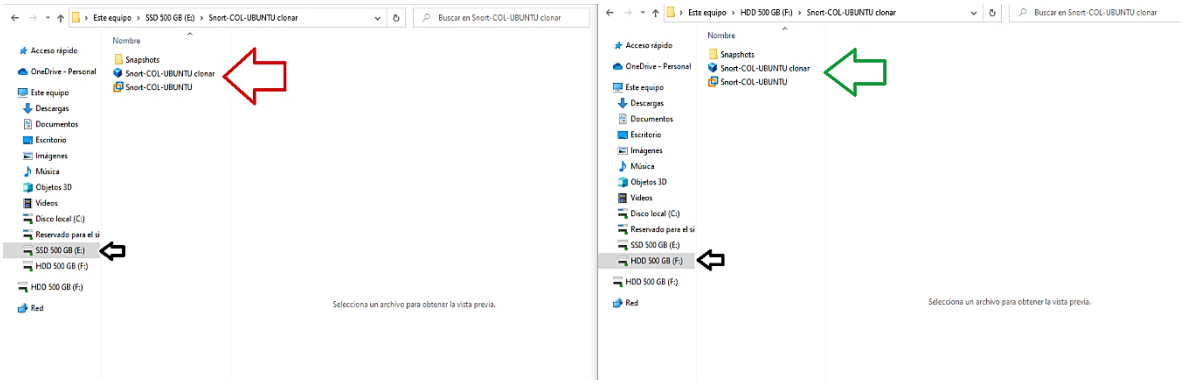


Nota. Características modelos y tipo de serial de dispositivos conectados a nuestra maquina local.

6.2 ADQUISICION DE EVIDENCIA DIGITAL HDD Y SSD CON LA HERRAMIENTA FTKImager.

Figura 12

Unidades examinadas



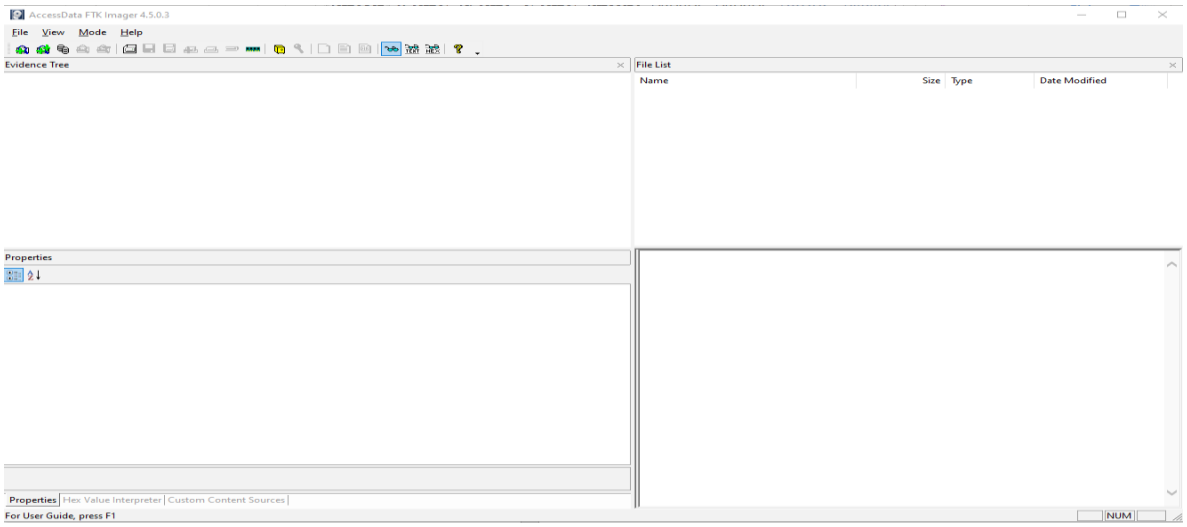
Nota**:** Unidades de almacenamiento conectadas a nuestra máquina auditor.

Creamos nuestra imagen de disco.

Después de realizar la descarga del instalador desde el sitio web oficial de AccessData y proceder con la instalación del programa, se apertura FTK Imager.

Figura 13

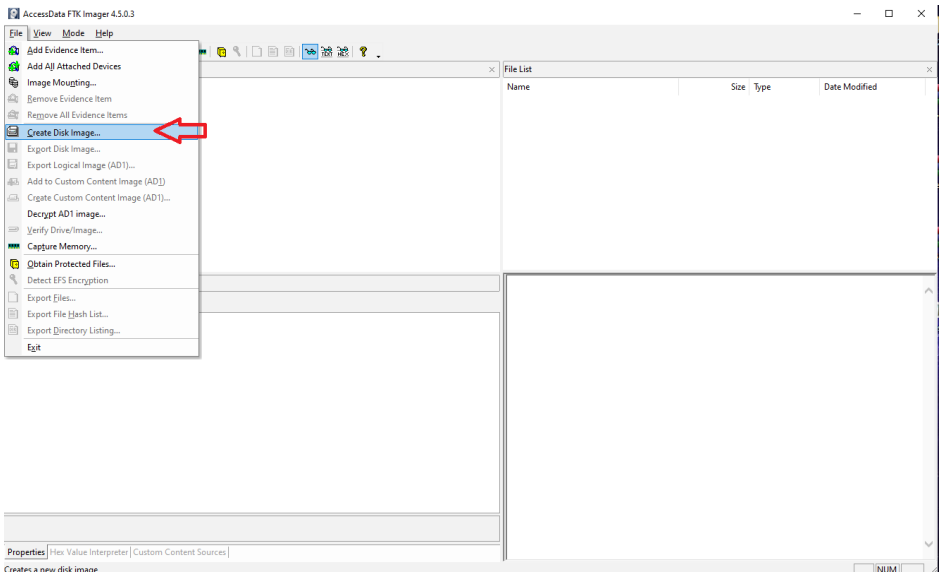
Inicio de software AccesData FTK Imager



Hacemos clic en la opción “File -> Create Disk Image” o Archivo -> Crear Imagen de Disco.

Figura 14

Creación de imagen física.

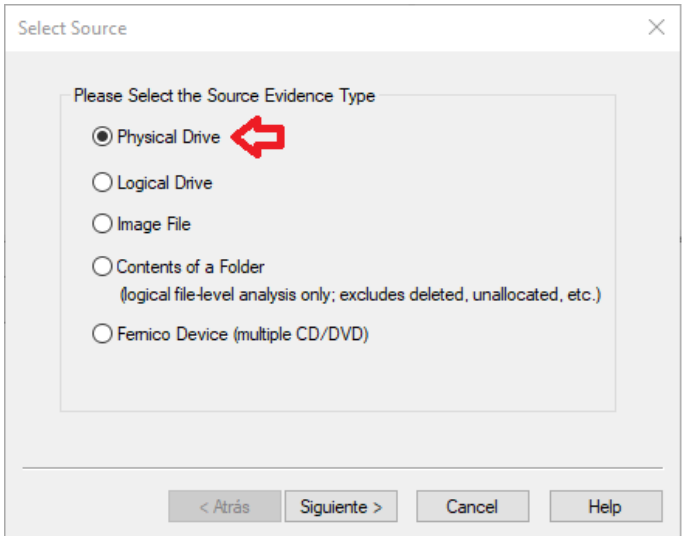


Nota: Proceso Adquisición forense en ambas unidades paso 1.

Se presentará una nueva ventana donde se requiere definir la Fuente.

Figura 15

Selección de unidad Physical Drive.

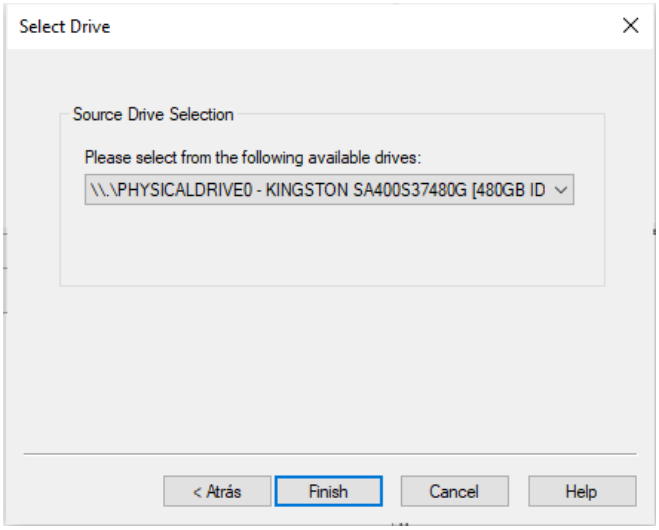


Nota: Proceso Adquisición forense en ambas unidades paso 2.

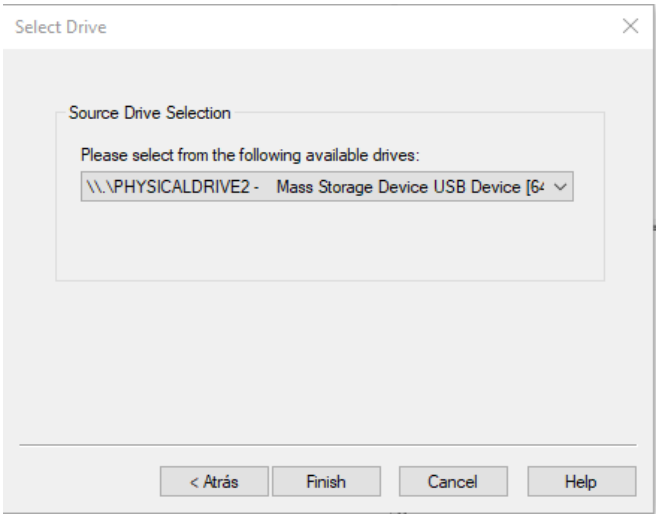
En una nueva ventana se muestra un menú desplegable, en el cual se selecciona la Unidad Fuente correspondiente, para luego hacer clic en el botón “Finish” o Finalizar.

Figura 16

Selección de unidad HDD y SSD.



Nota: Unidad SSD paso 3.

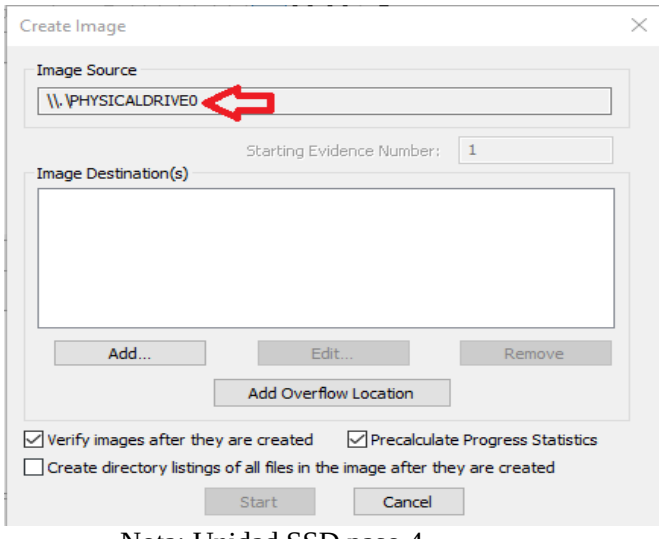


Nota: Unidad HDD paso 3.

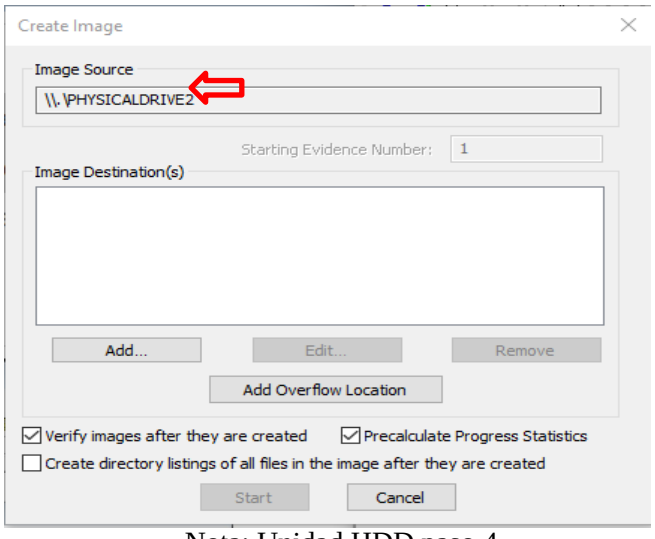
La siguiente ventana permite definir un Destino para la Imagen. Para esto es necesario hacer clic en el botón “Add...”

Figura 17

Destino de la Imágenes forenses.



Nota: Unidad SSD paso 4.

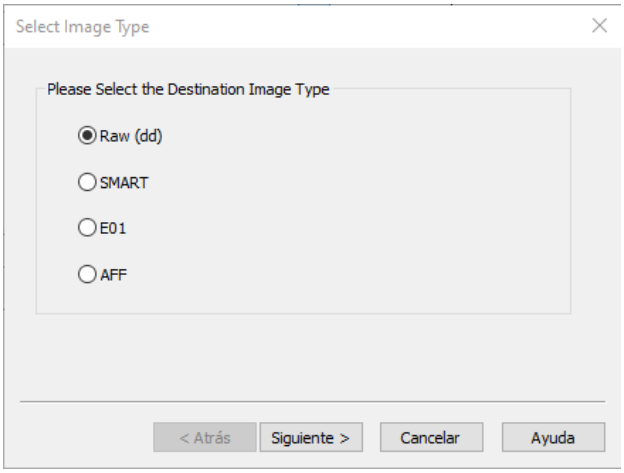


Nota: Unidad HDD paso 4.

En esta ventana se define el tipo de la imagen de destino a crear. Para el caso de la presente práctica será una imagen “Raw” o en bruto, es decir tal y como sería creada utilizando una herramienta como dd o dcfldd.

Figura 18

Tipo de imagen Forense Formato RAW.

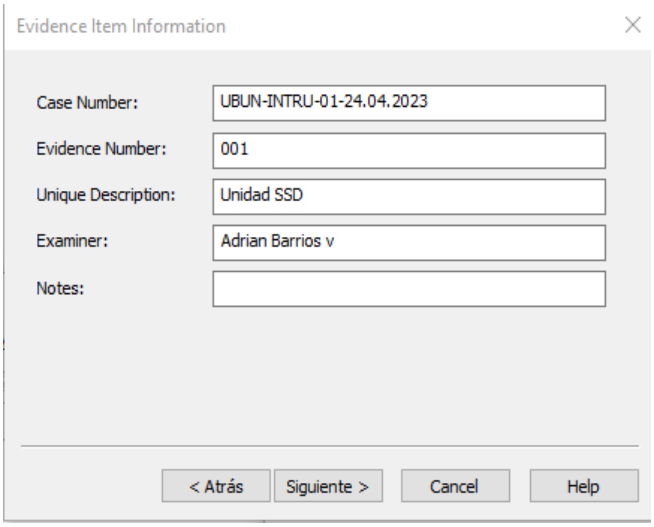


Nota: Formato de imagen a extraer.

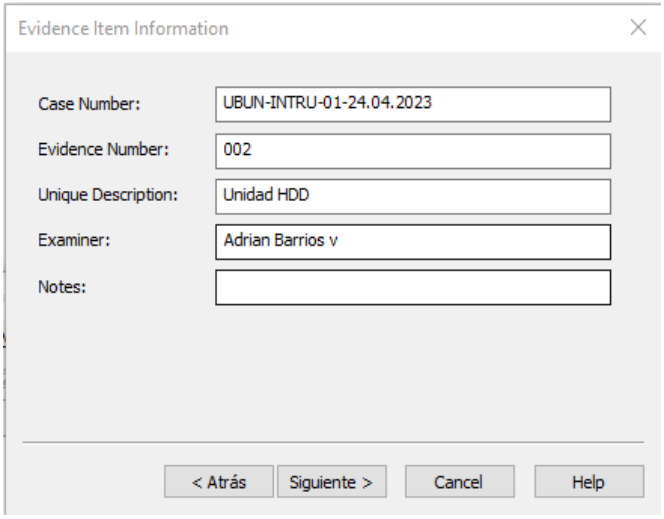
En la siguiente ventana solicita ingresar información sobre el ítem de evidencia.

Figura 19

información de evidencias



Nota: información del de evidencias por el perito informático paso 5.

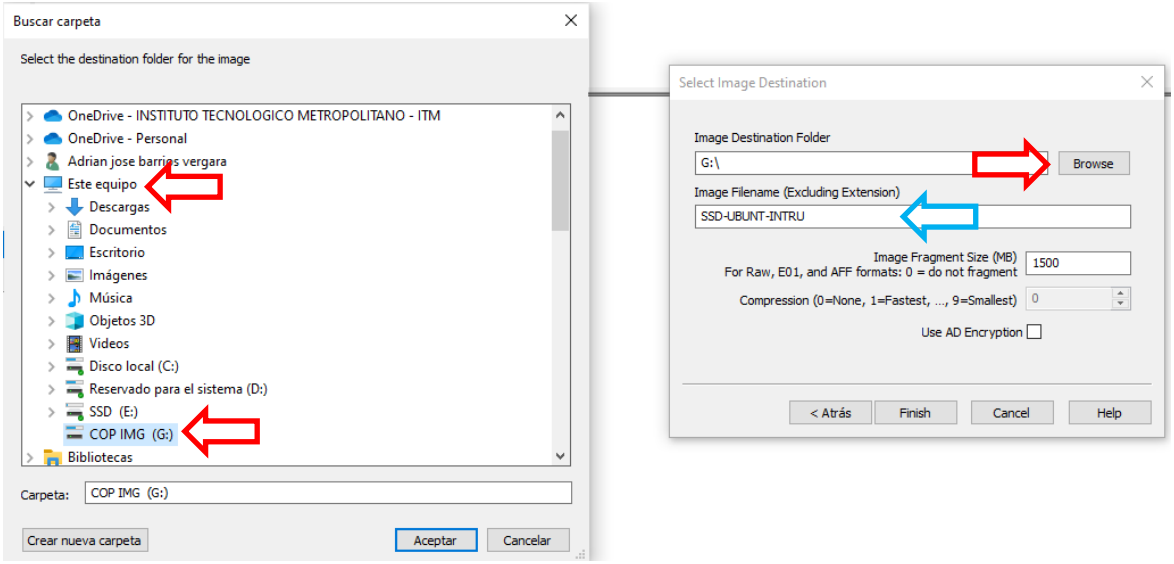


Nota: información del de evidencias por el perito informático paso 5.

Se definen las carpetas donde se almacenarán las imágenes forenses en la siguiente Ruta de mi unidad de respaldo G:\ . La cual es seleccionada haciendo clic en el botón “Browse” o Navegar.

Figura 20

Ruta de destino de Imágenes Forenses

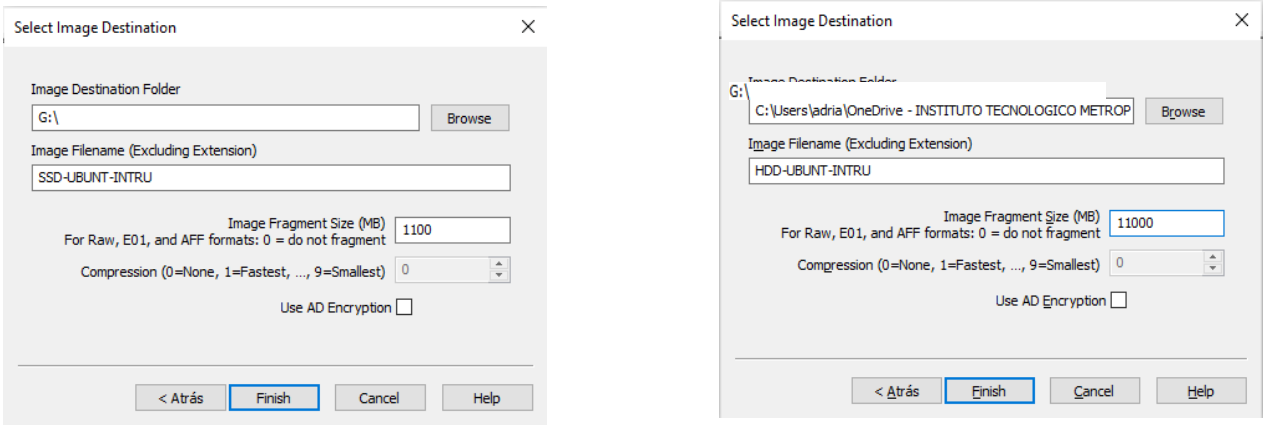


Nota: Ruta ò Localización de guardado de nuestra imagen a extraer paso 6.

A continuación, se requiere nombrar la imagen forense (Unidad SSD O HDD) flecha azul. Y opcionalmente definir si la imagen resultante será dividida en varias partes o sino no será fragmentada. Para el caso de la presente práctica será divida, por lo tanto, se define el valor “11000” en el campo “Image Fragment Size (MB)” o Tamaño del Fragmento de la Imagen.

Figura 21

Destino de imagen forense.

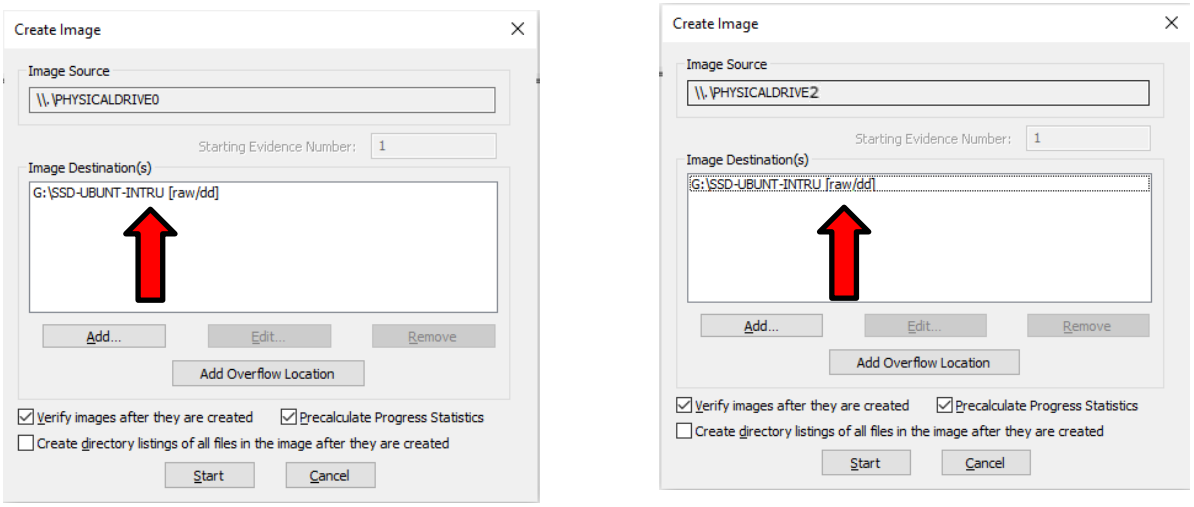


Nota: Ubicación de nuestra imagen SSD y HDD paso 7.

Al hacer clic en el botón “start” se mostrará un resumen de las opciones seleccionadas e iniciará nuestra clonación forense.

Figura 22

Configuración final

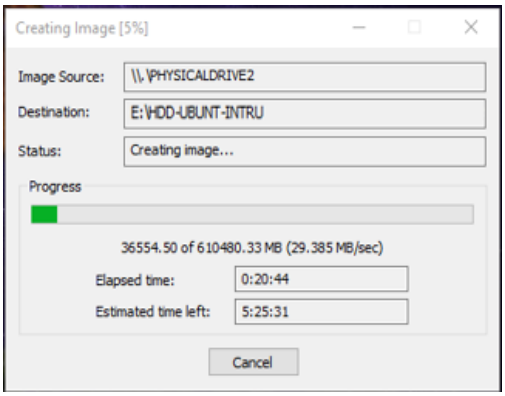


Nota: Configuración de guardado antes de iniciar copia en ambas unidades SSD y HDD paso 8.

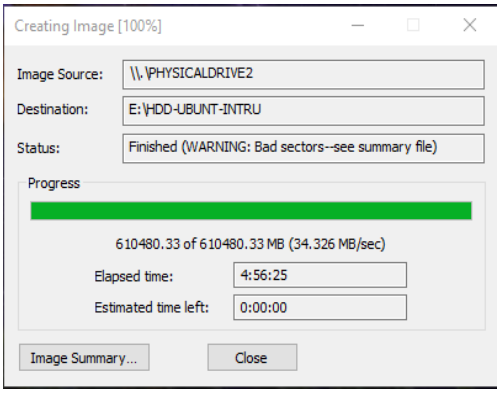
Después de hacer nuestra extracción exitosamente se procede a clonar nuestra imagen en la unidad. COP IMG (G:).

Figura 23

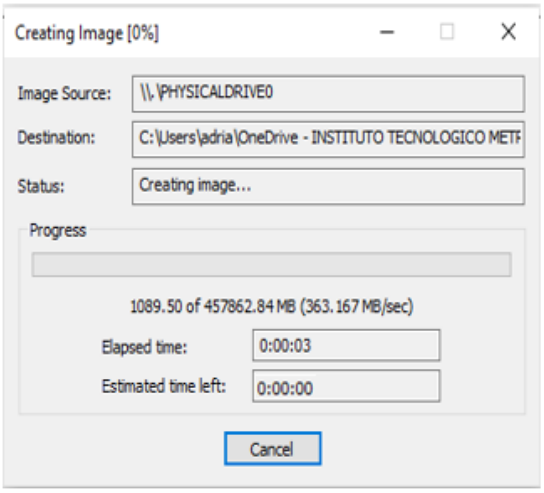
Resultados de la extracción forense SSD Y HDD



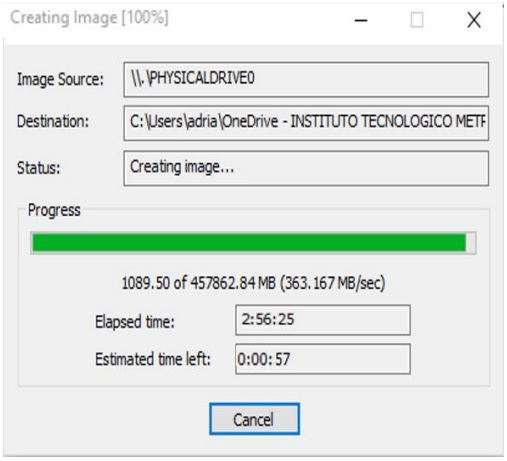
Nota. inicio de clonación copia Unidad HDD paso 9.



Nota. final de clonación copia Unidad HDD paso 9.



Nota. inicio de clonación copia Unidad SDD paso 9.

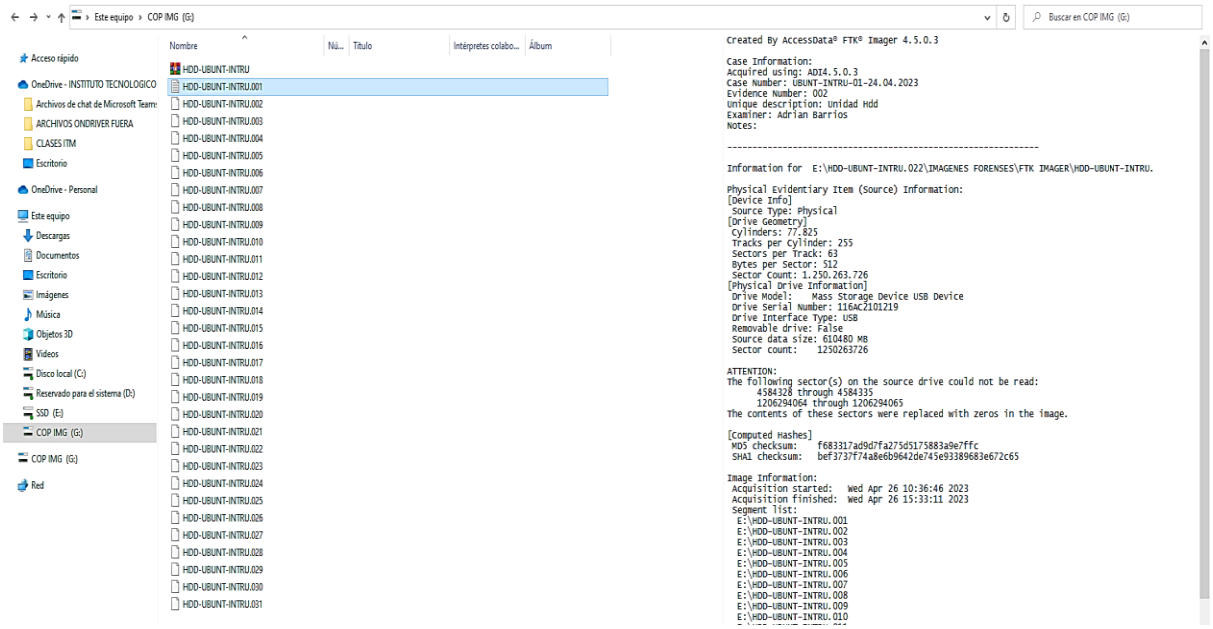


Nota. final de clonación copia Unidad SDD paso 9.

Resultados obtenidos de nuestra clonación.

Figura 24

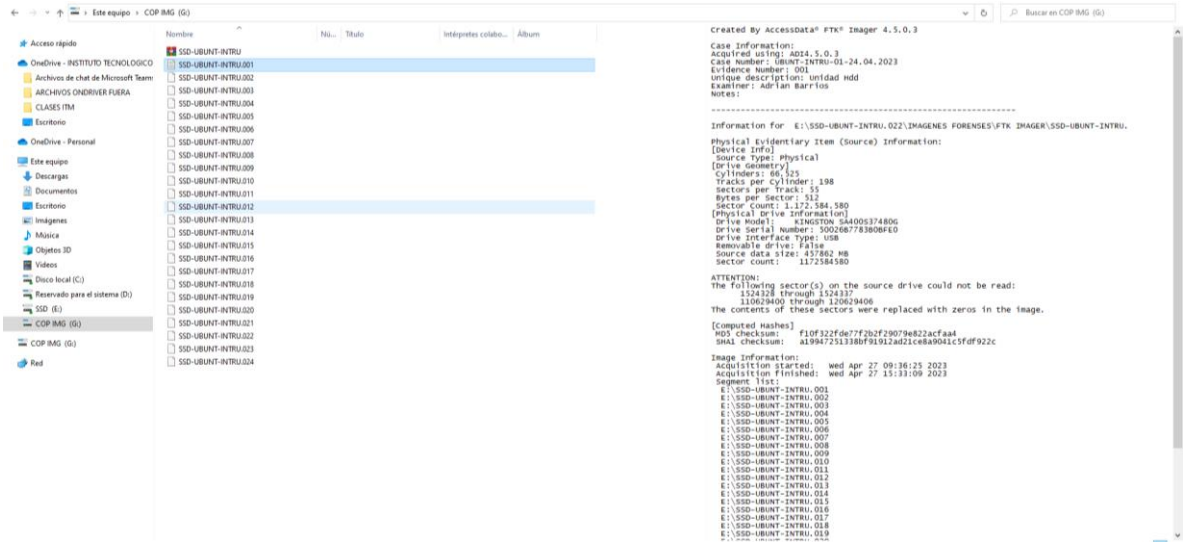
Resultado Imagen forense HDD.



Nota: Clonación exitosa verificación de Hash único paso 10.

Figura 25

Resultado Imagen forense SSD

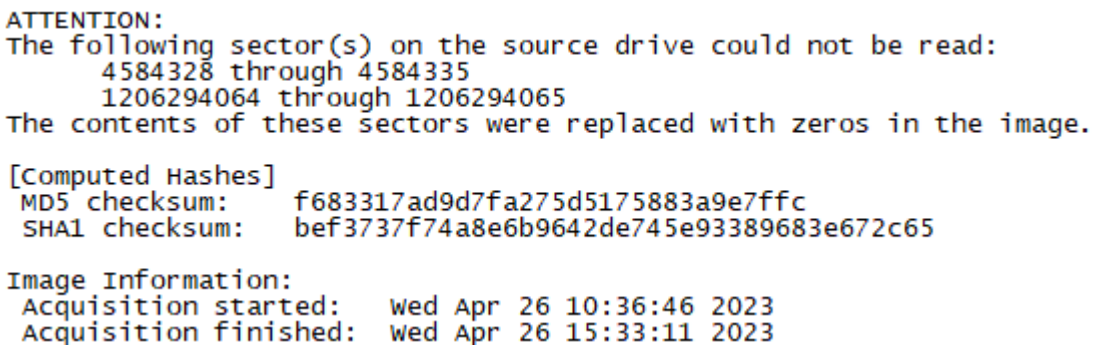


Nota: Clonación exitosa verificación de Hash único paso 10.

después de obtener nuestra clonación de la imagen verificamos el hash o identificador de nuestra copia original.

Figura 26

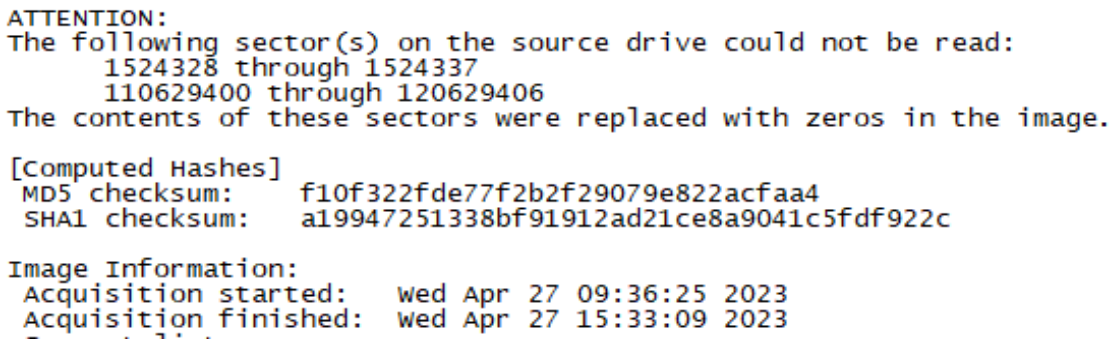
Verificación Hash copia original HDD



Nota: verificación de hash y errores de atención en sectores de nuestra clonación.

Figura 27

Verificación Hash copia original SSD



Nota: verificación de hash y errores de atención en sectores de nuestra clonación.

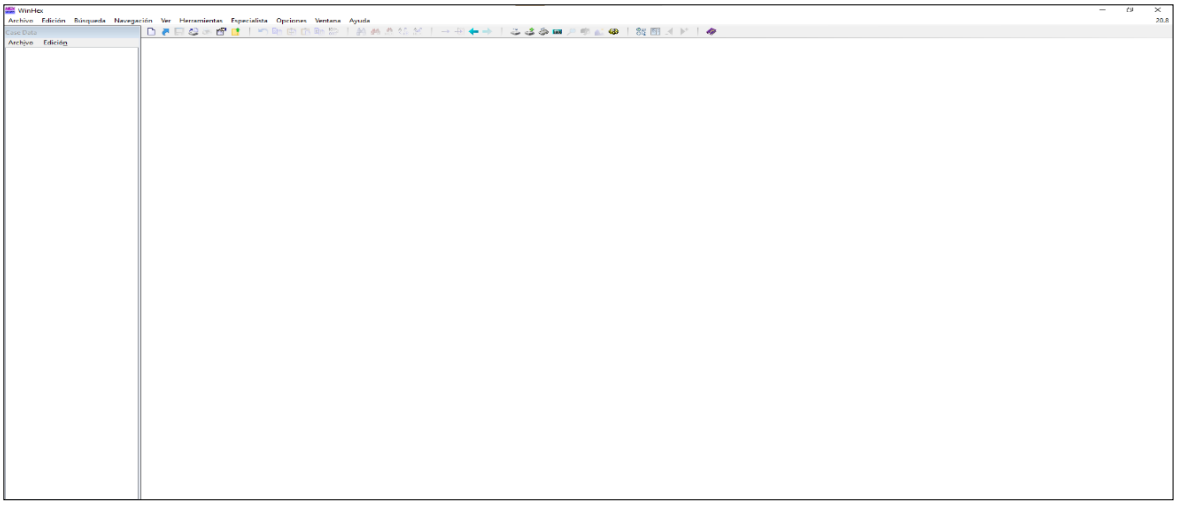
6.3 CLONADO FORENSE DE LA IMÁGEN ORIGINAL.

Existen múltiples software, Hardware y dispositivos de bloqueado de escritura para el proceso de clonado de imágenes forenses como Duplicadora Ditto DX Forensic, Velociraptor Forensic Station V3,V5,V7, Logicube WritheProtect Bay entre otros, de todas las herramientas disponibles seleccionamos nuestro software WINHEX con el que realizaremos el clonado de nuestras imágenes virtuales en ambas unidades con el fin de ser lo menos intrusivos y vulnerar la cadena de custodia.

Iniciamos nuestro software de clonado de imágenes virtuales llamado WINHEX descargamos y ejecutamos

Figura 28

Clonado de imágenes HDD y SSD 0.

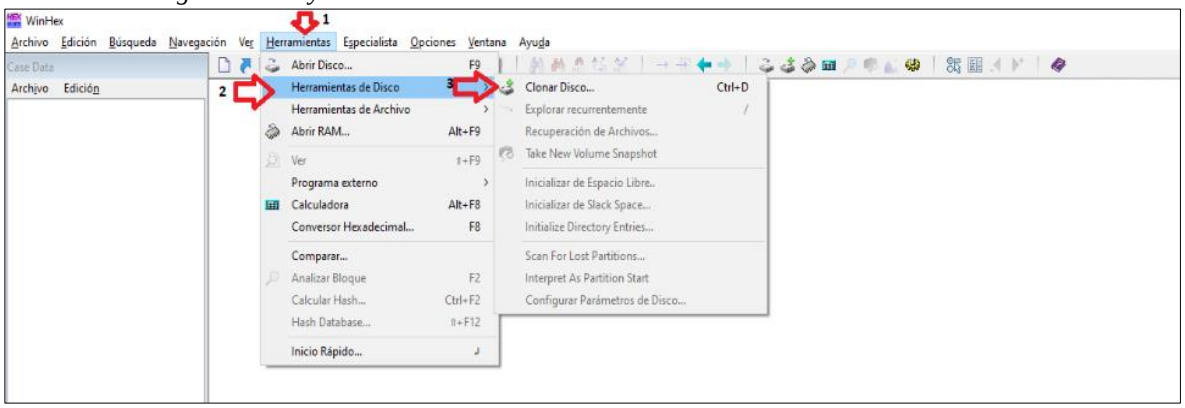


Nota. Software de clonado WinHex.

Clic en el menú herramientas, herramientas de disco, Clonar Disco.

Figura 29

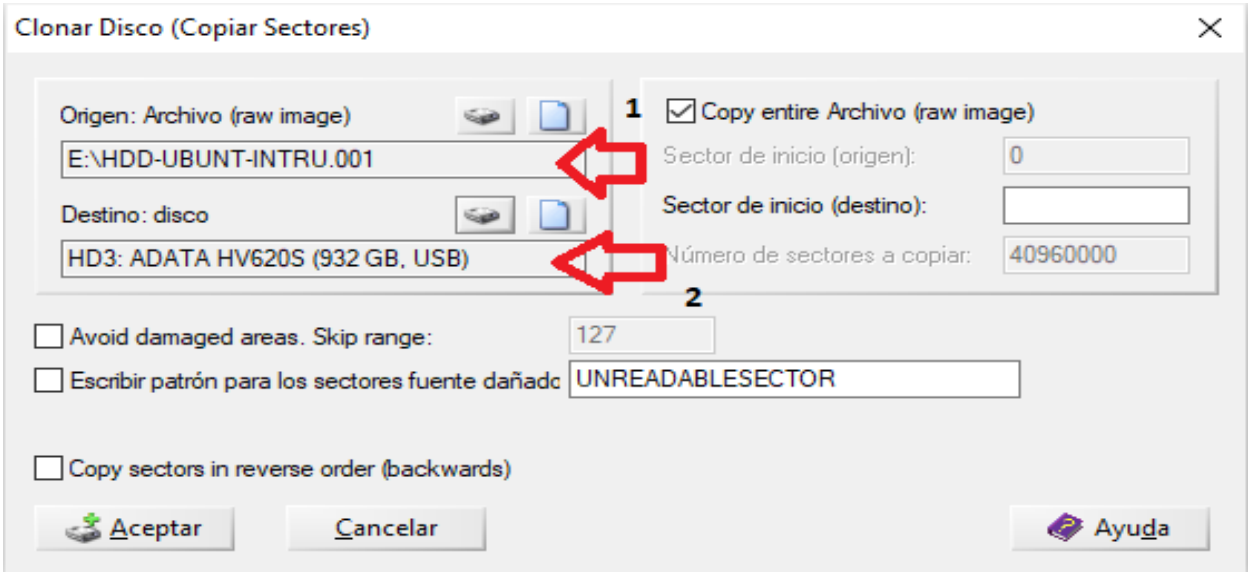
Clonado de imágenes HDD y SSD 1.



Nota: Software de clonado WinHex.

Figura 30

Selección de archivo origen y Destino WinHex

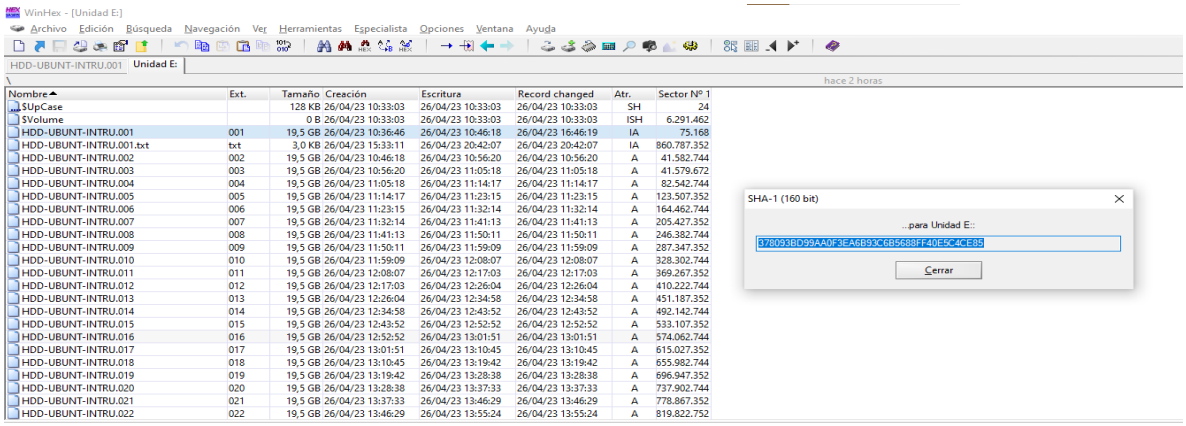


Iniciamos el clonado y guardamos la nueva copia en nuestra unidad de almacenado COP IMG (G:), 1. Origen de nuestra copia y 2. Destino de nuestra copia de clonado.

Después de tener nuestra imagen clonada y guardada en su nueva ubicación se procede a analizar la integridad de nuestra copia original en el siguiente punto.

Figura 31

Resultado de nuestro clonado forense



Nota. Resultado clonado forense.

6.4 PRESERVACION DE LA INTEGRIDAD E IDENTIDAD DE EVIDENCIAS.

Existen muchos tipos de herramientas de verificación de hash Power Shell de Windows**,** MD5 Hash generator, HashMyFiles, HashTab entre otras, con el único fin de obtener el hash del archivo y verificar la integridad de los archivos analizados para nuestro caso utilizaremos **MD5 & SHA Checksum Utility** Y **Quickhash-gui** son softwares gratuitos como también su versión paga donde nos dejan examinar sin límite de peso o longitud de los registros obtenidos de una imagen forense y si queremos obtener otros detalles más específicos esta la opción de pago.

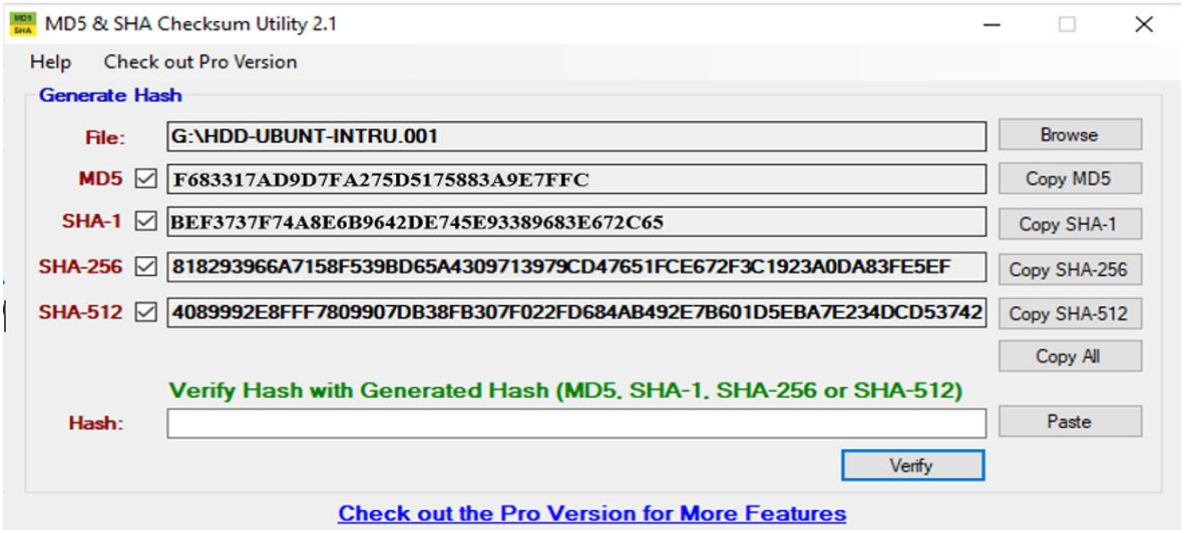
MD5 & SHA Checksum Utility: Nos permite generar y verificar los valores de resumen MD5 y SHA-1, SHA-256, SHA-384 y SHA-512 para archivos específicos. Estos resúmenes actúan como una "huella digital" única para cada archivo, lo que permite compararlos y confirmar si un archivo se ha modificado o corrompido.

Quickhash-gui: Es un software con interfaz gráfica de usuario intuitiva que facilita el cálculo de resúmenes para archivos utilizando varios algoritmos, como MD5, SHA-1, SHA-256, SHA-384, SHA-512 y CRC32. También permite comparar y verificar los resúmenes de múltiples archivos al mismo tiempo, lo cual es útil en situaciones donde se deben procesar varios archivos a la vez.

Verificamos que nuestra clonación original en nuestra figura 22 y 23 tengan el mismo hash que nuestras imágenes clonadas con WinHex.

Figura 32

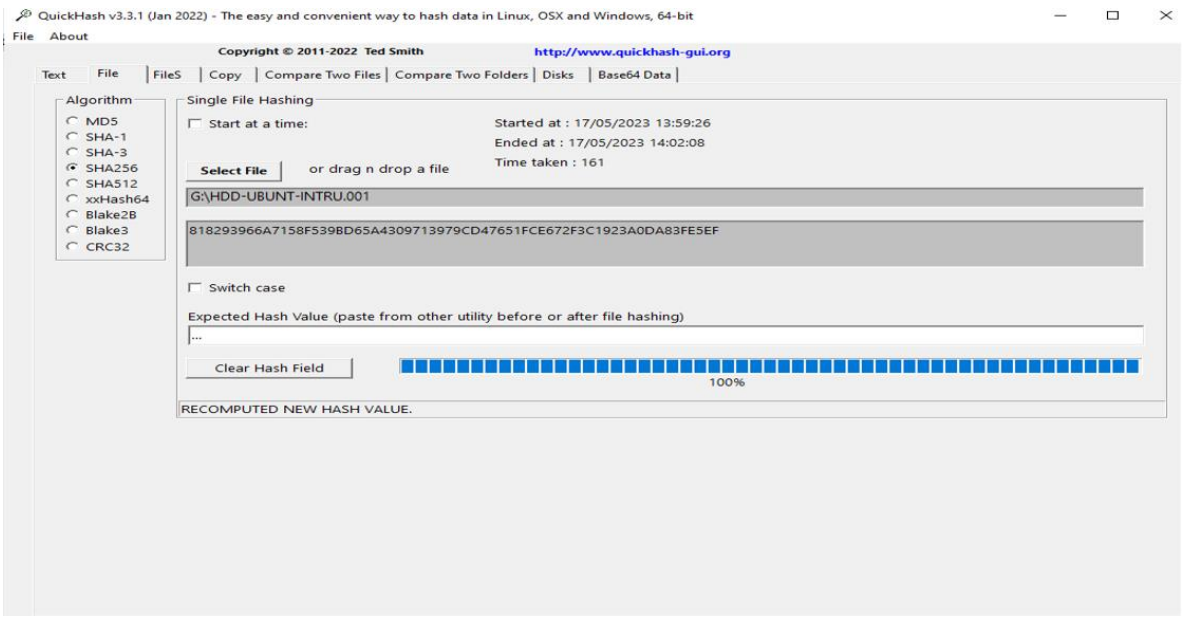
Preservación MD5 & SHA1 con la herramienta Checksum Utility a la unidad HDD.



Nota. generación de Hash con la herramienta de autenticación de la imagen forense HDD original.

Figura 33

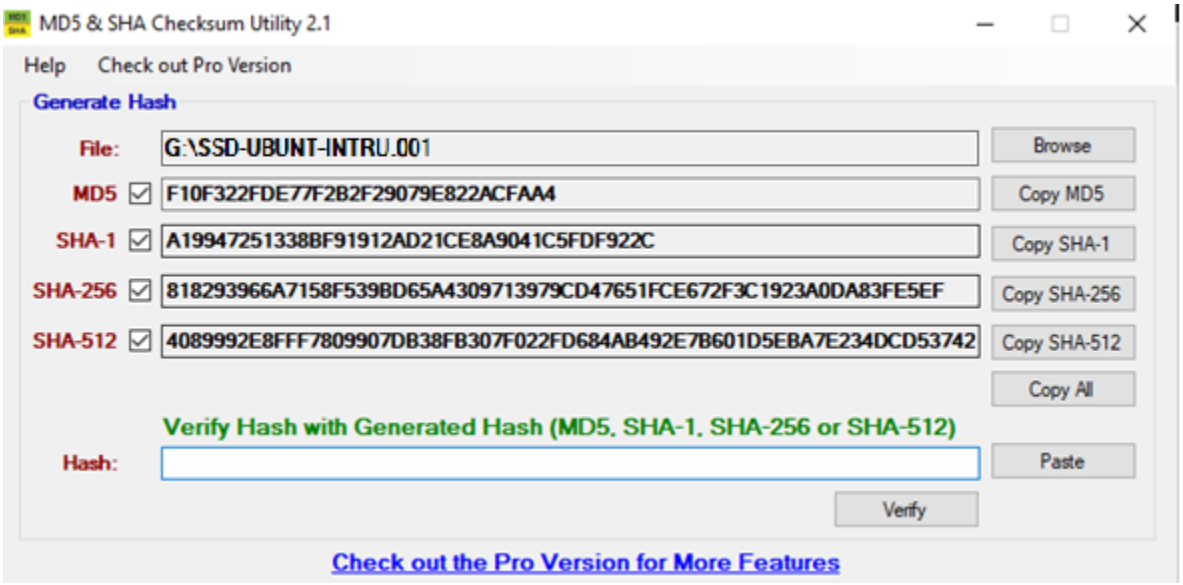
Preservación SHA256 con la herramienta Quickhash-gui a la unidad HDD.



Nota. Generación de Hash con la herramienta QuickHash a la imagen forense HDD original.

Figura 34

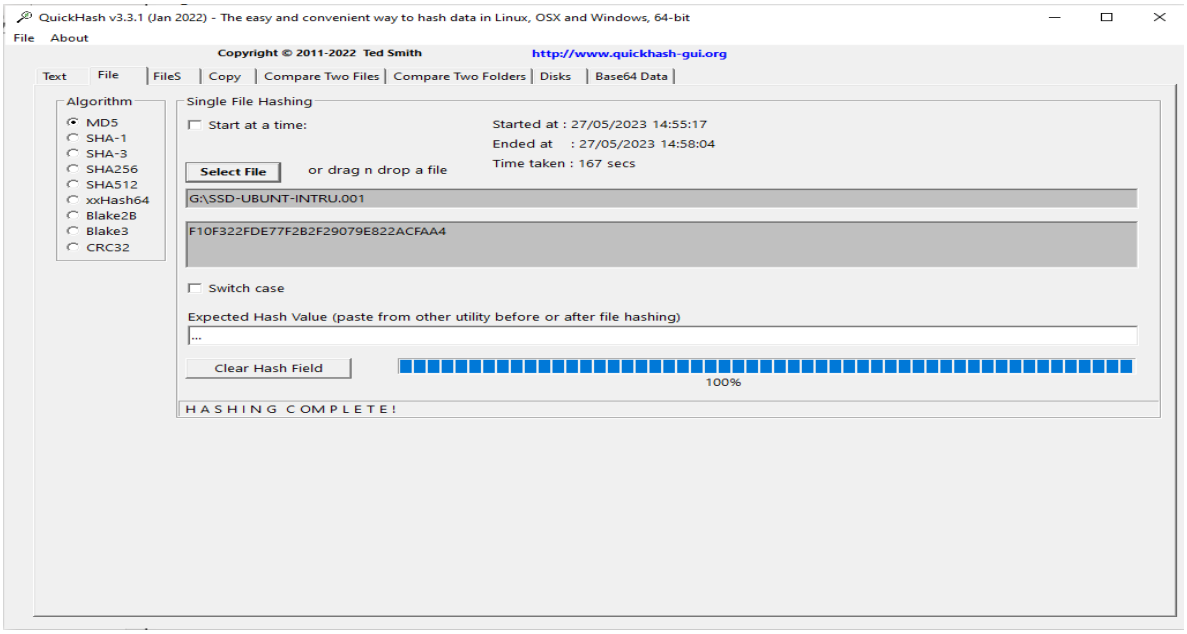
Preservación MD5 & SHA1 con la herramienta Checksum Utility a la unidad SSD.



Nota. Generación de Hash con la herramienta de autenticación de la imagen forense SSD original.

Figura 35

Preservación MD5 con la herramienta Quickhash-gui a la unidad SSD.



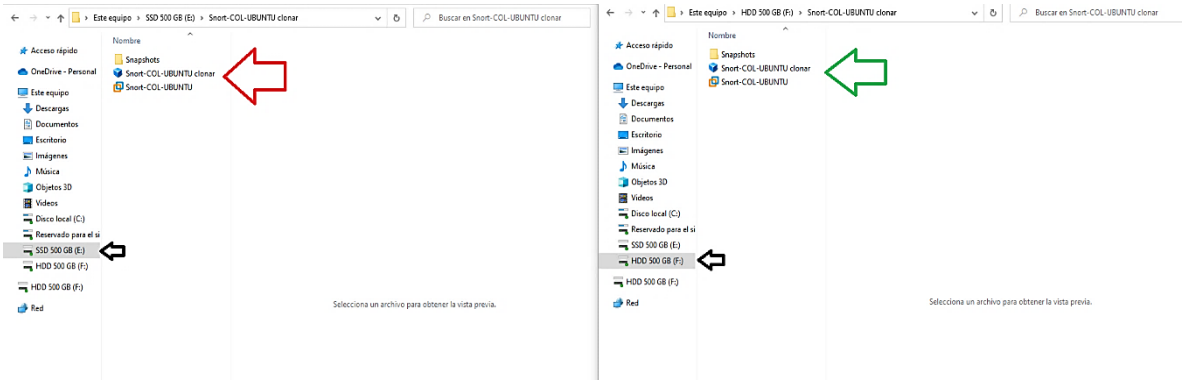
Nota. Generación de Hash con la herramienta QuickHash a la imagen forense SSD original.

6.5 ADQUISICION DE EVIDENCIA DIGITAL HDD Y SSD CON LA HERRAMIENTA OSForensics.

Antes de hacer nuestra adquisición forense con nuestra herramienta, es de tener en cuenta que, aunque existen muchas maneras de adquirir discos duros en nuestro caso para ser lo menos intrusivo con nuestras unidades analizadas verificamos que nuestro software forense no tenga interacción con nuestro disco para no interferir con nuestra extracción o alteración de la unidad examinada.

Figura 36

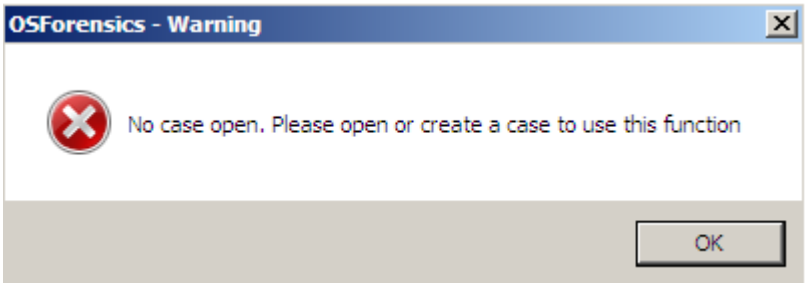
Unidades examinadas.



Nota. Unidades de almacenamiento conectadas a nuestra máquina auditor.

Figura 37

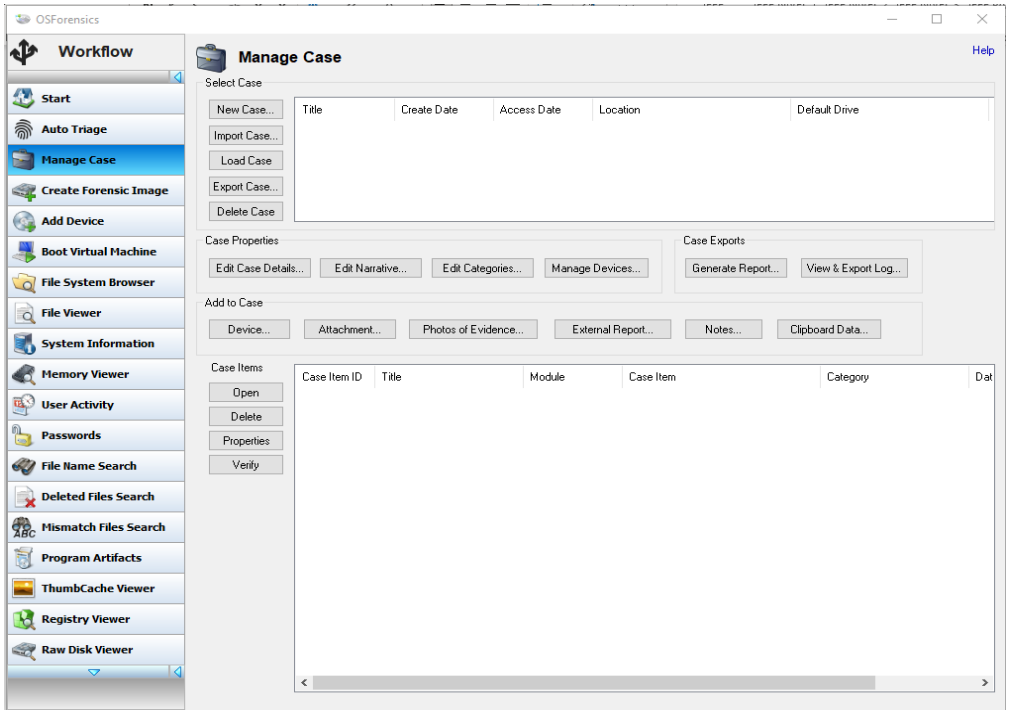
Cero Interacción con nuestras unidades HDD y SSD.



Nota. Verificación de no acceso a nuestras unidades de almacenamiento sin haber creado caso forense de dicha unidad examinada o seleccionada.

Figura 38

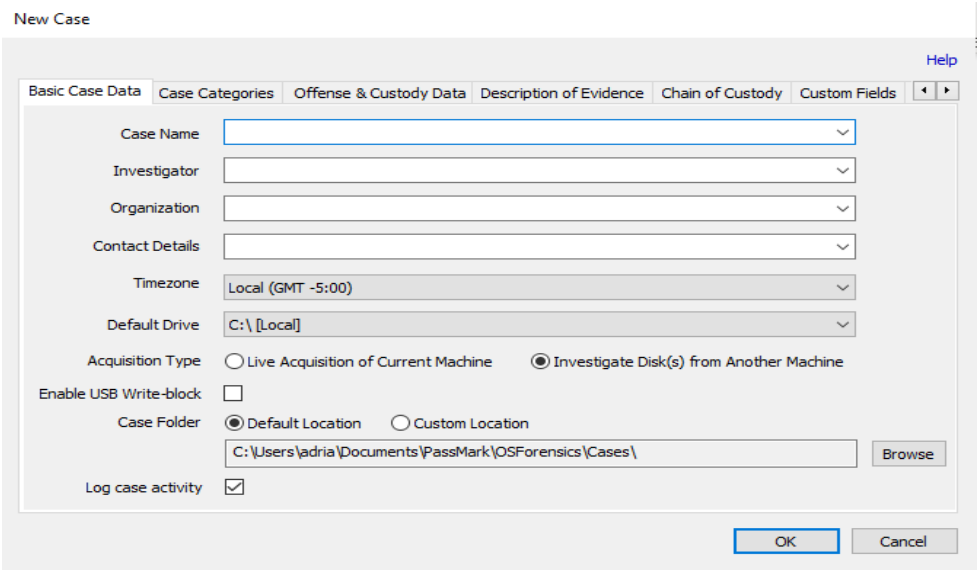
creación del caso con OSForensic



Nota. Inicio de software OSForensics.

Figura 39

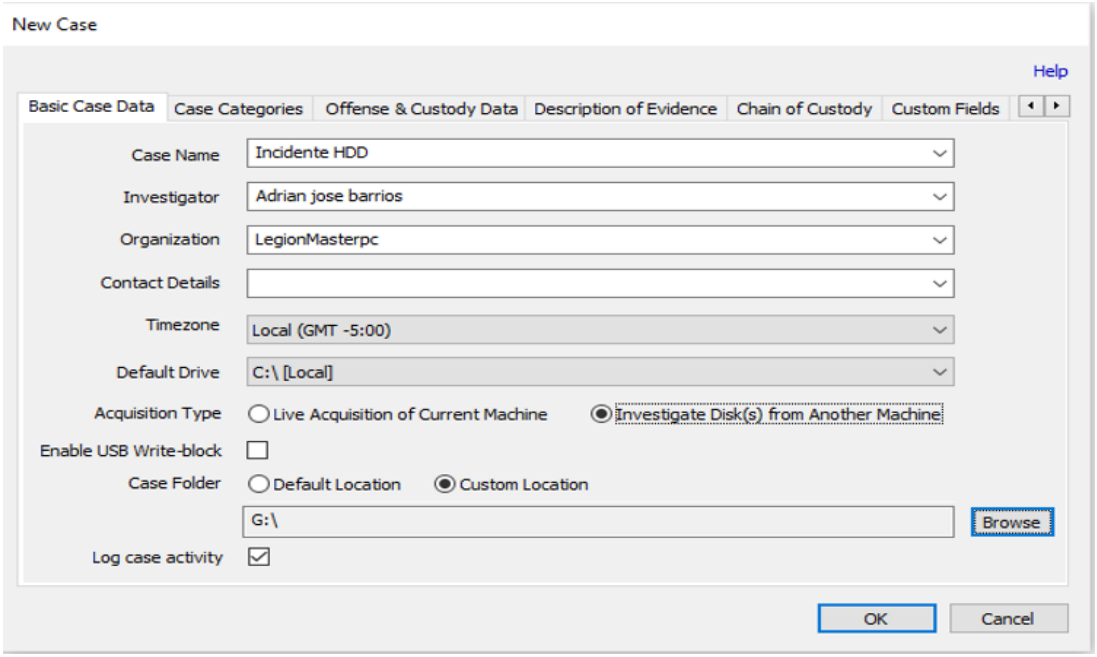
Creación del caso.



Nota. Creación del caso para la extracción forense.

Figura 40

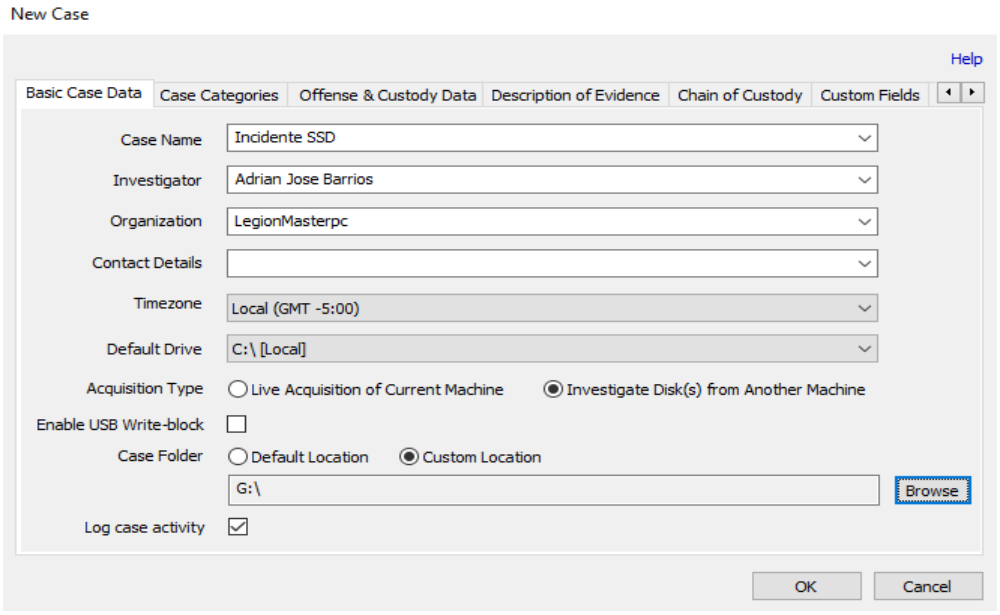
Creación de caso HDD



Nota. Ingreso de datos para la creación del caso, para tener en cuenta la zona horaria (cualquier cambio del uso horario puede provocar en un cambio en la extracción).

Figura 41

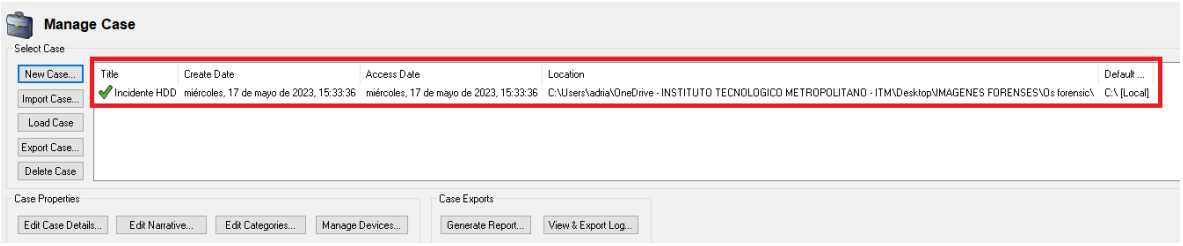
Creación de caso SSD



Nota. Ingreso de datos unidad SSD examinada.

Figura 42

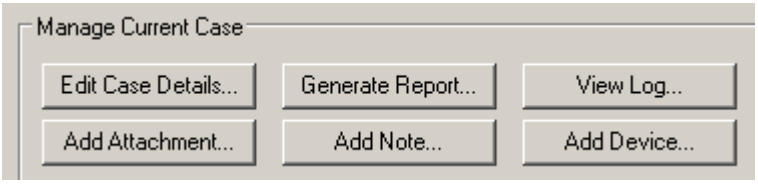
Caso creado



Luego de hacer el caso vamos al menú de “Manage Case” y agregamos nuestra evidencia para ello damos clic en Add Device.

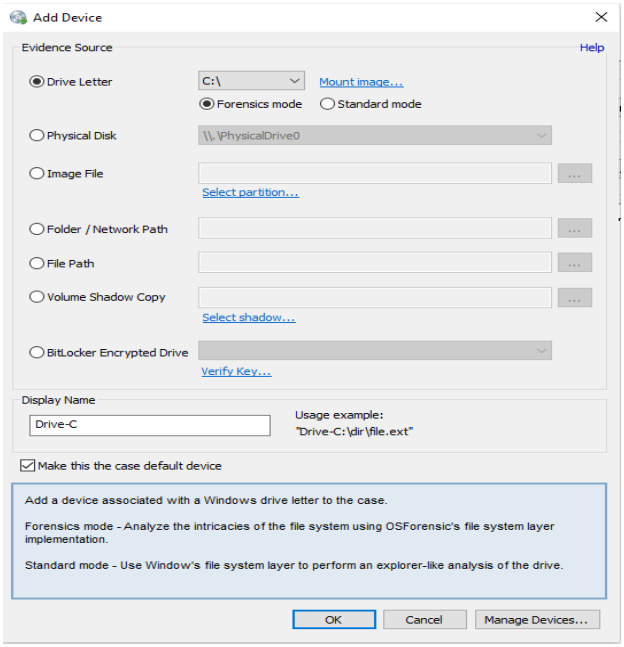
Figura 43

Administrar caso actual



Nota. Administrador de casos.

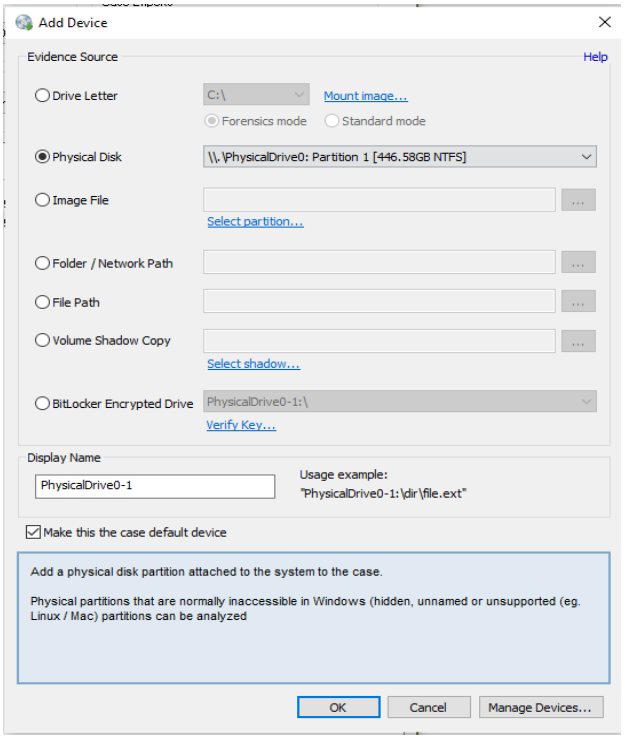
Se abrirá una nueva ventana donde seleccionaremos el tipo de evidencia que vamos a agregar al caso.



Nota. Selección de tipo de evidencias.

Figura 44

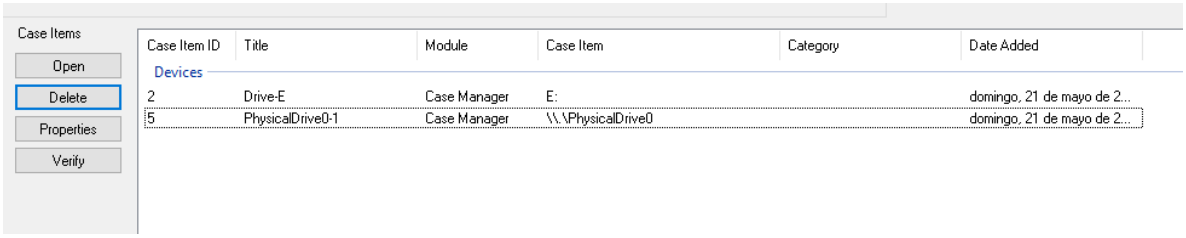
Selección de evidencia física



Nota. Selección de unidad de almacenamiento.

Figura 45

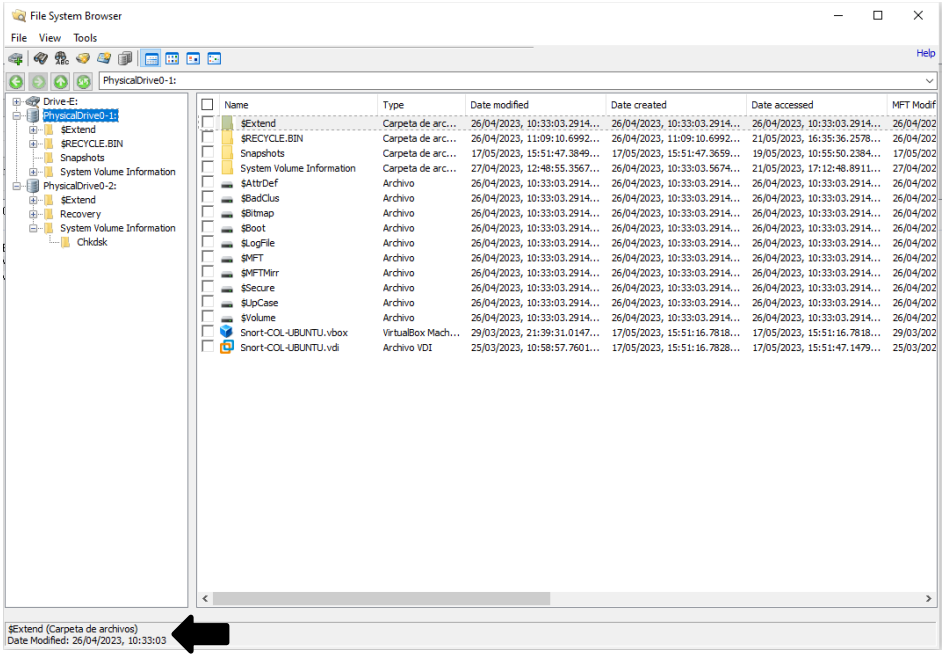
Ítem de unidades Seleccionados



Nota. Unidades físicas Hdd y SSD seleccionadas.

Figura 46

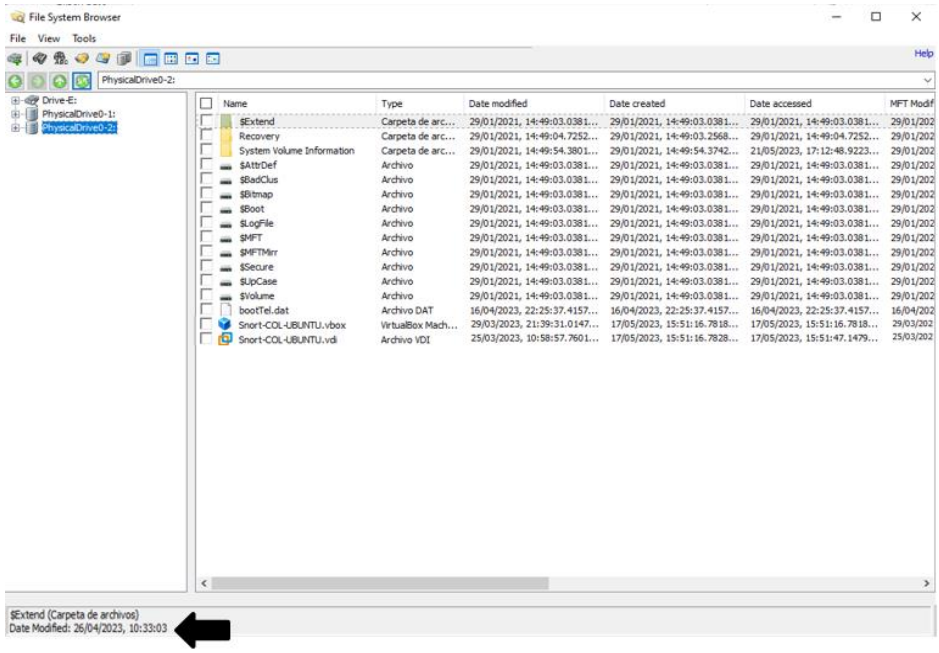
Tipo de unidad seleccionada HDD



Nota. Verificación de sistemas y archivos en unidad Hdd.

Figura 47

Tipo de unidad seleccionada SSD

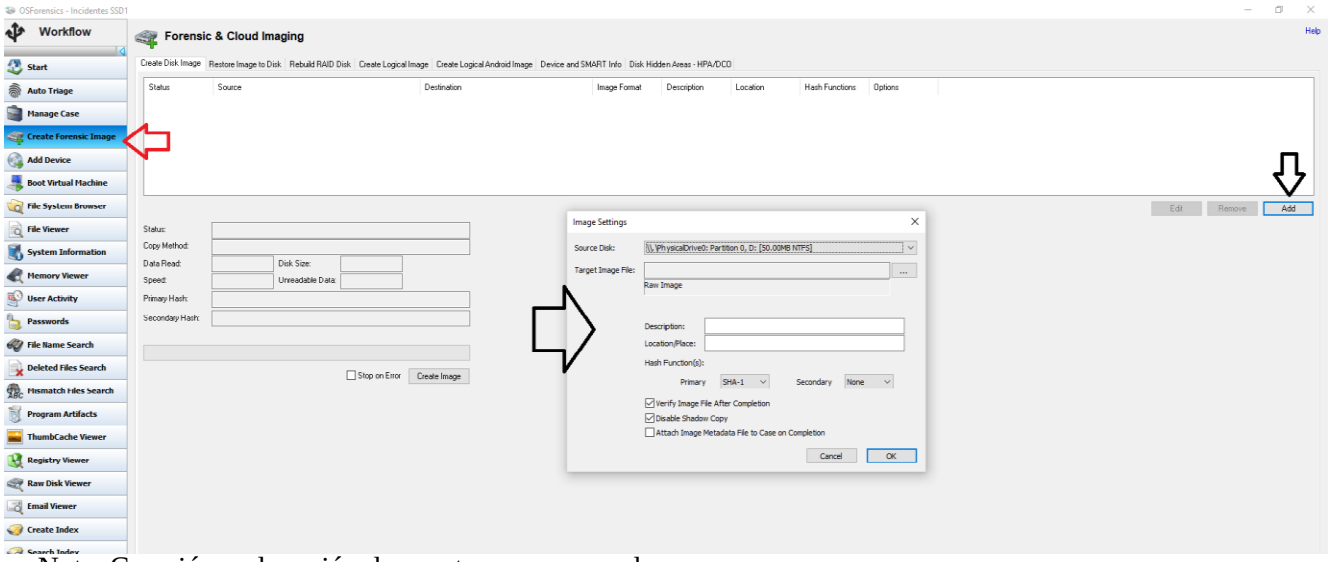


Nota. Verificación de sistemas y archivos en unidad Ssd.

Con estas opciones ya tenemos el caso creado procedemos a hacer el clonado de nuestras imágenes en ambas unidades de almacenamiento como origen Unidades HDD 500GB(F:) SSD y 500 GB (E:) con destino COP IMG (G:).

Figura 48

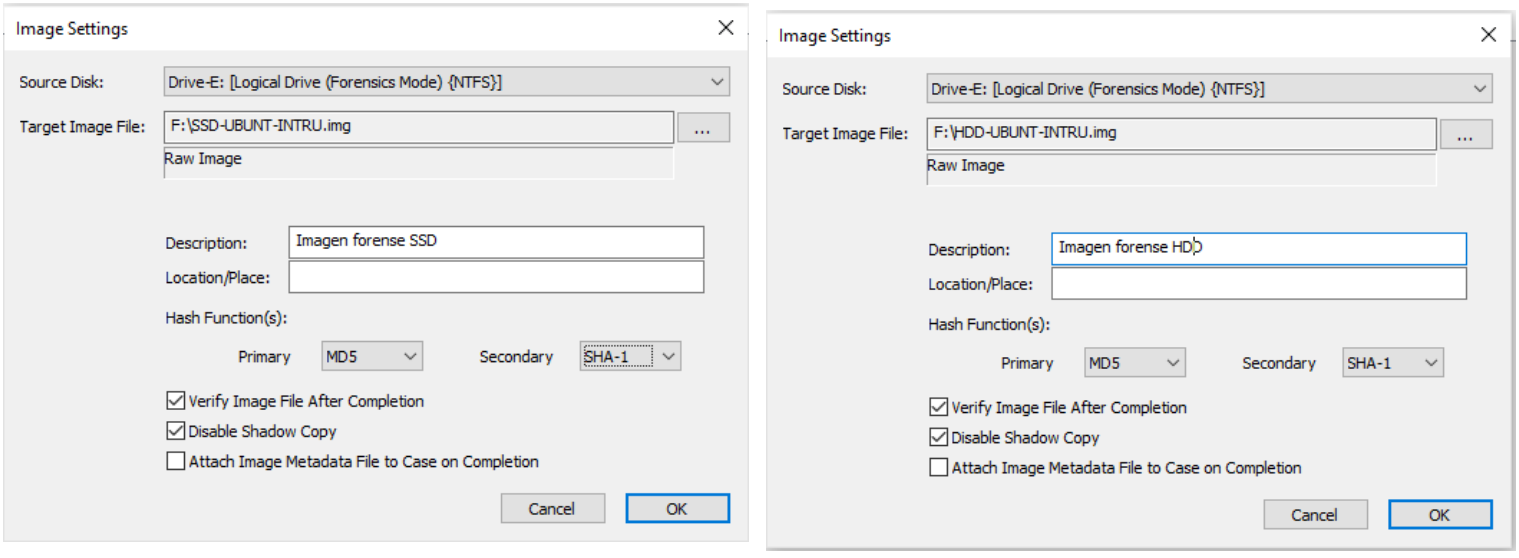
Creación Forensic Image



Nota. Creación y clonación de nuestros casos creados.

Figura 49

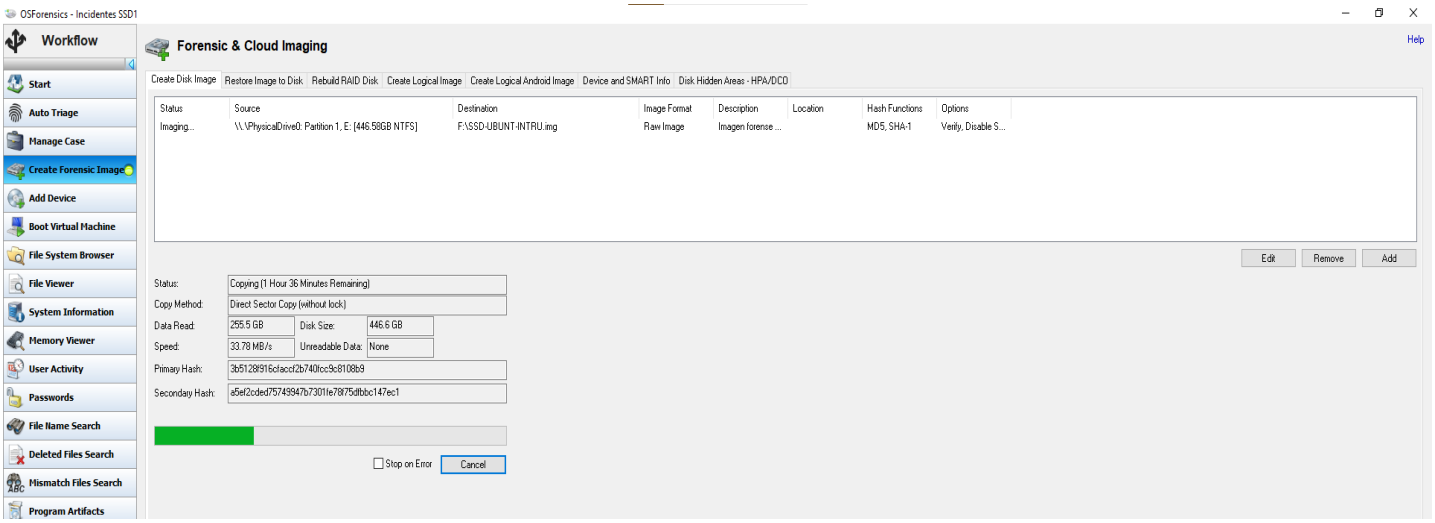
Configuración de imagen y tipo de Hash



Nota. Configuración de ruta de guardado y tipos de hash a generar.

Figura 50

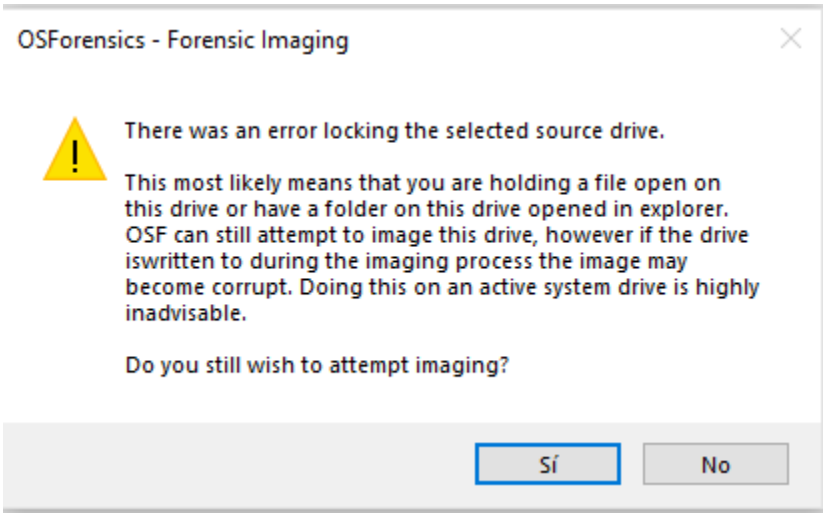
Inicio de Clonación SSD



Nota. Inicio de clonación de unidad SSD.

Figura 51

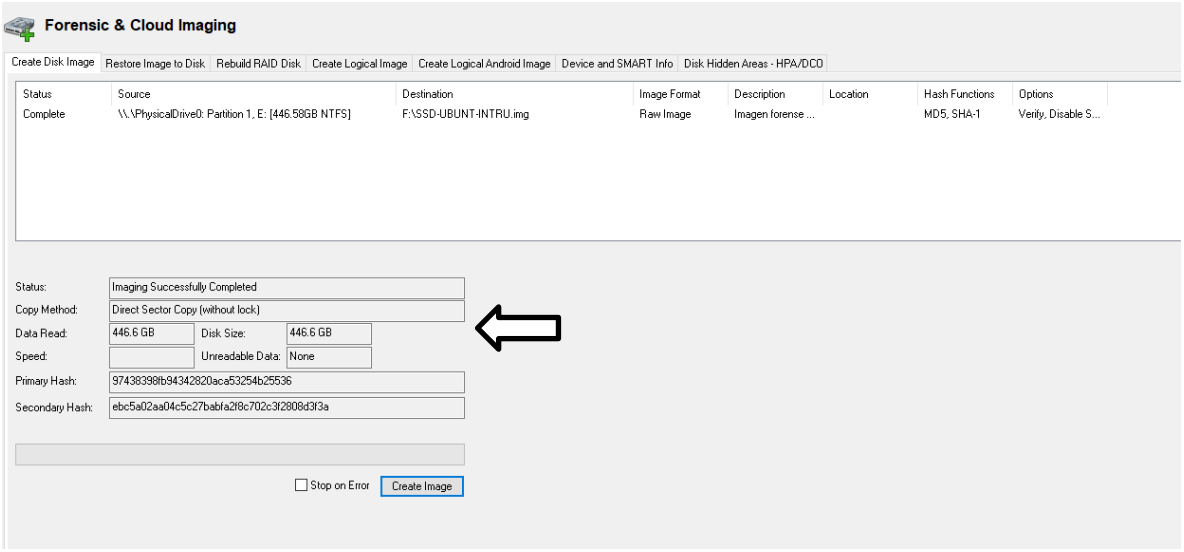
Mensaje de no acceso mientras se hace la extracción Forense.



Nota. Mensaje de alerta de no acceso a la unidad mientras hace la extracción de la imagen porque puede corromper la extracción en el proceso lo que generara un cambio en el hash y la imagen forense seria invalida para su contexto final.

Figura 52

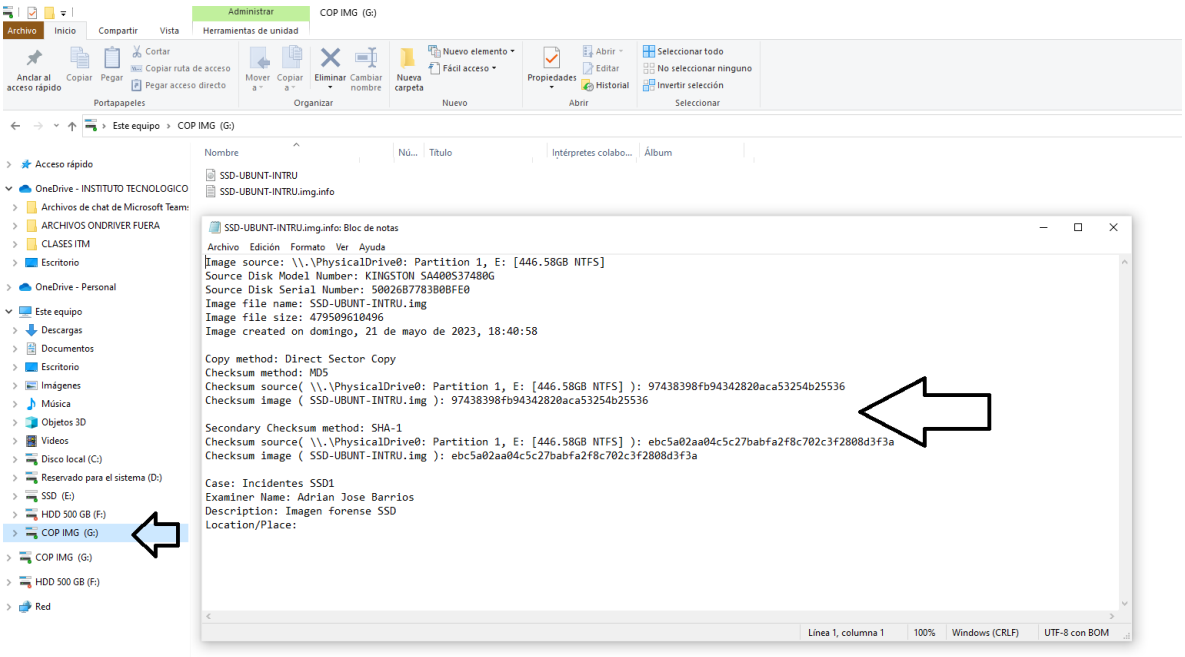
Extracción forense completa unidad SSD



Nota. Clonación exitosa generación de hash de la imagen.

Figura 53

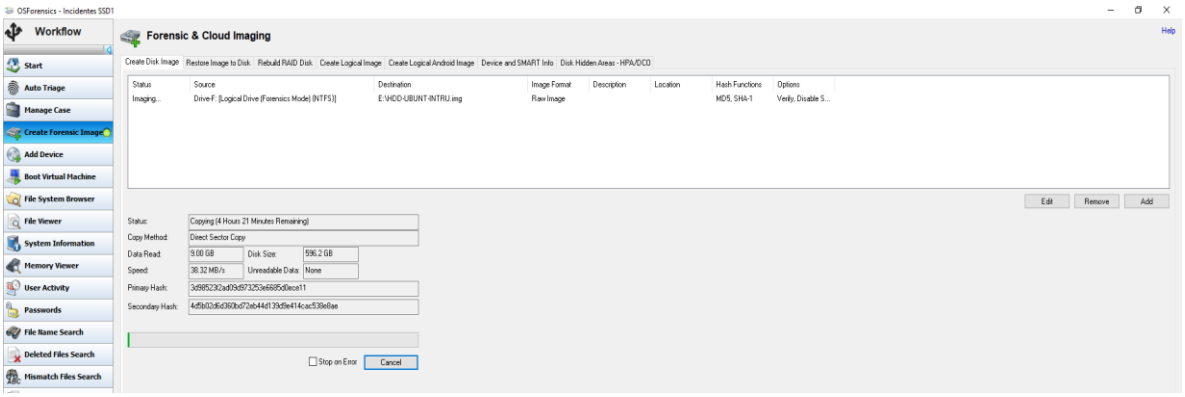
Propiedades extracción forense SSD



Nota. Extracción OSForensics a la unidad SSD.

Figura 54

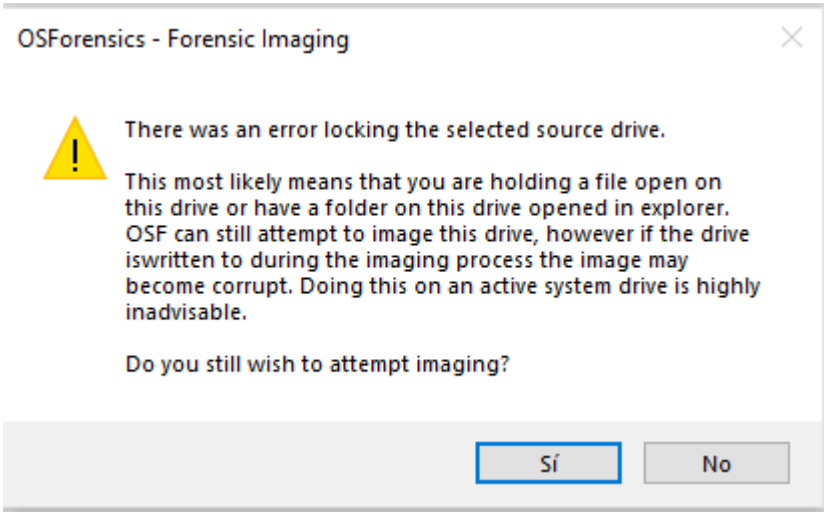
Inicio de Clonación HDD



Nota. Inicio de clonación de unidad HDD.

Figura 53

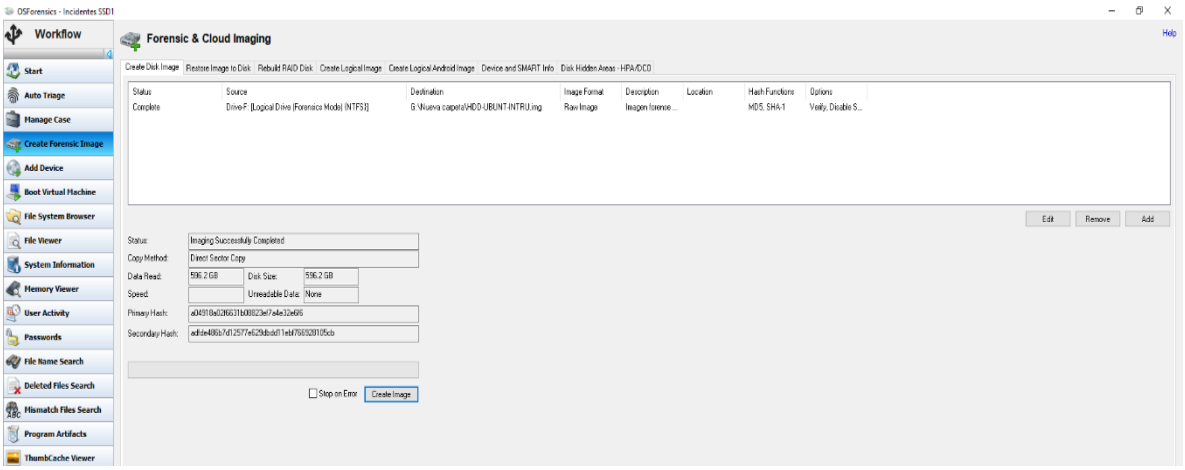
Mensaje de no acceso mientras se hace la extracción Forense.



Nota. Mensaje de alerta de no acceso a la unidad mientras hace la extracción de la imagen porque puede corromper la extracción en el proceso lo que generara un cambio en el hash y la imagen forense seria invalida para su contexto final.

Figura 55

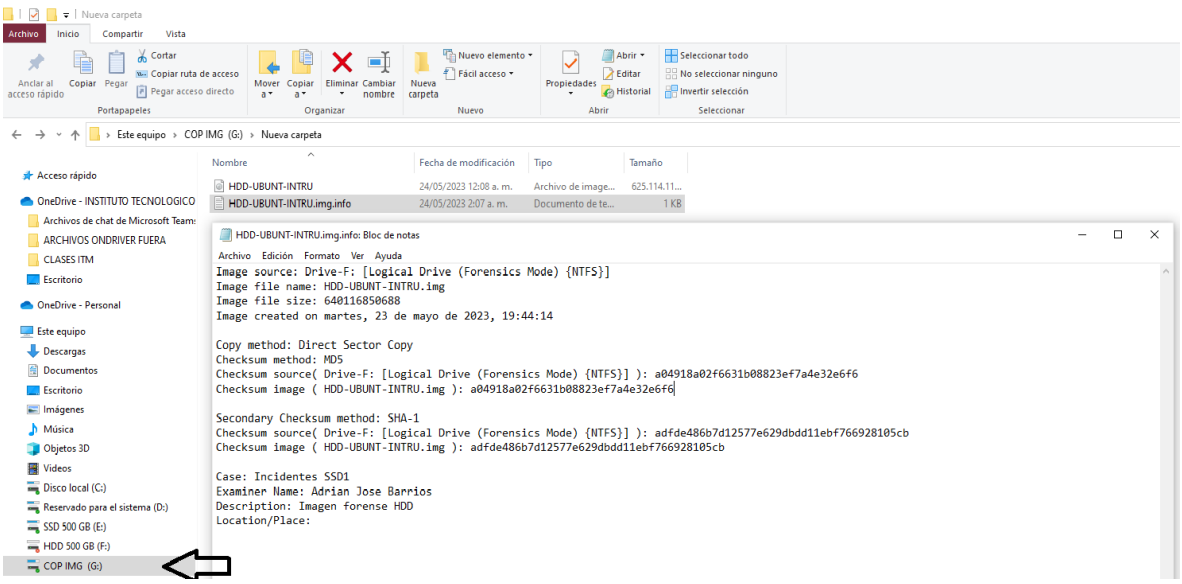
Extracción forense completa unidad HDD



Nota. Clonación exitosa generación de hash de la imagen.

Figura 56

Propiedades extracción forense HDD



Nota. Extracción OSForensics a la unidad HDD.

Entregable 2: Se entrega en la segunda fase una descripción con los diferentes tipos de herramientas de análisis digital que existen y la correcta interpretación de sus datos.

En esta fase se identifican y describen las diferentes herramientas de extracción forense sus características como también sus diferencias y que hay que tener en cuenta a la hora de seleccionar una buena herramienta que agilice una óptima extracción forense en las diferentes unidades de almacenamiento magnéticas y sólidas, también mencionamos la importancia de la informática forense y como esta se apoyan en herramientas que detectan vulnerabilidades o falencias de seguridad a la hora de hacer una extracción digital en los sistemas tecnológicos vulnerados, mediante la implementación de técnicas como herramientas que puedan sustraer información por una brecha de seguridad o borrado de información accidental o provocado en algún dispositivo y como tener una forma idónea de verificación de los resultados obtenidos a partir de estas atendiendo los tres pilares de la seguridad de la información y la norma ISO 27000 y el debido tratamiento en las diferentes unidades de almacenamiento.

FASE 3: Se describen los procesos y resultados obtenidos de las herramientas FTKImager y OSForensics durante toda la etapa de levantamiento de requisitos y resultados.
Objetivo 3: Se describirá como los resultados obtenidos de diferentes herramientas de extracción de imagen forenses y sus resultados interpretando sus diferencias
Actividad 3: Se analizan los resultados obtenidos de ambas herramientas describiendo diferencias y problemas al utilizar las herramientas a la hora de hacer una extracción virtual y clonación de diferentes imágenes, en diferentes dispositivos de almacenamiento dando credibilidad a la cadena de custodia, bajo la norma BS 10008:2008 “Garantía de un almacenamiento correcto de la información digital” [29].

En esta fase de adquisición bajo la norma BS 10008, vemos en nuestra figura 24 y 25 errores en los sectores 4584328, 4584335 Y 1206294064, 1206294065 los que hacen que nuestras imágenes forenses puedan obtener un resultado diferente al terminar nuestra clonación y estos son remplazados por ceros.

Figura 57

Verificación Hash copia original HDD

```
ATTENTION:
The following sector(s) on the source drive could not be read:
      4584328 through 4584335
      1206294064 through 1206294065
The contents of these sectors were replaced with zeros in the image.

[Computed Hashes]
 MD5 checksum:    f683317ad9d7fa275d5175883a9e7ffc
 SHA1 checksum:   bef3737f74a8e6b9642de745e93389683e672c65

Image Information:
 Acquisition started:   Wed Apr 26 10:36:46 2023
 Acquisition finished:  Wed Apr 26 15:33:11 2023
```

Nota: verificación de hash y errores de atención en sectores de nuestra clonación.

Figura 58

Verificación Hash copia original SSD

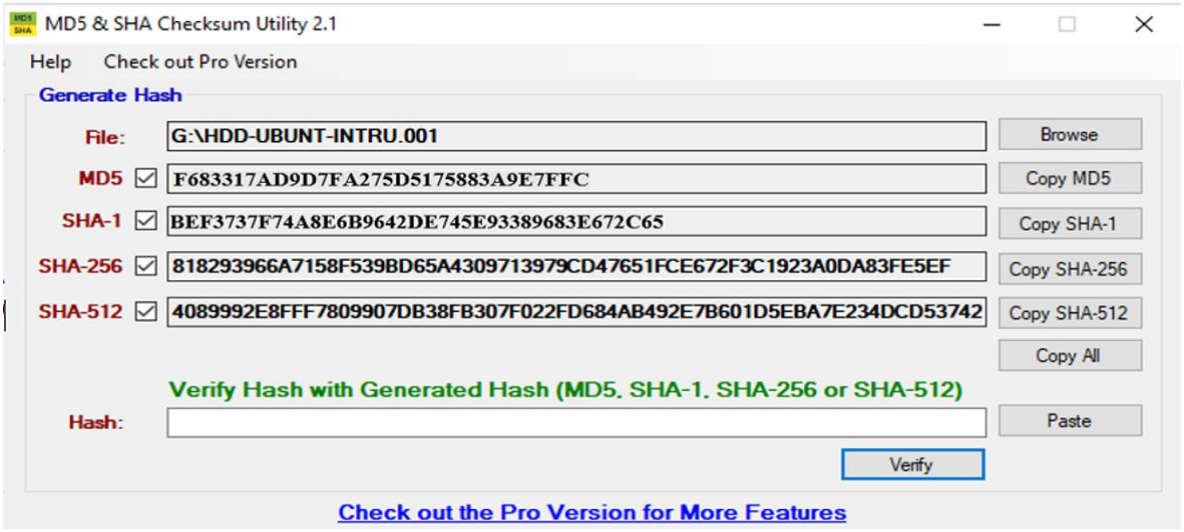
```
ATTENTION:
The following sector(s) on the source drive could not be read:
      1524328 through 1524337
      110629400 through 120629406
The contents of these sectors were replaced with zeros in the image.

[Computed Hashes]
 MD5 checksum:    f10f322fde77f2b2f29079e822acfaa4
 SHA1 checksum:   a19947251338bf91912ad21ce8a9041c5fdf922c

Image Information:
 Acquisition started:   Wed Apr 27 09:36:25 2023
 Acquisition finished:  Wed Apr 27 15:33:09 2023
```

Nota: verificación de hash y errores de atención en sectores de nuestra clonación.

En el momento de hacer las extracciones forenses con las herramientas seleccionadas, se puede evidenciar una incongruencia de hash a la hora de generar estas pruebas en las figuras 30, 32 en los hashes SHA-256 y SHA-512 son idénticos a la extracción de nuestra imagen SSD con diferencial de solo los MD5 y SHA-1.

Figura 59

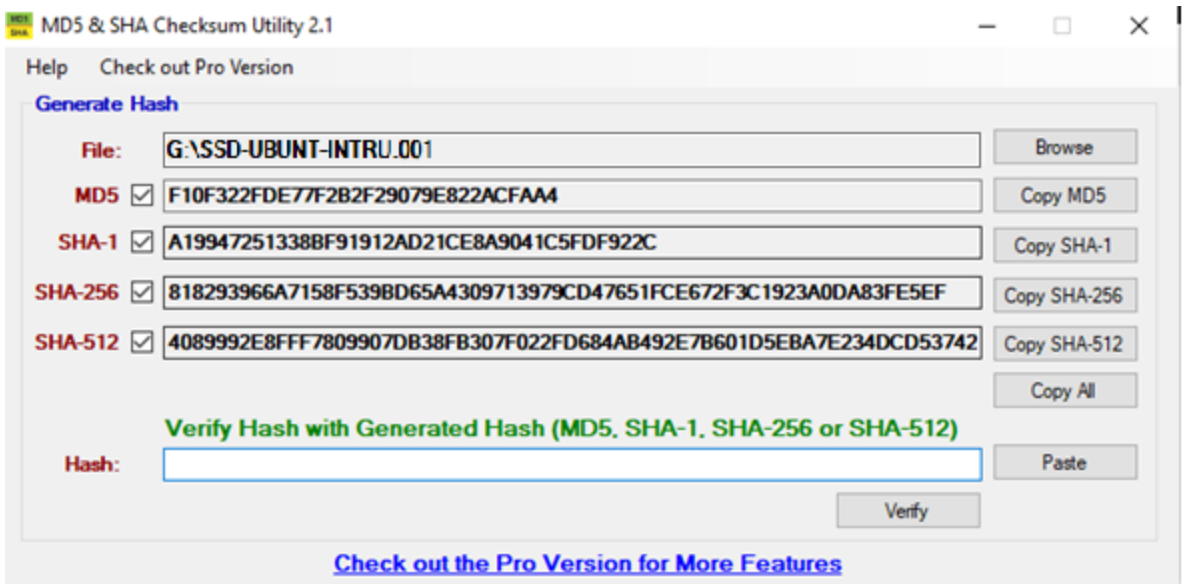
Preservación MD5 & SHA1 con la herramienta Checksum Utility a la unidad HDD.



Nota. generación de Hash con la herramienta de autenticación de la imagen forense HDD original.

Figura 60

Preservación MD5 & SHA1 con la herramienta Checksum Utility a la unidad SSD.

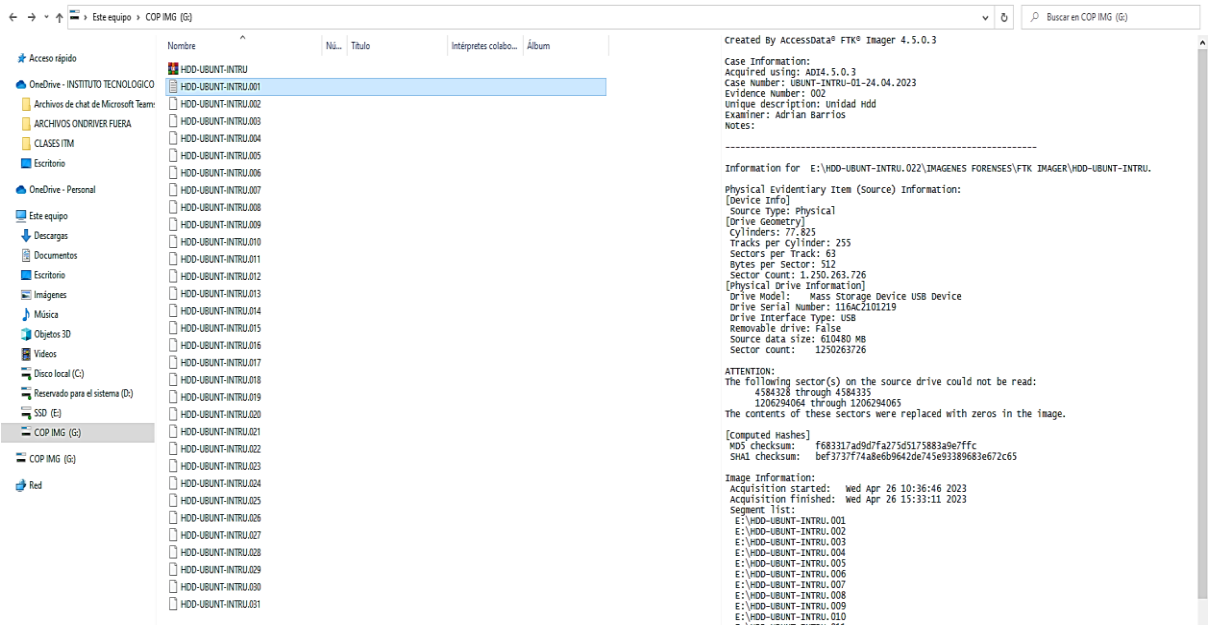


Nota. Generación de Hash con la herramienta de autenticación de la imagen forense SSD original.

En las figuras 22, 23 y 51, 55 el tamaño de archivos generados dependiendo de la unidad examinada se debe tener en cuenta ya que de la cantidad generada en nuestro caso puede provocar perdida de integridad en la generación de los hashes por falta de algún archivo a la hora de generar nuestras copias. En nuestras figuras con la herramienta FTKimager tenemos 31 archivos en nuestra imagen HDD y en nuestra unidad SSD 24 archivos, y con nuestra OSForensic obtenemos 1 solo archivo de imagen completo donde se es más integro la generación de nuestras imágenes forenses.

Figura 61

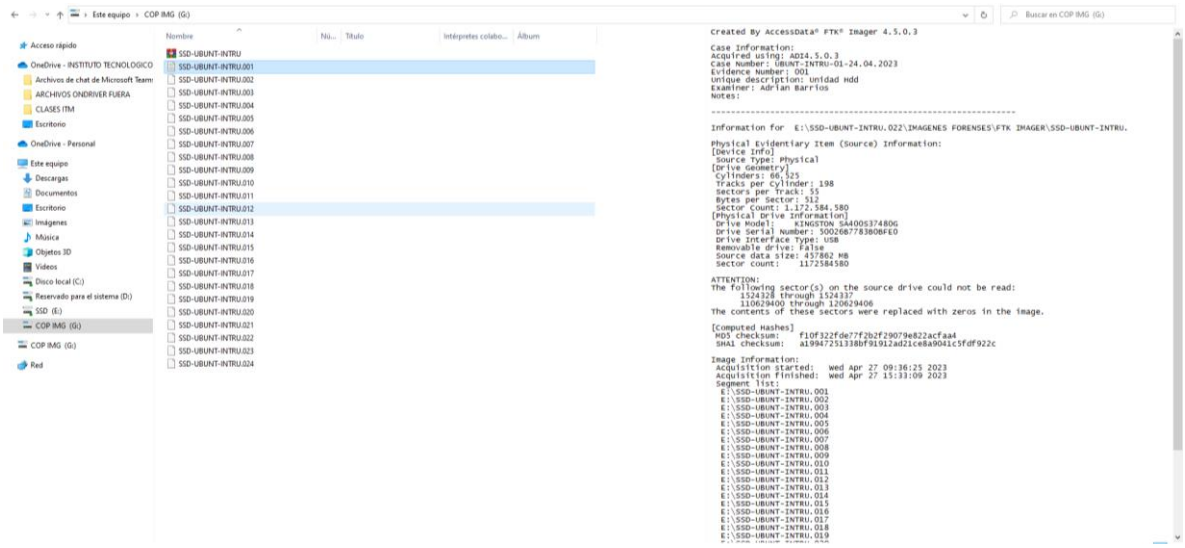
Resultado Imagen forense HDD.



Nota: Clonación exitosa verificación de Hash único paso 10.

Figura 62

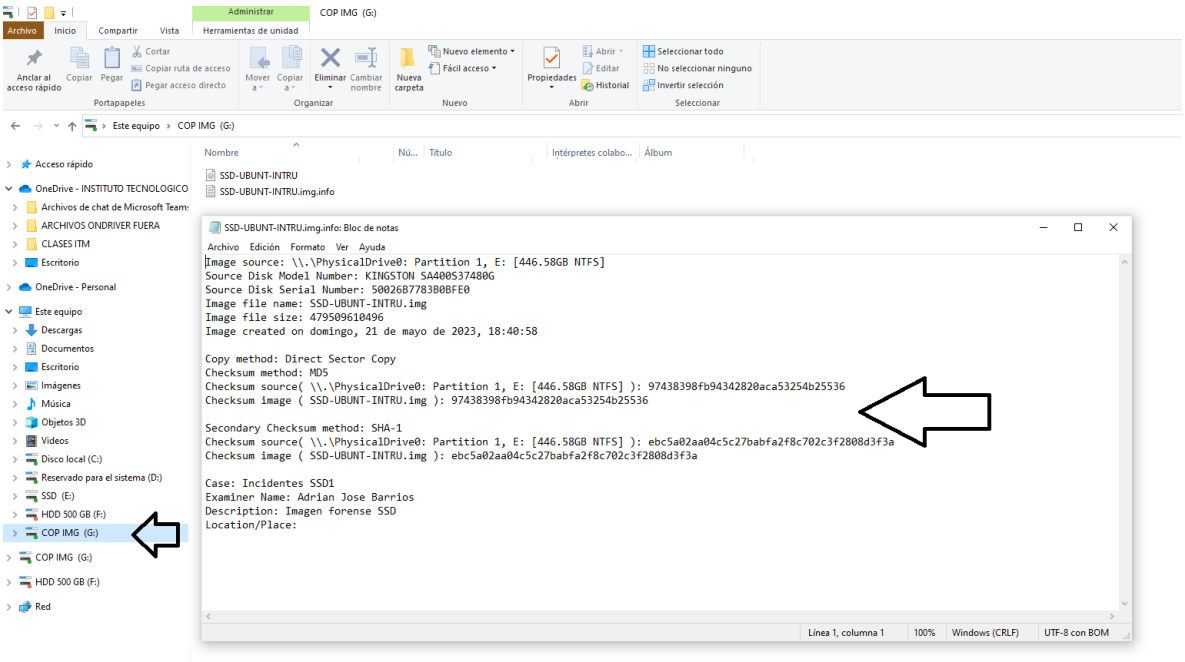
Resultado Imagen forense SSD



Nota: Clonación exitosa verificación de Hash único paso 10.

Figura 63

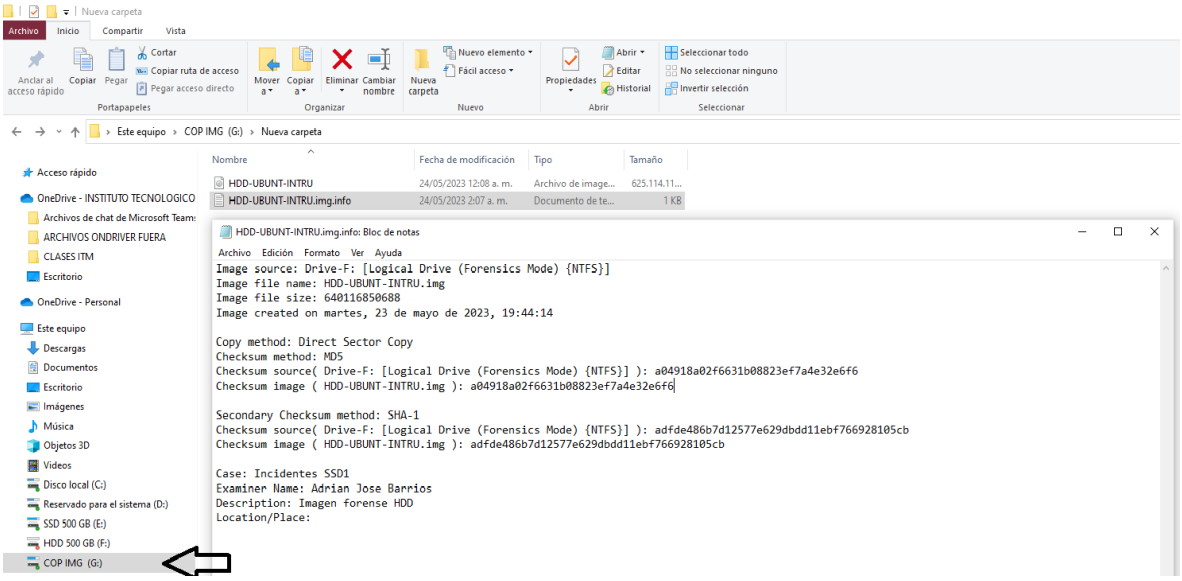
Propiedades extracción forense SSD



Nota. Extracción OSForensics a la unidad SSD.

Figura 64

Propiedades extracción forense HDD

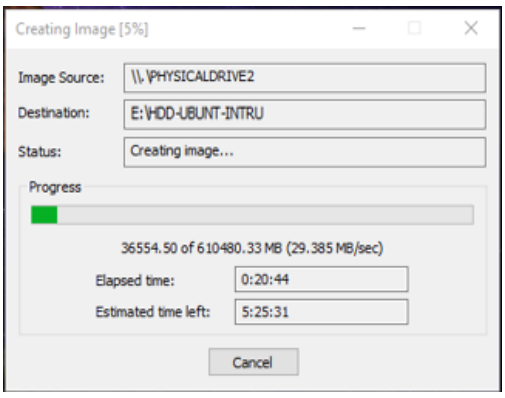


Nota. Extracción OSForensics a la unidad HDD.

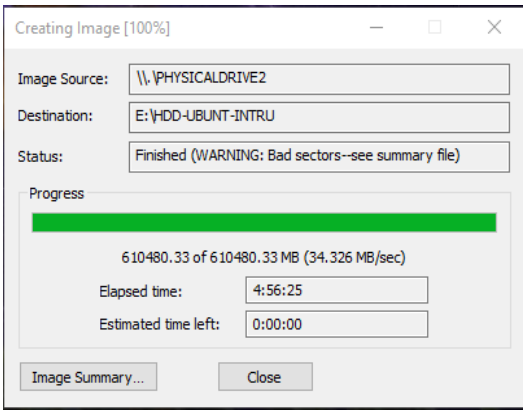
Los tiempos de generación de nuestras imágenes forenses con las herramientas seleccionadas en unidades magnéticas son muy amplios lo que converge a tener unidades de extracción mucho más volátiles y lentas con frecuencias más altas para que extraiga la información mucho más rápido como lo vemos en nuestras figuras 21 en ambos tipos de unidades con la herramienta FTKimager.

Figura 65

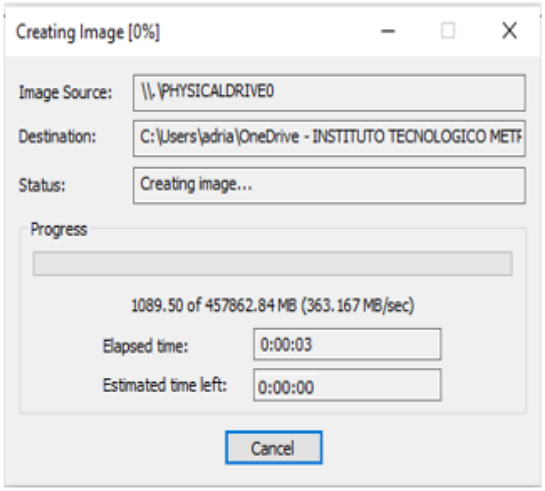
Resultados de la extracción forense SSD Y HDD



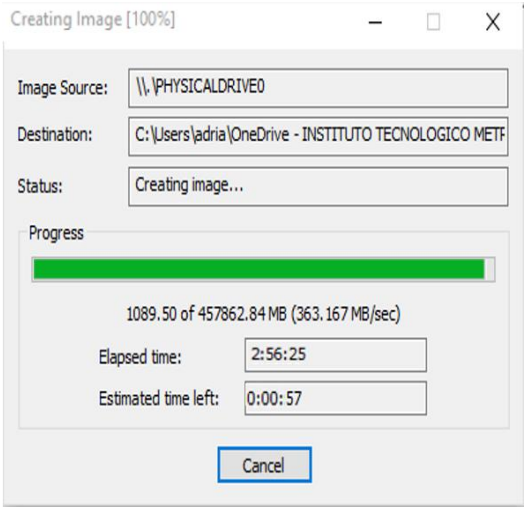
Nota. inicio de clonación copia Unidad HDD paso 9.



Nota. final de clonación copia Unidad HDD paso 9.



Nota. inicio de clonación copia Unidad SDD paso 9.



Nota. final de clonación copia Unidad SDD paso 9.

Utilización de unidad de extracción muchos más rápidas 3.0 ya que la que tenemos es 2.5 y la velocidad de lectura y escritura es menor como la siguiente.

Figura 66

Unidad portable 3.0

Nota. Unidad portable de almacenamiento 3.0 mhz.

Entregable 3: Se entrega en la tercera fase el proceso que se realizó en la implementación de las herramientas de análisis y la correcta interpretación de sus datos.

En esta fase se describen los resultados y procesos obtenidos a partir de las diferentes extracciones forenses en las unidades de almacenamiento magnéticas y solidas con las herramientas seleccionadas, como se hace el proceso de levantamiento de requerimientos bajo la norma ISO 27031 y el guardado de la información bajo la norma BS 10008, de cómo garantizar el correcto almacenamiento de la información digital y que se cumplan con el estándar como también el principio de confidencialidad è integridad de la información dando credibilidad a la cadena de custodia bajo esta normatividad, y como la combinación de estas para los investigadores forenses obtener capacidad de dar fiabilidad y resultados sólidos y confiables en sus investigaciones, lo que contribuye a la resolución de casos y al mantenimiento de la disponibilidad è integridad de la evidencia digital tratada en aspectos como lo jurídico o legal.

FASE 4: Evaluar los resultados obtenidos al implementar estas herramientas mejorando prácticas y resultados obtenidos de la comparación y obtención de resultado de estas.

Objetivo 4: Evaluar los datos obtenidos de la aplicación de las herramientas y sus diferencias como pueden inferir en un perito forense.

Actividad 4: En esta fase se evaluarán los datos y a partir de sus diferencias se describirán soluciones y mejores prácticas para un caso judicial al utilizar estas herramientas tratadas.

Para la implementación de las buenas prácticas bajo los estándares ISO 27037 y BS10008 es necesario tener claro como estas normas definen y tratan la información desde sus ámbitos de la propia norma. La definición de Identificación bajo la ISO 27037 es el proceso de identificación de los elementos relevantes para la recopilación de evidencia digital. En la fase de adquisición: la recopilación de la evidencia digital de manera forenses, asegurando su integridad y autenticidad, en la fase de Preservación: El tipo de almacenamiento y mantenimiento adecuados de las evidencias digitales para evitar su alteración o destrucción, en la fase análisis: Un examen detallado de la evidencia digital para extraer la información relevante y establecer conclusiones, en la fase de presentación: La presentación debe ser clara y comprensible de los hallazgos de la investigación forense digital en proceso, en la fase de revisión y evaluación: La verificación de la calidad de los procedimientos utilizados en la investigación forenses digital, y en nuestra última fase de Informe: La breve documentación detalla de todos los aspectos más relevantes de la investigación forenses, todas estas características hacen parte de cómo debe ser tratada y definida la información tratada bajo esta norma que nos facilite todo el proceso de entregarla judicialmente [27].

Para la implementación de las buenas prácticas bajo la norma británica BS 10008 que están definidas de esta forma. La Captura: de datos digitales, incluida la creación y recopilación de documentos o información digitales, el almacenamiento: La gestión y el guardado adecuado de los documentos digitales que garanticen su propia integridad y accesibilidad, la autenticidad: verificar la autenticidad de los documentos digitales, la integridad: El mantenimiento de la integridad de los documentos digitales a lo largo del tiempo, asegurando su no alteración o modificación, la disponibilidad: El acceso seguro y controlado a los documento digitales por partes autorizadas, la retención y disposición: La correcta gestión de estos documentos o registros virtuales de acuerdo a las normas legales del país, mejora continua: Establecer procesos claros y controles para garantizar la gestión de la evidencia digital [52].

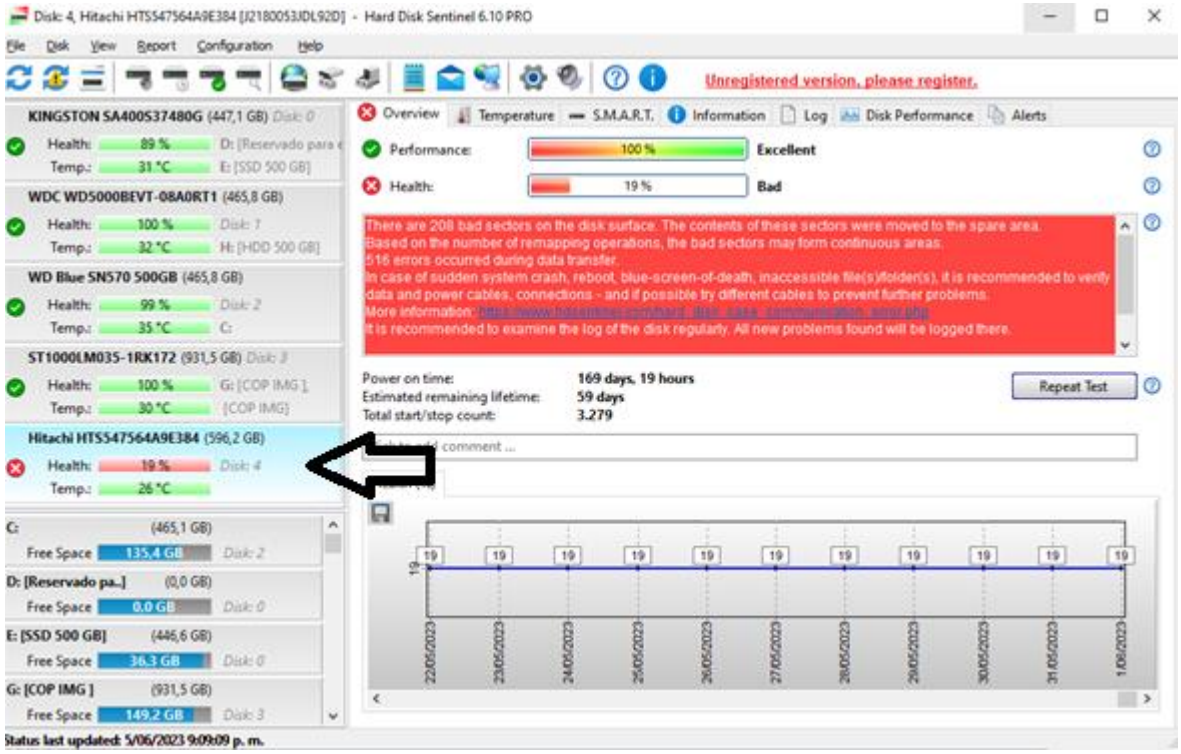
Una vez descritas las normas se continúa con la presentación de las mejores prácticas, se inicia con la norma ISO/IEC 27037 en donde las 3 primeras fases: La identificación, adquisición y preservación, son gestionadas sobre estas mismas, y como una complementa la otra y estas pueden gestionar de manera eficiente la información. Nuestra segunda norma BS10008 para las fases de autenticidad, integridad, y retención y disposición de la información tratada y que nuestra cadena de custodia se vea reflejada en los resultados de nuestra extracción forense. Podemos empezar con nuestra primera fase de buenas prácticas, iniciamos con la fase de identificación donde analizamos nuestras unidades magnéticas o sólidas y en qué estado se encuentra nuestra escena forense para tener como punto de partida esta, como segundo nuestra adquisición si es en frio o en caliente tener las herramientas listas y hacemos la recopilación de nuestra imagen y guardarla en una unidad externa sin tocar mucho la unidad examinada para no dañar nuestra integridad de nuestras clonaciones, a tercer fase la preservación de nuestras adquisiciones y el estado en que se almacenan nuestras clonaciones para poder trabajar sobre nuestras copias y mantener la integridad y disponibilidad de nuestro análisis a estas.

Continuando nuestras fases utilizando ahora la segunda norma BS10008 la fase de autenticidad; donde verificamos de manera implícita y muy detallada los hashes y la integridad de las copias creadas incluyendo las firmas o metadatos y el tiempo de creación de esta, para la fase de integridad el mantenimiento de los copias o documentos que se incluyan en la unidad donde se esté girando esta clonación que no sean fácil de acceder, y en nuestra última fase de retención y disposición se tenga muy breve las leyes o normas que garanticen estos resultados obtenidos en un caso judicial donde se pruebe toda la cadena de custodia.

Como primer ejemplo de mejor practica podemos analizar con nuestro software Hard disk Sentinel el estado en que se encuentra nuestra unidad y así descartar fallas en un escaneo a futuro de alguna prueba forense.

Figura 67

Hard Disk Sentinel

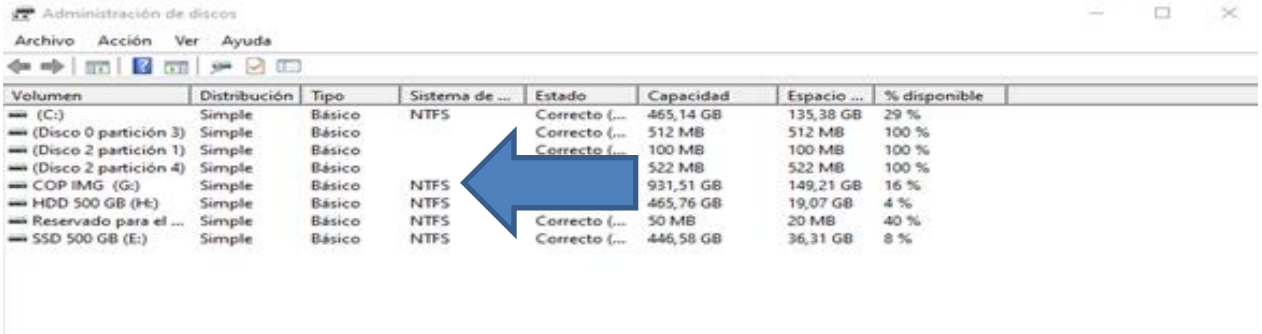


Nota. En este ejemplo vemos que la unidad de almacenamiento esta desgastada y tiene poca vida lo que en un caso tiene que describirse muy detallada que esto puede afectar en la creación de nuestra imagen forense.

Que procedemos a hacer vamos a nuestro panel de administrador de discos duros y miramos si la unidad esta inicializada o tiene inconveniente de inicio.

Figura 68

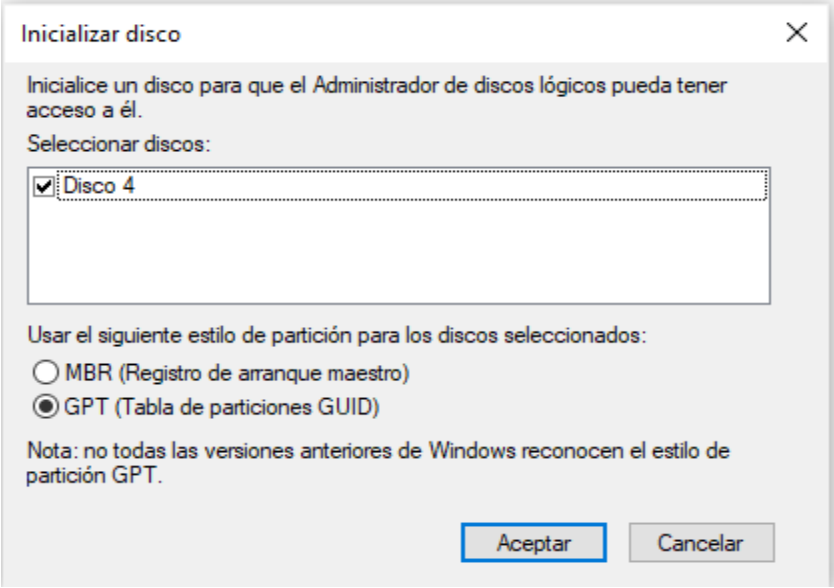
Administrador de Discos



Nota. Administrador de discos y activación para la detección en nuestro equipo local.

Figura 69

Inicializador de discos duros



Nota. Inicializador de discos y estilo de partición MBR o GPT.

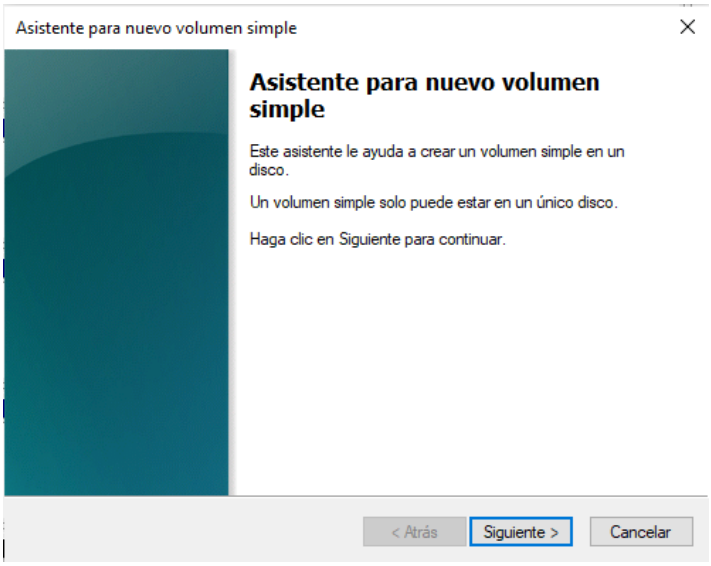
Figura 70

Activación de disco

Nota. Activamos la coneccion y el tipo de formato de la unidad

Figura 71

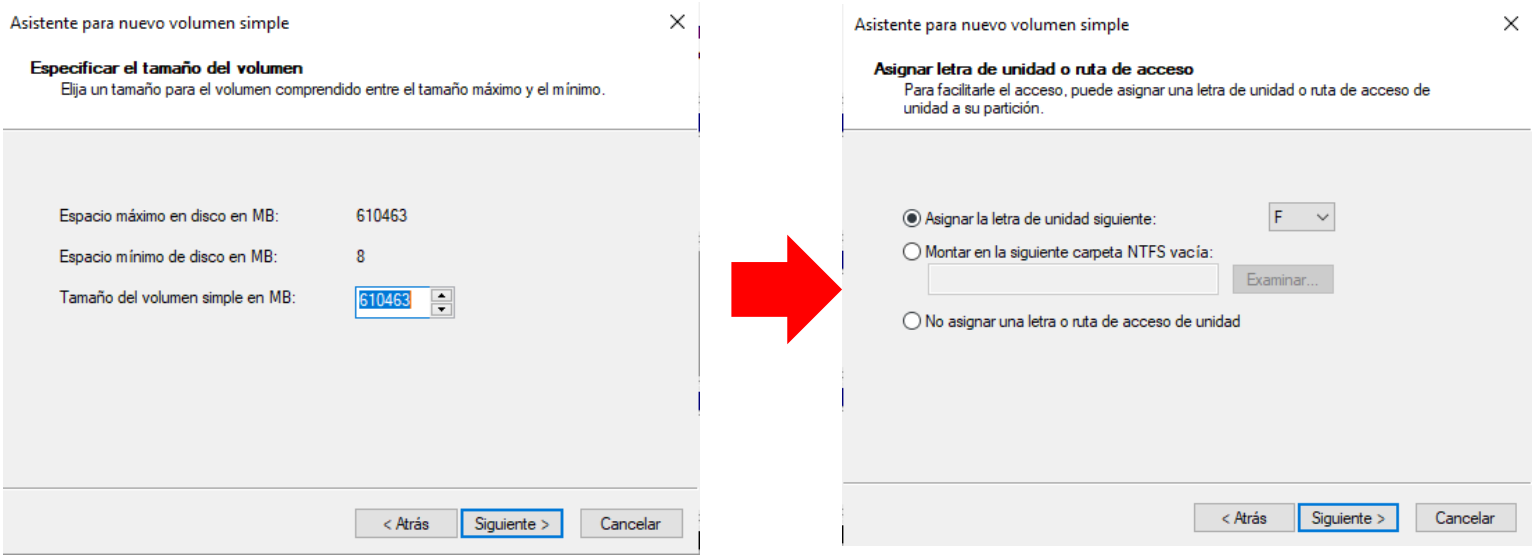
Asistente de creación de volumen y formato



Nota. Creamos nuestro formato, le asignamos el tamaño de la unidad con su respectiva letra.

Figura 72

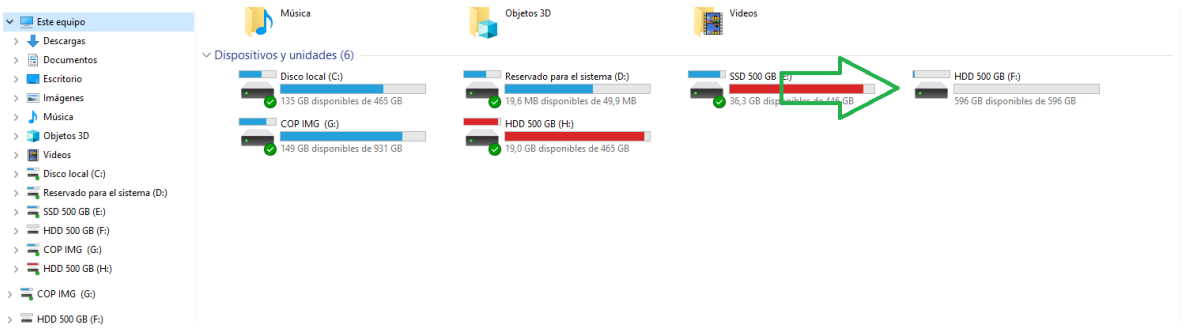
Asignación de tamaño y letra



Nota. Asignamos el tamaño total y el tipo de letra con formato para que nuestra unidad pueda funcionar y darle utilidad con el fin de hacer una buena extracción en los casos que se necesite.

Figura 73

Nueva Unidad leída



Nota. Nueva unidad creada y funcional para nuestra extracción o clonación forense según la necesidad de la prueba.

A nivel de software para hacer una correcta extracción forense después de haber investigado las herramientas que nos faciliten esta tarea, es recomendable utilizar software con licencias o comprados para no limitarse en el registro o funcionalidad de ciertas funcionalidades a la hora de hacer la extracción forense y que nos genere reportes y sea mucho más rapido la generación de una imagen forense en este caso nuestra herramienta OSForensics. El utilizar software de versión gratis no limita en su totalidad la prueba de ciertos aspectos en una imagen forense, pero es necesario para la generación más rápida y generación del reporte en óptimas condiciones.

Figura 74

Versión de prueba OSForensics

Nota. Software de versión de paga o free.

A nivel de equipo es importante tener unos mínimos requerimientos que nos faciliten el tiempo y que generen de una forma eficiente nuestra extracción forense para lograr una adquisición de imágenes forenses más rápida y eficiente, es necesario contar con un equipo PC que cumpla con ciertos requisitos específicos se requiere un sistema con un procesador de alto rendimiento y múltiples núcleos, como un procesador Intel Core i7, ryzen 7 o superior, para manejar eficientemente las tareas de adquisición de imágenes forenses. Además, se recomienda contar con una cantidad adecuada de memoria RAM, como mínimo 16 GB y máximo la que dese el usuario, para permitir la ejecución fluida de las aplicaciones forenses y facilitar la manipulación de grandes conjuntos de datos y, asimismo un disco duro de estado sólido (SSD) con capacidad de almacenamiento suficiente para guardar las imágenes adquiridas de manera rápida y confiable.
Es esencial disponer de puertos USB 3.0 o superiores para garantizar velocidades de transferencia de datos rápidas durante la conexión de dispositivos de almacenamiento externos o unidades flash forenses. Además, la tarjeta de red debe ser compatible con Ethernet Gigabit para facilitar la transferencia de imágenes forenses a través de la red.

Por último, es importante contar con una tarjeta gráfica potente y compatible con tecnologías de aceleración gráfica para facilitar el análisis y la visualización de imágenes forenses un monitor de alta resolución y calibrado adecuadamente también contribuirá a una experiencia de visualización óptima.

Entregable 4: Se entregará en la cuarta fase una descripción con los resultados obtenidos de los tipos de herramientas de análisis forense y como sus resultados pueden inferir en un perito judicial y la correcta interpretación de sus datos.

En esta fase a partir de los resultados obtenidos y las diferentes implementaciones con las herramientas seleccionadas una correcta interpretación de los resultados por parte de un perito judicial ya que estos proporcionan una base sólida para respaldar las fases de todas las actividades desarrolladas posteriormente a partir de estas se logran obtener una interpretación esencial y como con mejores herramientas se pueden obtener de manera más rápida y con mejores prácticas en la norma la obtención de las extracciones forenses y que estas no se vean comprometidas por factores externos de estas demostrando como un único fin la participación de una persona en algún delito

informático y que a partir de estos sucesos desarrollados los resultados pueden interferir en un caso judicial y como las unidades magnéticas y solidas deben ser tratadas para tener una forma más eficiente y confiables.

7. CONCLUSIONES

En el proceso de extracción forense se presentaron diferentes dificultades que al hacer un análisis detallado de la extracción forenses en las unidades magnéticas y sólidas y sus respectivos clonados a la imagen principal los resultados deben ser tenidos en cuenta. Al iniciar el análisis y el respectivo clonado en la unidad magnética se presentaron lentitudes y espacios en blanco que se ven reflejados en los hashes al final de los clonados de nuestra imagen forense principal y sus copias, y al hacer una lectura en las unidades magnéticas fue un comportamiento diferente porque al hacer el proceso de clonado más rapido se presentan menos problemas pero hay que tener en cuenta los estados en que estan las unidades examinadas inicialmente para evitar incongruencias de hash y sus resultados que se presentaron en esta monografia, y es muy importante resaltar la utilización de unidades portables de almacenamiento o cajas portables con voltajes entre 2.5 Mhz y 3.0 Mhz en el caso de sustraer la unidad de almacenamiento HDD o SSD del equipo afectado y hacer más eficiente el proceso de extracción forense con un % de éxito mayor al 90%, Además de tener el software de clonado y las herramientas indispensables para hacer el proceso y el tiempo más óptimos en la clonado de la imagen principal.

Para tener una extracción forense correcta se recomienda un equipo PC adecuado para obtener imágenes forenses de manera rápida y eficiente, debe tener un procesador potente, suficiente memoria RAM, almacenamiento rápido, de gran capacidad y puertos de alta velocidad, una tarjeta de red compatible y una tarjeta gráfica potente haciendo que estas características aseguraren un rendimiento óptimo durante la adquisición de imágenes forenses para que contribuya a una investigación eficiente y efectiva en nuestras extracciones forenses futura.

Por último, este manual de buenas prácticas permite optimizar el tiempo de obtención de las imágenes forenses preservando su fiabilidad y conservando la cadena de custodia según las normas y marcos jurídicos, facilitando el trabajo de los investigadores forenses.

8. REFERENCIAS BIBLIOGRÁFICAS

[1] ISO/IEC 27037:2012, «Guidelines for identification, collection, acquisition and preservation of digital evidence,» S.F S.F 2012. [En línea]. Available: https://www.iso.org/standard/44381.html. [Último acceso: 22 10 2022].

[2] GTC-ISO-TR - ICONTEC, «GESTIÓN DE DOCUMENTOS. INFORMACIÓN ALMACENADA ELECTRÓNICAMENTE. RECOMENDACIONES PARA LA INTEGRIDAD Y LA FIABILIDAD,» 19 02 2014. [En línea]. Available: https://tienda.icontec.org/sectores/servicios-organizacion-de-la-empresa-gestion-y-calidad-administracion-transporte-sociologia/servicios/otros-servicios/gp-gestion-de-documentos-informacion-almacenada-electronicamente-recomendaciones-para-la-integridad-y. [Último acceso: 21 10 2022].

[3] Brian H.Carrier, Eugene H.Spafford, «Un Marco de investigaciòn forensen Digital basado en eventos,» *DFRWS USA,* vol. 1, nº 0, p. 12, 2004.

[4] Karen, «Guide to Integrating Forensic Techniques into Incident, et al. SP 800-86.,» S.F S.F 2006. [En línea]. Available: https://tsapps.nist.gov/. [Último acceso: 26 10 2022].

[5] INTERPOL, «Innovación,» S.F S.F 2022. [En línea]. Available: https://www.interpol.int/es/Como-trabajamos/Innovacion/. [Último acceso: 16 09 2022].

[6] Karen Kent, Zussane Chevalier, Tim Grance, Hung Dang, «Guide to Integrating Forensic,» The National Institute of Standards and Technology (NIST) , Gaithersburg - EE.UU, 2006.

[7] J. C. Navarro, «Historia de la informatica forense,» s.f s.f 2018. [En línea]. Available: https://www.timetoast.com/timelines/historia-de-la-informatica-forense. [Último acceso: 16 09 2022].

[8] Dr. Santiago Acurio Del Pino, «Manual de Manejo de Evidencias Digitales y Entornos,» s.f s.f 2011. [En línea]. Available: https://www.oas.org/juridico/english/cyb_pan_manual.pdf. [Último acceso: 17 10 2022].

[9] Restrepo, Ana María, «11 de septiembre, día decisivo para la seguridad,» s.f 04 2007. [En línea]. Available: https://www.dragonjar.org/computacion-forense-analisis-de-cadaveres-virtuales.xhtml. [Último acceso: 26 10 2022].

[10] A. L. S. Iglesias, «Disco duro SSD, ¿Qué es?,» 1 08 2019. [En línea]. Available: https://cutt.ly/NNfJnVO. [Último acceso: 26 10 2022].

[11] Jorge Heli Espitia Ruiz, Wilmer muñoz Espitia, «forensic analysis on magnetic and solid state hard drives,» 24 01 2014. [En línea]. Available: https://cutt.ly/iNfHcu8. [Último acceso: 26 10 2022].

[12] David Oniera, «Devuelve a la vida y recupera tu disco o memoria USB con formato RAW,» 20 09 2022. [En línea]. Available:

https://www.softzone.es/windows/como-se-hace/disco-duro-raw-recuperar-datos/. [Último acceso: 1 11 2022].

[13] M. Á. C. C. J. Á. M. F. R. C. M. A. C. M. L. R. M. Q. B. D. L. Martha Irene Romero Castro, «LA-INFORMÁTICA-FORENSE-DESDE-UN-ENFOQUE-PRÁCTICO,» 09 2020. [En línea]. Available: https://www.3ciencias.com/wp-content/uploads/2020/09/LA-INFORM%C3%81TICA-FORENSE-DESDE-UN-ENFOQUE-PR%C3%81CTICO.pdf. [Último acceso: 08 05 2023].

[14] E. d. E. e. C. y. Tecnología, «Qué es la criptografía y cuáles son sus usos,» VIU España, 9 08 2021. [En línea]. Available: https://www.universidadviu.com/es/actualidad/nuestros-expertos/que-es-la-criptografia-y-cuales-son-sus-usos. [Último acceso: 08 05 2023].

[15] IBM, «¿Qué es un ciberataque?,» IBM, 04 04 2023. [En línea]. Available: https://www.ibm.com/es-es/topics/cyber-attack. [Último acceso: 08 05 20232].

[16] J. J. C. Javier Pimentel Calderón, «Consideraciones Sobre el Estado del Arte del Peritaje Informático y los estándares de manipulación de pruebas electrónicas en el mundo,» s.f 12 2007. [En línea]. Available: file:///C:/Users/adria/Downloads/Dialnet-ConsideracionesSobreElEstadoDelArteDelPeritajeInfo-7510290.pdf. [Último acceso: 08 05 2020].

[17] NIST, «Directrices sobre análisis forense de dispositivos móviles,» 05 2014. [En línea]. Available: https://csrc.nist.gov/publications/detail/sp/800-101/rev-1/final. [Último acceso: 08 05 2023].

[18] M. Ferreira, «Introducào a preservacào Digital conceitos, estratégias e actuais consensos,» 2006. [En línea]. Available: https://repositorium.sdum.uminho.pt/bitstream/1822/5820/1/livro.pdf . [Último acceso: 08 05 2023].

[19] UNESCO, «Carta de la UNESCO para la Preservación del Patrimonio Digital Actas de la Conferencia PARIS,» 2003. [En línea]. Available: https://unesdoc.unesco.org/ark:/48223/pf0000229034_spa.locale=es. [Último acceso: 08 05 2023].

[20] INTEF, «equipamiento-tecnologico,» 2021. [En línea]. Available: https://recursostic.educacion.es/observatorio/web/gl/equipamiento-tecnologico/hardware/362-eduardo-e-quiroga. [Último acceso: 08 05 2023].

[21] «INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES,» s.d 10 2018. [En línea]. Available: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf. [Último acceso: 05 05 2023].

[22] Jasmin Ćosić, Baca, «A framework to (Im) Prove „Chain of Custody “in Digital Investigation Process,» S.f S.f 2010. [En línea]. Available: https://www.researchgate.net/publication/279175021_A_framework_to_Im_P

rove_Chain_of_Custody_in_Digital_Investigation_Process. [Último acceso: 30 10 2022].

[23] SP 800-86, «Guide to Integrating Forensic Techniques into Incident Response,» S.F 08 2006. [En línea]. Available: https://csrc.nist.gov/publications/detail/sp/800-86/final. [Último acceso: 18 09 2022].

[24] CANO MARTÍNEZ, Jeimy José., «El peritaje informático y la evidencia digital,» Bogotá, 2012.

[25] Miles Tracy (Tecnología de la información de la Reserva Federal) , Wayne Jansen (NIST) , Karen Scarfone (NIST) , Theodore Winograd (BAH), «SP 800-44 Versión 2,» de *Directrices sobre la protección de servidores web públicos*, EE.UU, National Institute of Standards and Technology Special Publication 800-44 Version 2, 2007, p. 142.

[26] Brezinski & Killalea, «Mejores prácticas actuales de Brezinski & Killalea,» 02 2002. [En línea]. Available: https://www.ietf.org/rfc/rfc3227.txt. [Último acceso: 18 09 2022].

[27] I. 27037:2012, «ISO/CEI 27037:2012 Tecnología de la información Y Técnicas de seguridad.,» 10 2012. [En línea]. Available: https://www.iso.org/standard/44381.html. [Último acceso: 29 03 2023].

[28] «RFC 3227 - Directrices para la recopilación de evidencias y su almacenamiento.,» 18 06 2014. [En línea]. Available: https://www.incibe-cert.es/blog/rfc3227. [Último acceso: 30 10 2022].

[29] British Standards Institution, «BS 10008 Admisibilidad legal Información Electrónica,» S.F S.F 2022. [En línea]. Available: https://www.bsigroup.com/es-ES/Admisibilidad-legal-de-la-Informacion-Electronica-BS-10008/. [Último acceso: 18 10 2022].

[30] EUROPEAN NETWORK OF FORENSIC SCIENCE INSTITUTE., «Best Practice Manual for the Forensic Examination of Digital tecnology,» 2015. [En línea]. Available: https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf. [Último acceso: 18 09 2022].

[31] ACPO, «. Good Practice Guide for Computer-based Electronic Evidence,» 2014. [En línea]. Available: https://www.7safe.com/docs/default-source/default-document-library/acpo_guidelines_computer_evidence_v4_web.pdf. [Último acceso: 18 09 2022].

[32] J. C. Suárez & W. L. Pedreros, «Herramientas aplicadas en el desarrollo del Análisis Forense Informático en Colombia.,» 23 09 2016. [En línea]. Available: http://hdl.handle.net/10654/14395.. [Último acceso: 06 08 2023].

[33] Rada Jimenez, Kelly Katherine, «Herramientas de análisis forense digital orientadas a infraestructuras ti como medio de investigación en delitos informáticos.,» 21 05 2022. [En línea]. Available:

https://repository.unad.edu.co/handle/10596/48990. [Último acceso: 18 09 2022].

[34] Estrada, Alex Canedo, «La informática forensey los delitos informáticos,» Revista Pensamiento Americano, 04 06 2010. [En línea]. Available: https://www.academia.edu/27115286/La_inform%C3%A1tica_forense_y_los_delitos_inform%C3%A1ticos. [Último acceso: 20 08 2022].

[35] V. Reyes, «COURSE HERO Evidence Law, Evidence Custodian, EVIDENCE CHAIN OF CUSTODY TRACKING,» s.f s.f 2014. [En línea]. Available: https://www.coursehero.com/file/33469230/Chain-of-Custody-Formdocx/?__chid=988ac839-e0b0-4229-a937-ccc48ddfc32b. [Último acceso: 25 10 2022].

[36] Carlos Arturo Monje Álvarez , METODOLOGÍA DE LA INVESTIGACIÓN CUANTITATIVA Y CUALITATIVA, neiva: S.N, 2011.

[37] Hernández Sampieri, Roberto Fernández Collado, Carlos Baptista Lucio, Pilar, METODOLOGÍA DE LA INVESTIGACIÒN, MEXICO: MacGraw-Hill/Interamericana, 2006, 2014.

[38] UNIR - Universidad del internet, «Informática forense: en qué consiste, ámbitos de aplicación y perfiles profesionales,» 24 06 2021. [En línea]. Available: https://www.unir.net/ingenieria/revista/informatica-forense/. [Último acceso: 27 05 2023].

[39] Unir La Universidad en internet, «Informática forense: en qué consiste, ámbitos de aplicación y perfiles profesionales.,» 06 24 2021. [En línea]. Available: https://www.unir.net/ingenieria/revista/informatica-forense/. [Último acceso: 27 05 2023].

[40] Ciberseguridad PYME, «Phishing Suplantando a Netflix,» 04 08 2023. [En línea]. Available: https://www.ciberseguridadpyme.es/actualidad/phishing-suplantando-a-netflix/#:~:text=Los%20ciberdelincuentes%20indican%20en%20el,a%20trav%C3%A9s%20de%20un%20formulario.. [Último acceso: 06 08 2023].

[41] NETFLIX / Centro de Ayuda, «Emails o mensajes sospechosos o de suplantación de identidad supuestamente de Netflix,» S.F S.F 2023. [En línea]. Available: https://help.netflix.com/es/node/65674. [Último acceso: 06 08 2023].

[42] Saint Leo University, «¿Qué es la informática forense?,» 07 10 2022. [En línea]. Available: https://worldcampus.saintleo.edu/noticias/que-es-la-informatica-forense-analisis-forense-informatico. [Último acceso: 09 05 2023].

[43] «Las 20 mejores herramientas forenses digitales de código abierto para 2023,» SalvationData Tecnology, 28 12 2022. [En línea]. Available: https://www.salvationdata.com/work-tips/the-top-20-open-source-digital-forensic-tools-for-2022/. [Último acceso: 27 05 2023].

[44] JEFF - getapp, «GetApp - Software para la investigación forense digital Magnet AXIOM,» 31 07 2022. [En línea]. Available: https://www.getapp.com.co/software/2047816/magnet-axiom. [Último acceso: 29 03 2023].

[45] A. Cervera, «4 Soluciones | Recuperar Archivos Borrados de la Papelera en Mac,» 07 01 2023. [En línea]. Available: https://recoverit.wondershare.es/. [Último acceso: 29 03 2023].

[46] Ondata International, «Recuperar Datos - Recuperación de Datos,» 2023. [En línea]. Available: https://www.ondata.es/recuperar/encase_forensic.htm. [Último acceso: 29 03 2023].

[47] G. -. M. D. 1. A. R. SOFTWARE, «Forensic Toolkit (FTK),» GettApp, 2023. [En línea]. Available: https://www.getapp.com.co/software/2047889/forensic-toolkit-ftk. [Último acceso: 29 03 2023].

[48] ONDATASHOP, «FORENSIC TOOLKIT (FTK),» 2023 2023 2023. [En línea]. Available: https://www.ondata.es/recuperar/ftk-forensic-toolkit.htm#. [Último acceso: 29 03 2023].

[49] X-Ways Software Technology AG, «X-Ways Software Software de informática forense fabricado en Alemania .·,» 2023. [En línea]. Available: https://www.x-ways.net/. [Último acceso: 09 04 2023].

[50] OSGorensics V10, «Analsis forense del sistema operativo V10.,» ACTUALIDAD ACTUALIDAD 2023. [En línea]. Available: https://www.osforensics.com/. [Último acceso: 09 04 2023].

[51] Rafael_L_R, «ISO/IEC 27037:2012 Nueva norma para la Recopilación de Evidencias.,» 23 10 2012. [En línea]. Available: https://peritoit.com/2012/10/23/isoiec-270372012-nueva-norma-para-la-recopilacion-de-evidencias/. [Último acceso: 09 04 2023].

[52] BS 10008, «Garantía de un almacenamiento correcto de la información digital,» 29 05 2020. [En línea]. Available: https://www.bsigroup.com/es-ES/Admisibilidad-legal-de-la-Informacion-Electronica-BS-10008/. [Último acceso: 01 06 2023].

[53] B. H. E. H.Spafford.

[54] Garrido, Antonio, «Fundamentos de programación en C++,» s.f s.f 2005. [En línea]. Available: https://books.google.com.co/books?id=OC17arE5xukC&lpg=PA19&dq=titulo%3A%20Fundamentos%20de%20programaci%C3%B3n%20en%20C%2B%2B%20autor%3A%20Antonio%20Garrido%20Carrillo&hl=es&pg=PA19#v=onepage&q=titulo:%20Fundamentos%20de%20programaci%C3%B3n%20en%20C++%20a. [Último acceso: 17 09 2022].

[55] Carlos Alcívar Trejo, Gustavo Arturo Domenech Alvarez, Karla Maribel Ortìz Chimbo, «La seguridad jurídica frente a los delitos informáticos,» *Pensamiento penal,* vol. 1, nº S.INF, p. 17, 31 08 2016.

[56] Nidia Callegari, «Delitos Informáticos: Generalidades,» OEA, 2016. [En línea]. Available: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf. [Último acceso: 18 09 2022].

[57] Félix Antonio Guevara Gamboa, «Computación Paso a Paso,» de *Paso a Paso Office 2013*, 1 ed., S.N, Megacorp Editorial, 2013, p. 36.

[58] Espitia Muñoz, Wilmer, Espitia Ruiz, Jorge Heli, «Análisis forense en discos duros magnéticos y de estado sólido,» S.F S.F 2014. [En línea]. Available: http://polux.unipiloto.edu.co:8080/00001357.pdf. [Último acceso: 18 09 2022].

[59] Angel Luis Sanchez Iglesias, «Disco duro SSD, ¿Qué es?,» 01 11 2019. [En línea]. Available: http://computadoras.about.com/od/preguntas-frecuentes/a/Que-Es-Un-Disco-Duro-Ssd.htm. [Último acceso: 18 09 2022].

[60] M. TIC, «COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA.,» 28 03 2016. [En línea].

[61] FISCALÍA GENERAL DE LA NACIÓN, «Manual del sistema de Cadena de Custodia,» 2018. [En línea]. Available: https://www.fiscalia.gov.co/colombia/wp-content/uploads/MANUAL-DEL-SISTEMA-DE-CADENA-DE-CUSTODIA.pdf. [Último acceso: 18 09 2022].

[62] TÉRMENS, Miquel, «Preservación digital,» Editorial UOC, 2014. [En línea]. Available: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/57604?page=20. [Último acceso: 18 09 2022].

COMPROMISO PARA EL DESARROLLO DE TRABAJOS DE GRADO

Fecha	29	08	2023

Información general

Título del Trabajo de Grado	MANUAL DE BUENAS PRÁCTICAS UTILIZANDO HERRAMIENTAS DE ANALISIS FORENSE DIGITAL EN UNIDADES DE ALMACENAMIENTO.
Modalidad	Proyecto de grado

Estudiante(s)

Nombre completo	Adrián José Barrios Vergara
Cédula de ciudadanía	1233343655
Programa	Especialización en Ciberseguridad

Nombre completo	
Cédula de ciudadanía	
Programa	

Nombre completo	
Cédula de ciudadanía	
Programa	

Asesor(es)

Nombre completo	Juan Fernando Hurtado Rivera
Cédula de ciudadanía	98647456
Departamento	Sistemas

Nombre completo	
Cédula de ciudadanía	
Departamento	

El(Los) asesor(es) del trabajo de grado en mención se compromete(n) con los siguientes deberes:

a) Orientar el desarrollo técnico y metodológico necesario para cumplir con los objetivos definidos en el trabajo de grado.
b) Hacer seguimiento del cronograma aprobado.
c) Informar al Comité de Trabajos de Grado de la Facultad sobre cualquier anomalía en relación con el desarrollo del trabajo de grado.
d) Cumplir y velar por el respeto a las normas de propiedad intelectual y derechos de autor.

El(Los) estudiante(s) se compromete(n) con los siguientes deberes:

a) Manejar de forma confidencial la información institucional a la cual tendrá acceso en virtud del desarrollo del trabajo de grado, a usarla única y exclusivamente para los fines del trabajo de grado mencionado y a no revelarla directa o indirectamente a ninguna persona, durante

la vigencia de este trabajo, ni después de su terminación. En caso de violar la confidencialidad a la que se compromete responderá en los términos de ley y normativa interna de la Institución.

b) Respetar la propiedad intelectual de terceros y con ello evitar el plagio u otra clase de reclamación que al respecto pudiera sobrevenir y que resulte violatoria de los derechos de autor y relativos a la propiedad intelectual.

c) Asumir toda la responsabilidad en caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión.

d) Abstenerse de llevar a cabo cualquier actuación que implique la comisión de falta disciplinaria o delito, tales como falsificación de firmas o su uso indebido, suplantación, alteración de documentos públicos o privados, y demás actuaciones que atenten contra la fe pública.

Los aspectos relacionados con la propiedad intelectual del trabajo de grado se regirán de acuerdo con lo establecido en el Estatuto de Propiedad Intelectual del Instituto Tecnológico Metropolitano - ITM, Acuerdo No. 34 de julio 23 de 2013 del Consejo Directivo.

En señal de aceptación se firma este documento.

FIRMA ESTUDIANTES 

FIRMA ASESORES 

FECHA ENTREGA: 29/08/2023