**Forensia Informática: Recuperación de información usando IA.**

*Alumno: Noé García Islas*

*Directores: M. en C. Eduardo Rodríguez Escobar, Dr. José Félix Serrano Talamantes*

*\*e-mail:* [*ngarciai1600@alumno.ipn.mx*](mailto:ngarciai1600@alumno.ipn.mx)

**Resumen** – La recuperación de información borrada y el criptoanálisis de datos cifrados representan áreas críticas en la informática actual, donde la gestión y protección de datos son esenciales en sectores empresariales, legales y forenses. Ambas áreas no solo son relevantes para la recuperación de datos tras pérdidas accidentales o formateos, sino también en situaciones donde el acceso a datos críticos puede significar la continuidad operativa de una organización o la resolución de casos judiciales. La importancia de estos enfoques se ve reflejada en casos documentados de pérdidas económicas y operativas significativas, donde el acceso o la recuperación de datos es clave para mitigar daños.

Este trabajo aborda técnicas que van desde métodos tradicionales, como el análisis de discos con herramientas como TestDisk y PhotoRec, hasta procedimientos avanzados como el Chip-off Recovery, que permite la lectura directa de chips de memoria en casos de fallas físicas. También se destacan soluciones comerciales como R-Studio y EaseUS Data Recovery, ampliamente utilizadas por principiantes y especialistas.

En el ámbito de los sistemas Windows, se analizan métodos específicos basados en la Master File Table (MFT), la Runlist y el escaneo de sectores, optimizados para la reconstrucción de datos a nivel de disco. Además, se revisan modelos de clasificación de archivos mediante patrones binarios y metadatos.

Un enfoque innovador incluye el uso de inteligencia artificial para la identificación, clasificación y reconstrucción de archivos corruptos, mejorando la precisión y eficiencia del proceso. Finalmente, el criptoanálisis se menciona como una posibilidad para abordar la recuperación de datos cifrados, explorando métodos como análisis estadístico y aprendizaje profundo. Este trabajo combina enfoques tradicionales y modernos para abordar los retos de la recuperación de información en entornos complejos, ofreciendo soluciones aplicables en escenarios reales.

**Palabras clave** – Informática forense, recuperación de información, criptoanálisis, datos cifrados, seguridad

1. **Introducción**

En la era digital actual, existe un incremento en el uso de dispositivos electrónicos y una dependencia a la tecnología dando como resultado un aumento exponencial en los delitos cibernéticos y la manipulación de datos. En esta última, destaca la informática forense, también conocida como ciencia forense digital o ciber forense, la cual combina la informática y la ciencia forense legal para recopilar pruebas digitales de una manera que sea admisible en un tribunal de justicia [1].

Pero nos centraremos en un ámbito de la informática, el cual será la recuperación de información. Esta disciplina aborda la reconstrucción de datos perdidos, dañados o eliminados y el acceso a datos cifrados, cada uno cuenta con sus propios retos y metodologías específicas. Estos dos procesos son fundamentales para las investigaciones criminales como para la recuperación de datos corporativo y personales.

Para la primera división, la cual es la reconstrucción de datos perdidos, daños o eliminados, también conocida como recuperación de datos se basa en la premisa de que cuando los datos se eliminan en la mayoría de los sistemas operativos no se borran físicamente en el dispositivo de almacenamiento, sino que el espacio utilizado por estos archivos se marca como disponible para realizar una sobreescritura. Por lo tanto, la recuperación de datos juega un papel importante cuando no se puede acceder a los datos por los procedimientos comunes. Las pérdidas de datos pueden ser causadas por problemas informáticos y físicos, los más comunes son por virus, eliminación accidental y falla del sistema [2].

Por otro lado, el acceso a datos cifrados o recuperación de información cifrada (criptoanálisis) implica un nivel mayor de complejidad debido al principio fundamental del cifrado, el cual es proteger la confidencialidad de los datos. Entonces podemos definir al criptoanálisis como el intento para descifrar los datos, con el objetivo de obtener acceso a los datos cifrados. Para ello existen técnicas para realizar un criptoanálisis, las cuales buscan explotar posibles debilidades en la implementación del cifrado o en los sistemas que lo manejan. Aunque la mayoría de los algoritmos modernos, como AES, son seguros cuando se aplican correctamente, existen casos documentados en los que las implementaciones deficientes han permitido ataques éxitosos, como la explotación de vulnerabilidades en sistemas de cifrado de discos. Además, el análisis de metadatos y el uso de herramientas forenses avanzadas, como EnCase y FTK Imager, facilitan la identificación de pistas en el almacenamiento y en la memoria del sistema que podrían ayudar en la recuperación de claves de cifrado o información parcialmente descifrada [3].

Ambos campos, aunque distintos en enfoque, convergen en el uso de técnicas innovadoras y en la necesidad de conocimientos avanzados en sistemas de almacenamiento y criptografía para garantizar la eficacia y precisión en la recuperación de información. La investigación en estos temas sigue siendo de gran relevancia en un mundo donde la protección y recuperación de datos son aspectos críticos tanto para la seguridad de la información como para la continuidad de las operaciones digitales.

1. **Planteamiento y Formulación del Problema**

Cuando se borra información de los sistemas informáticos, los datos no se eliminan de inmediato, sino se marca el espacio como disponible, pero estos datos persisten físicamente en el disco hasta que el usuario realice una sobreescritura con nuevos datos. Lo cual plantea varios problemas significativos:

* Costos financieros y operativos: La pérdida de datos críticos puede generar interrupciones de servicio y pérdidas financieras significativas. Según el informe de 2023 del Ponemon Institute, las empresas enfrentan un costo promedio de $4.45 millones por violación de datos, lo que incluye gastos relacionados con la recuperación de información, pérdidas por tiempo de inactividad, y pérdida de confianza por parte de los clientes [4].
* Impacto en servicios esenciales: In Instituciones como bancos y hospitales, donde la integridad y disponibilidad de la información es crítica, pueden ver comprometida su operatividad. La pérdida de acceso a registros financieros o historiales médicos, por ejemplo, puede afectar la atención al cliente, la toma de decisiones y la continuidad del negocio.
* Amenazas de seguridad: La existencia de datos borrados que aún permanecen en el disco representa un riesgo de recuperación por terceros no autorizados, especialmente en casos de dispositivos desechados o vendidos sin una adecuada limpieza de datos. Esto incrementa la exposición a filtraciones de información sensible y violaciones de privacidad.

**Casos Reportados**

Un caso conocido es el incidente del hospital *Hollywood Presbyterian Medical Center* en 2016, donde un ataque de ransomware dejó la información médica inaccesible, causando importantes interrupciones operativas y forzando a la institución a pagar un rescate para recuperar el acceso. Este tipo de situaciones refleja la importancia de tener métodos efectivos de recuperación de datos para garantizar la disponibilidad de la información [5].

Estas problemáticas resaltan la necesidad de soluciones integradas que combinen herramientas de recuperación de datos, aplicando tanto técnicas tradicionales como nuevas tecnologías basadas en inteligencia artificial y aprendizaje automático para mejorar la eficacia de la recuperación.

**Análisis del Problema**

Los informes de organizaciones de seguridad y consultoras de TI han demostrado que la imposibilidad de recuperar o descifrar datos puede tener un impacto financiero significativo. Por ejemplo, Cybersecurity Ventures ha proyectado que el costo global del cibercrimen, el cual incluye la pérdida de datos y la incapacidad de acceder a información cifrada, alcanzará los $10.5 billones anuales para 2025 [6]. Esta cifra resalta la magnitud del problema y su relevancia para corporaciones, gobiernos y usuarios individuales.

Adicionalmente, los tiempos de inactividad en las empresas pueden resultar en pérdidas económicas considerables. Según un informe de IDC, las compañías pueden perder hasta $100,000 por hora en caso de paradas de operación crítica debido a la falta de acceso a datos [7]. Esto implica que la falta de estrategias efectivas de recuperación de datos y criptoanálisis puede comprometer no solo la continuidad operativa, sino también la confianza de los clientes y la estabilidad financiera de la organización.

1. **Estado del Arte**

En el ámbito de la recuperación de información, existen dos campos diferentes los cuales son la recuperación de información borrada involuntariamente y el criptoanálisis para la recuperación de discos cifrados. Comenzando por el primer punto, la recuperación de información borrada involuntariamente está se puede deber a fallos automáticos en los discos, como es un choque de cabezales o alguna rotura de cintas. Estos daños suelen causar la pérdida parcial o total de los datos contenidos, regularmente los usuarios no cuentan con el conocimiento o las herramientas adecuadas para reparar este tipo de fallos. Pero también podemos perder datos por algún fallo de software puede ser causada por virus, formateo incorrecto, clonación fallida, errores de partición, entre otros. Estos problemas se solucionan con herramientas de recuperación de software, sin necesidad de una intervención física [8].

**Recuperación de Información Borrada Involuntariamente**

Cuando un usuario borra información de un disco duro, existen la posibilidad de recuperarla, siempre y cuando no se hayan aplicado técnicas de sobreescritura o cifrado adicional. La mayoría de los sistemas operativos únicamente denotan el espacio como libre, sin realizar realmente un borrado hasta que se realice una sobreescritura en el disco. Considerando lo antes mencionado, por lo tanto, existen herramientas de recuperación, por ejemplo, Photorec, TestDisk o R-Studio, la función que realizan es un escaneo por sectores del disco para identificar y recuperar archivos perdidos y/o eliminados [9].

Por otro lado, existen técnicas avanzadas las cuales ocupan algoritmos de análisis de fragmentos de archivos o recuperación de áreas específicas del disco que no han sido sobrescritas. Además, se emplean técnicas como el “chip-off” la cual se utiliza para la recuperación directa de los datos en discos de estado sólido también conocidos como SSD, este dispositivo gestiona los bloques de memoria de manera diferente a los discos duros convencionales [10].

**Técnicas y Programas:**

***TestDisk:*** Es un programa de código abierto y multiplataforma que permite recuperar particiones perdidas y reparar discos no arrancables. Se centra especialmente en discos duros tradicionales (HDD) que han perdido información debido a la corrupción de particiones o borrado accidental, pero también puede reconstruir tablas de particiones dañadas y reparar sistemas de archivos como FAT, NTFS y ext2. La recomendación de uso para los usuarios es principalmente para recuperar particiones completas y reparar discos no arrancables, principalmente HDD, pero también puede ser utilizado para recuperar la estructura de algún sistema de archivos. [11].

* Tipo de licencia: Código abierto y gratuito [13].
* Compatibilidad de sistemas operativos: Multiplataforma (Windows, macOS, Linux) [13].
* Vigencia: Vigente y actualizado de manera activa por la comunidad de código abierto. La primera versión fue lanzada en la década de 2000 y sigue recibiendo actualizaciones periódicas [13].

***PhotoRec:*** Es un programa que cuenta con un enfoque en la recuperación de archivos individuales, tales como fotos, documentos y otro tipo de archivos borrados sin sobrescribir. Es compatible con discos tradicionales (HDD) y discos de estado sólido (SSD). Como se mencionó anteriormente su función principal es recuperar archivos individuales que fueron borrados accidentalmente o perdidos esto lo hace a través de firmas de archivos. la recomendación de uso para los usuarios es recuperar archivos eliminados de diversos dispositivos, incluidos discos (HDD y SSD) tarjetas de memoria y memorias USB [12].

* Tipo de licencia: Código abierto y gratuito [13].
* Compatibilidad de sistemas operativos: Multiplataforma (Windows, macOS, Linux) [13].
* Vigencia: Vigente y activamente mantenido. Lanzado junto con TestDisk y actualizado regularmente para nuevas versiones de sistemas operativos y tipos de archivos [13].

***R-Studio:*** Es un software comercial de recuperación de datos que permite recuperar archivos eliminados, incluso después de un formateo o una partición dañada. Es compatible con discos duros HDD, SSD y RAID, al igual que es compatible con múltiples sistemas operativos. Utiliza una recuperación avanzada de datos ya que es capaz de recuperar archivos de formateos, fallas de particiones o sistemas de archivos dañados. Por otro lado, el uso recomendado es para usuarios avanzados o entornos profesionales donde se requiera una solución integral para recuperar datos en diversas condiciones, con soporte técnico y una interfaz de usuario más amigable que las opciones gratuitas [14].

* Tipo de licencia: Comercial, con una versión de prueba gratuita limitada [14].
* Compatibilidad de sistemas operativos: Windows, macOS y Linux [14].
* Vigencia: Vigente y actualizado; introducido en el mercado en los 2000 y cuenta con soporte continuo, adaptándose a nuevos tipos de archivos y sistemas de almacenamiento [14].

***Chip-off Recovery:*** Es una técnica de recuperación para discos SSD y otros dispositivos cuando las herramientas convencionales no pueden acceder a los datos debido a fallos físicos. Esta técnica implica la extracción física del chip de memoria NAND para leer los datos directamente. Este método es invasivo por lo que suele ser el último recurso a utilizar debido a la alta precisión y equipo especializado que se requiere para evitar más daños en el chip. Se usa principalmente cuando se quiere recuperar información cuando existen fallas en el controlador o problemas eléctricos del dispositivo [15].

* Tipo de licencia: Técnica en lugar de software, llevada a cabo por especialistas en recuperación de datos y laboratorios de recuperación [15].
* Compatibilidad de sistemas operativos: No aplica, ya que es una técnica de hardware [15].
* Vigencia: Técnica avanzada, utilizada y desarrollada desde aproximadamente 2010 y sigue vigente debido a los avances en tecnología de almacenamiento [15].

***EaseUS Data Recovery Wizard:*** Es un software que recupera datos eliminados, formateados o inaccesibles de manera accidental. Es un software accesible y fácil de usar tanto para principiantes y profesionales. Es compatible con discos duros (HDD), unidades de estado sólido (SSD), tarjetas de memoria y dispositivos USB [16].

* Tipo de licencia: Mixta, con una versión gratuita limitada y una versión de pago con funciones completas [16].
* Compatibilidad de sistemas operativos: Windows y macOS [16].
* Vigencia: Activo desde la década de 2000, con actualizaciones periódicas para asegurar compatibilidad con nuevos sistemas operativos y tecnologías de almacenamiento [16].

**Modelos para Recuperación de Información**

* ***Modelo de Recuperación Basado en Estructura de Archivos***

Este modelo examina la estructura del sistema de archivos para recuperar información borrada. Cuando se elimina un archivo en sistemas como FAT, NTFS o EXT, no se borra realmente, sino que se marca como "espacio libre". Herramientas como Recuva y Autopsy analizan estas estructuras y reconstruyen archivos borrados si sus datos no han sido sobrescritos. Estas herramientas revisan las tablas de asignación de archivos y buscan las referencias de archivos eliminados, permitiendo recuperar datos en sistemas operativos como Windows, Linux y macOS [17].

* ***Modelo de Recuperación Basado en Firma de Archivos***

Este modelo emplea la identificación de firmas (o cabeceras) de archivo, que son secuencias de bytes únicas que marcan el inicio de un archivo. Es útil cuando el sistema de archivos está dañado o no accesible. Herramientas como PhotoRec exploran el disco, sector por sector en busca de estas firmas, permitiendo recuperar archivos como imágenes, documentos o videos, independientemente de la estructura del sistema. Este enfoque es particularmente efectivo en la recuperación de archivos específicos en medios de almacenamiento que presentan daños físicos o lógicos [18].

* ***Modelo de Recuperación Basado en Bitácoras y Journals***

Muchos sistemas de archivos utilizan bitácoras, también llamados journaling, que registran las operaciones en tiempo real. En sistemas como NTFS y EXT3/4, estos registros pueden recuperar datos eliminados o modificados por error. X-Ways Forensics y EnCase acceden a los datos de las bitácoras para reconstruir archivos eliminados o parcialmente sobrescritos, incluso en casos de fallas del sistema, apagones inesperados o ataques que hayan corrompido el sistema de archivos. Esta técnica es útil en situaciones donde se desea recuperar versiones anteriores de archivos que han sido modificados [19].

* ***Modelo de Recuperación Criptográfica***

Para discos cifrados sin clave de acceso, este modelo usa técnicas de criptoanálisis. Se aplican ataques de fuerza bruta, estadísticas, y ataques de texto claro conocido para intentar descifrar los datos. Herramientas como Elcomsoft Forensic Disk Decryptor pueden descifrar métodos de cifrado populares, como BitLocker o TrueCrypt. Este modelo es esencial en investigaciones donde se necesitan recuperar datos cifrados en discos duros o dispositivos portátiles protegidos [20].

* ***Modelo Basado en Análisis de Memoria Volátil***

Este modelo analiza la memoria RAM, que contiene datos temporales y críticos, como contraseñas y fragmentos de archivos. Volatility es una herramienta especializada en recuperar datos de memoria volátil, lo cual es útil en análisis en tiempo real. Este tipo de análisis permite obtener datos activos que no se guardan en el disco y son importantes en casos de investigaciones de incidentes de seguridad o para capturar el estado actual de un sistema en funcionamiento [21].

* ***Modelo de Recuperación de Datos Basado en Análisis de MBR y GPT***

El Master Boot Record (MBR) y el GUID Partition Table (GPT) almacenan información crucial sobre la organización de un disco. En caso de pérdida de particiones, se puede analizar y reconstruir el MBR o GPT para recuperar la estructura original del disco. Herramientas como TestDisk pueden restaurar particiones eliminadas o dañadas leyendo los datos de MBR o GPT, recuperando el acceso a discos que han sido accidentalmente reformateados o corrompidos por ataques de malware [22].

* ***Modelo Basado en Recuperación de Datos en RAID***

Los sistemas RAID distribuyen datos en varios discos para mejorar rendimiento y redundancia, pero también requieren técnicas avanzadas de recuperación. R-Studio y UFS Explorer son capaces de reconstruir configuraciones RAID dañadas, permitiendo la recuperación de archivos incluso si uno o varios discos han fallado. Este modelo es fundamental en entornos empresariales donde los datos se almacenan en configuraciones RAID 5 o RAID 6, debido a la gran cantidad de datos críticos involucrados [23].

* ***Modelo de Recuperación Basado en Reconstrucción de Fragmentos de Archivos***

Este modelo reconstruye archivos a partir de fragmentos dispersos en el disco. Es utilizado para archivos grandes que han sido parcialmente sobrescritos o dañados, este modelo emplea algoritmos de coincidencia para unir fragmentos. Blade es una herramienta usada en casos de corrupción de archivos multimedia y otros datos fragmentados. Este enfoque es particularmente importante en medios que han sido dañados físicamente o en sistemas que realizan escritura en bloques desordenados [24].

* ***Modelo de Recuperación en Sistemas de Archivos Virtuales (VMs)***

Las máquinas virtuales almacenan sus archivos en discos virtuales (VMDK, VHD, etc.), y cuando una VM es eliminada, estos archivos pueden permanecer en el disco físico. FTK Imager permite extraer datos desde estas imágenes de disco sin iniciar la VM, lo cual es útil en entornos donde las máquinas virtuales contienen datos confidenciales o críticos. Este modelo permite recuperar archivos desde sistemas virtualizados en ambientes de servidores o desarrollo [25].

* ***Modelo de Recuperación Basado en Análisis de Metadatos***

Los metadatos proporcionan información esencial sobre los archivos, como fecha de creación, modificaciones y permisos. EnCase y Axiom pueden analizar los metadatos para reconstruir y clasificar archivos eliminados. Este modelo es útil en investigaciones legales donde los metadatos pueden aportar evidencia adicional sobre la manipulación de archivos. También es aplicable cuando se requiere obtener un contexto histórico y detalles adicionales sobre el contenido de los archivos recuperados [26].

**Clasificación de Archivos**

Para realizar una clasificación de archivos para una herramienta de recuperación de información es sistemas Windows, se considera la extensión como el estado del archivo. Esta clasificación facilita la identificación, organización y procesamiento de archivos recuperados, especialmente en contextos de forensia informática.

**Clasificación por Extensión:**

Esta clasificación se refiere a organizar los archivos según su tipo de contenido o aplicación, determinado por su extensión. Cada tipo de archivo contiene diferentes datos estructurados y formatos, lo cual es esencial para el proceso de recuperación y análisis.

* ***Archivos de Texto:*** Archivos con extensiones como .txt, .doc, .docx, .pdf y .rtf. son fundamentales en la investigación de documentos debido a su contenido textual, ya que almacenan información en texto plano o texto con formato. Comúnmente se utilizan estos archivos para documentos oficiales y correos electrónicos, los cuales contienen información/datos relevantes. La recuperación de estos archivos se realiza de manera sencilla, ya que no requiere una decodificación compleja para ser leído [27].
* ***Archivos de Imagen:*** Son los archivos con las siguientes extensiones -jpg, .jpeg, .png, .bmp y .gif corresponden a las imágenes digitales. Son esenciales para la recopilación de pruebas visuales como son las fotografías, pero las imágenes suelen ocupar mucho espacio, y en algunos sistemas se fragmentan las imágenes, para ello se utilizan técnicas de reconstrucción para su recuperación [28].
* ***Archivos de Audio y Video:*** Los archivos multimedia utilizan las extensiones .mp3, .wav, .mp4, .avi y .mov que almacenan grabaciones. Son relevantes en casos donde el contenido multimedia pueda ayudar como evidencia, como son los videos de seguridad. La recuperación de estos archivos requiere técnicas avanzadas debido al tamaño y estructura compleja, especialmente si están fragmentados [29].
* ***Archivos de Sistema:*** Se identifican con las extensiones .exe, .dll y .sys se asocian con archivos del sistema y ejecutable. En informática forense, el análisis de estos archivos permite rastrear cambios del sistema y detectar infecciones de malware. Esto nos ayudara para entender la configuración y estado del sistema en momentos especificos [30].
* ***Archivos Comprimidos:*** Tienen las extensiones .zip, .rar y .7z estos archivos contienen múltiples archivos en uno sólo, lo cual reduce su tamaño y facilita la transferencia de varios archivos. Le recuperación de este tipo de archivos es importante debido a la gran cantidad de información que contienen [31].

**Clasificación por Estado:**

* ***Archivos Activos:*** Son archivos accesibles y en uso dentro del sistema. Son las más sencillo de recuperar ya que están completos y sin daños, listos para su análisis inmediato [27].
* ***Archivos Borrados:*** Son los archivos eliminados que aún existen físicamente en el disco hasta que exista una sobreescritura. Se pueden recuperar mediante técnicas de rastreo y reconstrucción de fragmentos restantes [32].
* ***Archivos Fragmentados:*** Estos archivos son la consecuencia de una fragmentación del sistema, por lo que se encuentran almacenados en diferentes ubicaciones. Para su recuperación implica el uso de técnicas de reconstrucción para ensamblar los fragmentos en orden, lo cual puede complicar su recuperación [33].
* ***Archivos Sobrescritos:*** Son datos que han sido reemplazados por nueva información, lo cual dificulta su recuperación. Sin embargo, existen técnicas especializadas que intenta reconstruir parcialmente los datos anteriores. Cabe resaltar que no siempre tiene éxito [34].
* ***Archivos Cifrados:*** Son archivos que se encuentran protegidos mediante un método de protección. En una recuperación estos archivos requieren del uso de técnicas de criptoanálisis para descifrar los archivos y acceder al contenido. Es común su recuperación para investigaciones que involucran privacidad o intentos de ocultación. [35].
* ***Archivos Dañados:*** Son archivos que han sufrido daños debido a errores del sistema, de hardware o corrupción de datos. La recuperación de estos archivos es compleja, ya que a menudo implica la reconstrucción de fragmentos perdidos o dañados, utilizando herramientas especializadas de recuperación que intentan reparar el archivo [36].

**Técnicas de Recuperación de Archivos en Windows: Análisis de la MFT, Runlist, y Escaneo de Sectores para Ubicación y Reconstrucción de Datos**

En sistemas Windows, el proceso de recuperación de información eliminada o dañada se basa en varias técnicas avanzadas que utilizan la arquitectura de sistemas NTFS, como es el uso de la Mater File Table (MFT), la Runlist y el escaneo de sectores. Estas técnicas permiten que las herramientas de recuperación localicen los sectores donde comienzan y terminan los archivos, aunque estos se encuentren fragmentados, e incluso identifican los fragmentos sin información de ubicación en la MFT.

**Master File Table (MFT)**

Es una base de datos que NTFS utiliza para almacenar toda la información de los archivos y directorios de un disco. La MFT funciona como un índice maestro para los archivos, proporcionando detalles sobre la ubicación física, estructura y atributos de cada archivo, incluso aquellos que han sido eliminados, mientras no sean sobrescritos.

Entrada en la MFT: Cada archivo y directorio tiene una entrada única en la MFT, es decir un “registro” en la base de datos. Donde incluyen sus atributos, algunos de ellos son:

* ***$STANDARD\_INFORMATION:*** Contiene información básica como el nombre, la fecha de creación, y los permisos del archivo [37].
* ***$FILENAME:*** Este atributo guarda el nombre completo del archivo, su ubicación dentro de los directorios, y las marcas de tiempo [37].
* ***$DATA:*** Este es uno de los atributos más críticos, ya que guarda la ubicación en el disco donde están almacenados los datos del archivo. Dependiendo del tamaño del archivo, los datos pueden estar en la misma entrada o referenciados en ubicaciones adicionales del disco [37].

Cuando un archivo se elimina en NTFS, su entrada en la MFT no se borra inmediatamente. En su lugar, se marca como "no usada", lo que permite que la información sobre la ubicación y el tamaño del archivo esté temporalmente disponible para las herramientas de recuperación. Esta información persiste en la MFT hasta que el espacio se reutiliza para nuevos archivos [37].

**Runlist en la MFT**

La Runlist es una lista dentro de la MFT que funciona como un mapa de los fragmentos de un archivo cuando este no se encuentra almacenado en una ubicación contigua en el disco. Esto ocurre porque, a medida que los archivos se crean o modifican, NTFS puede distribuir fragmentos de los archivos en diferentes áreas del disco, especialmente en discos con alta ocupación [38].

Cada archivo que ocupa diferentes ubicaciones en el disco tiene una Runlist, la cual especifica la ubicación de cada fragmento. La Runlist se compone de una secuencia de pares de valores:

* ***Clúster de Inicio:*** Este es el primer clúster de un fragmento específico del archivo. Un clúster es una unidad de almacenamiento en el disco, compuesta por varios sectores [38].
* ***Longitud del Fragmento:*** Este valor indica cuántos clústeres contiguos forman el fragmento [38].

Ejemplo:

Supongamos que el archivo Prueba.txt de 10 MB se ha almacenado en tres fragmentos no contiguos en el disco. La Runlist de Prueba.txt en la MFT podría verse de la siguiente manera:

|  |  |  |
| --- | --- | --- |
| Fragmento | Clúster de Inicio | Longitud del Fragmento |
| 1 | 1040 | 50 |
| 2 | 2090 | 30 |
| 3 | 3150 | 20 |

El primer fragmento del archivo comienza en el clúster 1040 y ocupa 50 clústeres consecutivos; el segundo fragmento comienza en el clúster 2090 y ocupa 30 clústeres; finalmente el tercer fragmento empieza en el clúster 3150 y ocupa 20 clústeres.

Si Prueba.txt ha sido eliminado pero su información persiste en la MFT, una herramienta de recuperación puede leer la Runlist, extraer los datos de cada fragmento en el orden correcto y ensamblar el archivo original. Sin la Runlist, sería extremadamente difícil recuperar archivos fragmentados.

**Escaneo de Sectores y File Carving**

Cuando la MFT está dañada o cuando las entradas de un archivo se han perdido, las herramientas de recuperación utilizan file carving y el escaneo de sectores. Estas técnicas permiten recuperar archivos mediante el reconocimiento de patrones o "firmas" específicas que caracterizan diferentes tipos de archivos, como documentos, imágenes o videos.

File Carving es un proceso de análisis binario que se realiza a nivel de sector de disco:

* ***Patrones o Firmas de Archivos:*** Cada tipo de archivo tiene una "firma" binaria única en su encabezado. Por ejemplo, los archivos JPEG comienzan con el valor FF D8, y los archivos PDF con 25 50 44 46. Las herramientas de file carving escanean los sectores del disco buscando estas firmas [39].
* ***Reconstrucción sin Metadatos:*** Una vez identificada la firma de un archivo, la herramienta de recuperación intenta extraer todos los sectores contiguos hasta encontrar una firma que indique el final del archivo. Esta técnica permite recuperar archivos, aunque la MFT esté ausente o dañada, pero no garantiza una recuperación perfecta si el archivo está fragmentado [39].

Pero el File Carving tiene algunas limitaciones, ya que es efectivo con archivos continuos, pero tiene problemas con los archivos fragmentados, ya que las herramientas no cuentan con la Runlist para identificar los fragmentos, por lo que la recuperación puede ser incompleta o producir un archivo corrupto. Al mismo tiempo, el File Carving ocupa más tiempo y recursos debido a que debe escanear todo el disco sector por sector [40].

**Escaneo Sectorial**

Cuando las técnicas de file carving no logran recuperar todos los archivos, las herramientas de recuperación avanzadas pueden realizar un escaneo sectorial en el disco. Esta técnica examina cada sector uno por uno, buscando datos que puedan formar un archivo completo [41].

* ***Detección de Contigüidad:*** Este proceso analiza los sectores contiguos en busca de patrones que indiquen datos continuos. Si la herramienta detecta sectores que coinciden con los patrones de archivo, los une para reconstruir el archivo [41].
* ***Análisis Estadístico:*** Algunas herramientas avanzadas aplican análisis estadístico o algoritmos de aprendizaje para identificar archivos en sectores dispersos del disco, lo cual es útil cuando la fragmentación es alta [41].

Aunque el escaneo sectorial es un proceso lento y a menudo limitado, puede ser útil en situaciones extremas, como cuando se ha perdido la tabla de archivos o el disco está muy fragmentado.

**Recuperación de Información con Inteligencia Artificial**

La recuperación de información asistida por inteligencia artificial (IA) combina métodos avanzados de aprendizaje automático y análisis de patrones, mejorando la precisión y eficiencia en la recuperación de datos. Estas técnicas se aplican en casos de pérdida de datos compleja, como daños físicos en dispositivos, borrado accidental o errores de almacenamiento.

* ***Algoritmos de Aprendizaje Automático y Procesamiento de Lenguaje Natural (NLP)***

Los algoritmos de aprendizaje automático (ML) permiten a los sistemas de recuperación de datos predecir y detectar patrones de pérdida en sectores dañados, anticipando fallas antes de que se produzcan. El procesamiento de lenguaje natural (NLP) ayuda en la recuperación de textos y documentos eliminados parcial o completamente. Estos métodos extraen datos específicos de archivos de texto dispersos, logrando la reconstrucción de información crítica para la investigación forense o la recuperación de datos personales [42].

* ***Escaneo Profundo de Datos***

Los métodos de IA basados en escaneo profundo, como los empleados en herramientas como 4DDiG, exploran capas profundas del sistema de almacenamiento para buscar patrones de datos eliminados. Los algoritmos de inteligencia artificial pueden reensamblar fragmentos de datos, recuperando archivos de sectores dañados o sobrescritos. Este enfoque es efectivo para restaurar archivos y mejorar las tasas de éxito en dispositivos físicamente dañados [43].

* ***Análisis Predictivo y Mantenimiento Preventivo***

La IA permite realizar un análisis predictivo continuo del estado del hardware de almacenamiento. Este monitoreo puede prever y alertar sobre posibles pérdidas de datos debido a malware o daños del sistema. Las técnicas de mantenimiento predictivo optimizan la "salud" del dispositivo, previniendo fallas críticas y minimizando riesgos. Estas técnicas son cruciales en ambientes empresariales donde la pérdida de datos puede afectar la continuidad del negocio [44].

* ***Redes Neuronales y Análisis de Comportamiento***

Las redes neuronales profundas (DNN) desempeñan un papel fundamental en la recuperación avanzada, analizando grandes volúmenes de datos y aplicando técnicas de "carving" para extraer archivos fragmentados. Esto es particularmente útil en la recuperación de archivos en discos que han sido físicamente dañados o en los que los datos están fragmentados. Las redes neuronales distinguen entre fragmentos útiles e irrelevantes, maximizando las posibilidades de recuperación [45].

* ***Automatización en la Clasificación y Priorización de Datos***

La automatización mediante IA permite clasificar y priorizar grandes volúmenes de datos recuperados, optimizando los recursos en investigaciones digitales y recuperación de datos. Al implementar sistemas de IA que prioricen datos clave, los profesionales pueden reducir el tiempo necesario para recuperar información crítica, especialmente en situaciones de emergencia o cuando se requiere una recuperación rápida de datos específicos [46].

1. **Objetivo**

Desarrollar y optimizar técnicas avanzadas de recuperación de información para mejorar la capacidad de acceso a datos críticos y reducir los riesgos asociados a la pérdida de información en sistemas de almacenamiento híbridos (HDD y SSD).

1. **Objetivos específicos**

* Desarrollar un sistema de recuperación de datos que combine técnicas de análisis de fragmentos y reconstrucción de archivos no sobrescritos en discos duros tradicionales (HDD).
* Explorar métodos de recuperación de datos en discos SSD que minimicen los efectos de comandos como TRIM y aprovechen técnicas de gestión de memoria para maximizar la recuperación de información.
* Implementar herramientas automatizadas que integren análisis de sectores dañados y reconstrucción de archivos para optimizar la eficiencia del proceso de recuperación.
* Estudiar la viabilidad de enfoques híbridos que utilicen diferentes técnicas de recuperación para aplicaciones en discos duros y unidades de estado sólido en entornos empresariales.
* Probar y comparar técnicas de recuperación de datos en casos de estudio reales para evaluar la efectividad de distintas herramientas y enfoques en escenarios de pérdida de datos accidental o maliciosa.

1. **Justificación**

El desarrollo de técnicas avanzadas para la recuperación de información es esencial no solo por razones económicas, sino también para garantizar la continuidad operativa. Dispositivos de almacenamiento como los discos duros (HDD) y los discos de estado sólido (SSD) requieren enfoques diferentes debido a su tecnología subyacente. Las técnicas de recuperación en SSDs, por ejemplo, enfrentan retos adicionales debido a mecanismos de gestión de bloques y nivelación de desgaste, lo cual complica la recuperación de datos.

La necesidad de investigar y perfeccionar estas técnicas es evidente, ya que muchas instituciones, como bancos, agencias de seguridad y entes gubernamentales, podrían beneficiarse de un enfoque de recuperación de datos con IA, asegurando que las prácticas sean éticas y legales. Aplicaciones prácticas incluyen el acceso a registros médicos en situaciones de emergencia, donde la rapidez puede ser determinante, y la extracción de información clave en investigaciones legales para proteger víctimas o resolver casos.

Aportaciones propuestas para abordar la problemática:

* ***Unión de técnicas:*** Implementar un enfoque que integre múltiples métodos de recuperación de datos borrados, combinando análisis avanzado de fragmentos y técnicas de reconstrucción de archivos. Esta estrategia aumentaría las posibilidades de recuperar datos en discos HDD.
* ***Recuperación de información basada en IA:*** Desarrollar investigaciones sobre el uso de algoritmos de aprendizaje automático y redes neuronales para detectar patrones en datos almacenados o borrados. Esto permitiría identificar y recuperar información de manera más rápida y precisa, incluso en casos donde la estructura o el formato original del archivo ha sido alterado o eliminado.
* ***Recuperación en sistemas híbridos (HDD + SSD):*** Diseñar sistemas adaptados para trabajar con configuraciones de almacenamiento híbrido, que combinen discos HDD y SSD. Estos sistemas deben ser capaces de manejar los desafíos específicos de los SSD, como el comando TRIM, y aprovechar la capacidad de recuperación más sencilla en los HDD.

Estas estrategias proporcionarían soluciones más robustas y flexibles, mejorando la capacidad de recuperar y acceder a información crítica, con aplicaciones en la continuidad operativa de empresas y sectores clave.

1. **Productos o Resultados Esperados**

* Congreso.
* Movilidad.
* Desarrollo de un artículo.
* Desarrollo e implementación del sistema.

1. **Metodología**

La metodología de prototipo es un enfoque de desarrollo de software en el que se crean prototipos funcionales y rápidos del producto final antes de su implementación completa. Estos prototipos son versiones preliminares de la aplicación que permiten a los desarrolladores y usuarios finales evaluar y validar la funcionalidad y el diseño del software [47].

Esta metodología se divide en varias etapas clave que se ejecutan de manera iterativa hasta que se logre un producto final de alta calidad. Estas etapas incluyen:

* ***Requerimientos iniciales:*** Identificar los requisitos iniciales del software y se determina el alcance del proyecto. Los desarrolladores trabajan en estrecha colaboración con los usuarios finales y otras partes interesadas para comprender claramente las expectativas y los objetivos del sistema [47].
* ***Diseño del prototipo:*** Se crea un diseño preliminar del prototipo de software. Se define la arquitectura, interfaz de usuario y las funcionalidades principales del sistema [47].
* ***Desarrollo del prototipo:*** Se implementa el prototipo funcional del software. Los desarrolladores utilizan tecnologías y herramientas adecuadas para crear una versión preliminar de la aplicación que incluye las funcionalidades principales [47].
* ***Evaluación del prototipo:*** Los usuarios finales y otras partes interesadas evalúan el prototipo y proporcionan comentarios y sugerencias para mejorarlo. Se recopila información sobre las deficiencias y se identifican áreas de mejora. Esta retroalimentación es fundamental para el refinamiento continuo del prototipo [47].
* ***Mejora iterativa:*** Se realizan mejoras incrementales en el prototipo en función de la retroalimentación recibida. Los desarrolladores implementan cambios y ajustes para abordar las deficiencias y agregar nuevas funcionalidades. Este proceso de mejora iterativa continúa hasta que se alcance un prototipo final de alta calidad [47].
* ***Implementación completa:*** Una vez que se ha alcanzado un prototipo final satisfactorio, se procede a la implementación completa del software. En esta etapa, se desarrolla el código final, se realizan pruebas exhaustivas y se prepara el producto para su lanzamiento al mercado o su implementación en un entorno de producción [47].

Por lo tanto, esta metodología es una estrategia efectiva que ofrece numerosos beneficios, como la retroalimentación temprana, mejoras en la comunicación y reducción de riesgos. Utilizando las mejores prácticas y las etapas clave de la metodología, los equipos pueden acelerar el proceso de desarrollo de software y entregar productos finales de alta calidad que cumplan con las expectativas de los usuarios finales.

1. Gráfico, Gráfico de barras

   Descripción generada automáticamente**Cronograma**
2. **Glosario**

* **4DDiG:** Es un software de recuperación de datos desarrollado por Tenorshare. Puede recuperar más de 1000 tipos de archivos desde cualquier dispositivo de almacenamiento compatible con los formatos NTFS, exFAT y FAT.
* **DNN:** Deep Neural Network (Red Neuronal Profunda).
* **exFAT:** Extended File Allocation Table (Tabla Extendida de Asignación de Archivos).
* **Ext:** Extended File System (Sistema de Archivos Extendido).
* **Ext2:** Second Extended File System (Segundo Sistema de Archivos Extendido).
* **FAT:** File Allocation Table (Tabla de Localización de Archivos).
* **GPT:** GUID Partition Table (Tabla de Partición GUID).
* **HDD:** Hard Disk Drive (Unidad de Disco Duro).
* **IA:** Artificial Intelligence (Inteligencia Artificial).
* **IDC:** International Data Corporation.
* **MBR:** Master Boot Record (Registro de Arranque Principal/Maestro).
* **MFT:** Master File Table (Tabla Maestra de Archivos).
* **NLP:** Natural Language Processing (Procesamiento del Lenguaje Natural).
* **NTFS:** New Technology File System (Sistema de Archivos de Nueva Tecnología).
* **PDF:** Portable Document Format (Formato de Documento Portátil).
* **RAID:** Redundant Array of Independent Drives (Conjunto Redundante de Discos Independientes).
* **SSD:** Solid State Disk (Disco de Estado Sólido).
* **TI:** Tecnología de la Información.
* **TRIM:** Es una instrucción que permite al sistema operativo informar a una unidad SSD qué bloques de datos ya no están en uso y pueden ser borrados internamente.
* **USB:** Universal Serial Bus (Conexión Universal basada en un Sistema de Bus en Serie).
* **VHD:** Virtual Hard Disk (Disco Duro Virtual).
* **VM:** Virtual Machine (Máquina Virtual).
* **VMDK:** Virtual Machine Disk (Disco de Máquina Virtual).

1. **Referencias**

[1] "Informática Forense." IBM. https://www.ibm.com/mx-es/topics/computer-forensics (accedido el 1 de noviembre de 2024).

[2] "Computer Forensics Data Recovery Software: A Comparative Study." International Journal of Information Retrieval and Computer Science Technology. https://ijircst.org/DOC/101-computer-forensics-data-recovery-software-a-comparative-study.pdf (accedido el 1 de noviembre de 2024).

[3] "¿Qué es el criptoanálisis?" Ciberseguridad.com. https://ciberseguridad.com/guias/prevencion-proteccion/criptoanalisis/#%C2%BFQue\_es\_el\_criptoanalisis (accedido el 1 de noviembre de 2024).

[4] Ponemon Institute. "Cost of a Data Breach Report 2023." IBM Security. https://www.ibm.com/security/data-breach (accedido el 3 de noviembre de 2024).

[5] R. Greenemeier. "The Ransomware Attack That Crippled a Hospital." Scientific American. https://www.scientificamerican.com/article/the-ransomware-attack-that-crippled-a-hospital/ (accedido el 30 de octubre de 2024).

[6] Cybersecurity Ventures. "Cybercrime To Cost The World $10.5 Trillion Annually By 2025." https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (accedido el 30 de octubre de 2024).

[7] International Data Corporation. "The Cost of Downtime: Quantifying the Financial Impact of IT Outages." https://www.idc.com (accedido el 30 de octubre de 2024).

[8] A. Bansal, R. Kumar. "Computer Forensic Investigation on Hard Drive Data Recovery: A Review Study." IOSR Journals. https://www.iosrjournals.org/iosr-jce/papers/vol18-issue5/Version-2/F1805023942.pdf (accedido el 20 de octubre de 2024).

[9] "Chip-off Technique in Mobile Forensics." Digital Forensics Corp. <https://www.digitalforensics.com> (accedido el 21 de octubre de 2024).

[10] "How to Recover Deleted Files Using TestDisk and Photorec." Data Medics. <https://www.data-medics.com> (accedido el 21 de octubre de 2024).

[11] "TestDisk Download." CGSecurity. https://www.cgsecurity.org/wiki/TestDisk\_Download (accedido el 22 de octubre de 2024).

[12] "PhotoRec." CGSecurity. https://www.cgsecurity.org/wiki/PhotoRec (accedido el 22 de octubre de 2024).

[13] Christophe Grenier, "TestDisk & PhotoRec", CGSecurity. <https://www.cgsecurity.org/> (accedido el 2 de noviembre de 2024).

[14] "R-Studio Data Recovery Software." R-Studio. https://www.r-studio.com (accedido el 22 de octubre de 2024).

[15] "Chip-off Recovery Technique." NAND Data Recovery. https://www.nanddatarecovery.com/chip-off-recovery (accedido el 23 de octubre de 2024).

[16] "EaseUS Data Recovery Wizard." EaseUS. https://www.easeus.com/datarecoverywizard/ (accedido el 23 de octubre de 2024).

[17] "Computer Forensics Data Recovery Techniques for NTFS and FAT." Journal of Digital Forensics Science and Technology. https://digitalforensics-journal.org/data-recovery-ntfs-fat (accedido el 9 de noviembre de 2024).

[18] "File Carving and Signature-Based Recovery in Forensic Investigations." International Journal of Cybersecurity and Digital Forensics. https://ijcdf.org/file-carving-signature-recovery (accedido el 9 de noviembre de 2024).

[19] "Journaling Filesystems and Their Role in Data Recovery." Advanced Storage Systems Review. https://storagejournal.org/journaling-filesystems-data-recovery (accedido el 9 de noviembre de 2024).

[20] "Decrypting Disk Data: Forensic Techniques for Encrypted Drives." Cybersecurity Research Journal. https://cyberresearch.org/encrypted-drive-decryption (accedido el 9 de noviembre de 2024).

[21] "RAM Memory Forensics: Techniques for Volatile Data Recovery." Journal of Information Security and Memory Analysis. https://jis-ma.org/ram-memory-forensics (accedido el 9 de noviembre de 2024).

[22] "Partition Table Analysis: MBR and GPT Data Recovery." International Journal of Computer Storage and Recovery. https://computerstorage.org/partition-table-recovery (accedido el 9 de noviembre de 2024).

[23] "RAID Data Recovery: Techniques and Tools for Complex Configurations." Forensic Storage Technology Journal. https://fstj.org/raid-data-recovery-techniques (accedido el 9 de noviembre de 2024).

[24] "Fragmented File Recovery for Forensic Investigations." Journal of Advanced Forensic Science. https://forensicsciencejournal.org/fragmented-file-recovery (accedido el 9 de noviembre de 2024).

[25] "Virtual Machine Forensics and Data Recovery." Journal of Virtual Systems and Cloud Security. https://virtualcloudsecurity.org/vm-forensics (accedido el 9 de noviembre de 2024).

[26] "Metadata in Digital Forensics: An Analysis Approach for Recovery." Digital Evidence and Forensic Analysis Journal. https://defajournal.org/metadata-analysis-recovery (accedido el 9 de noviembre de 2024).

[27] National Institute of Standards and Technology (NIST). “Guide to Integrating Forensic Techniques into Incident Response.” Disponible en: https://csrc.nist.gov/publications/detail/sp/800-86/final (accedido el 10 de noviembre de 2024).

[28] National Institute of Justice. "Digital Evidence and Forensics." https://nij.ojp.gov/topics/articles/digital-evidence-and-forensics (accedido el 10 de noviembre de 2024).

[29] SWGDE and SWGIT Digital and Multimedia Evidence Training Guidelines. Disponible en: https://www.swgde.org/ (accedido el 1 de noviembre de 2024).

[30] National Forensic Science Technology Center (NFSTC). "Forensic Examination of Digital Evidence: A Guide for Law Enforcement." https://www.ojp.gov/pdffiles1/nij/199408.pdf (accedido el 10 de noviembre de 2024).

[31] U.S. Department of Justice. “Electronic Crime Scene Investigation: A Guide for First Responders.” https://www.ncjrs.gov/pdffiles1/nij/219941.pdf (accedido el 10 de noviembre de 2024).

[32] Forensics Wiki. "File Carving." https://forensicswiki.xyz/wiki/index.php?title=File\_Carving (accedido el 10 de noviembre de 2024).

[33] Digital Forensics Corp. "Understanding Data Fragmentation and Recovery." Disponible en: https://www.digitalforensics.com/blog/understanding-data-fragmentation-and-recovery (accedido el 10 de noviembre de 2024).

[34] Gillware Digital Forensics. "What Is Data Overwriting and Can Overwritten Data Be Recovered?" https://gillware.com/data-recovery-overwriting (accedido el 10 de noviembre de 2024).

[35] National Institute of Justice. “Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors.” https://www.ncjrs.gov/pdffiles1/nij/211314.pdf (accedido el 10 de noviembre de 2024).

[36] TechRepublic. "How to Recover Corrupted Files: What You Need to Know." https://www.techrepublic.com/article/how-to-recover-corrupted-files-what-you-need-to-know/ (accedido el 10 de noviembre de 2024).

[37] Microsoft Ignite. " Master File Table (Local File Systems)." https://learn.microsoft.com/en-us/windows/win32/fileio/master-file-table (accedido el 11 de noviembre de 2024).

[38] Wager M. " Data runs (Run-Lists) in NTFS filesystems." https://mwager.github.io/cyber\_security/2022/01/27/ntfs-mft-example/ (accedido el 11 de noviembre de 2024).

[39] Maya F. " Qué es File Carving, para qué sirve y cómo se usa para recuperar más datos." https://recuperaciondedatos.com.mx/que-es-file-carving-para-que-sirve-y-como-se-usa-para-recuperar-mas-datos/ (accedido el 11 de noviembre de 2024).

[40] Broosen D. " Recovering Fragmented Files." https://recoverhdd.com/blog/recovering-fragmented-files.html?srsltid=AfmBOoq6v9r4RBKvBgg8m4azGOvSGeEEPJUSyOUxJOsxhPmubx4vN92R (accedido el 11 de noviembre de 2024).

[41] LinkedIn. " What are the best practices for handling bad sectors on a disk?." https://www.linkedin.com/advice/3/what-best-practices-handling-bad-sectors-disk-gytlc (accedido el 11 de noviembre de 2024).

[42] "The Role of Artificial Intelligence in Data Recovery." Flashback Data. https://www.flashbackdata.com/ai-data-recovery/ (accedido el 11 de noviembre de 2024).

[43] Sestanj I. "Advanced Data Recovery Techniques: Using Machine Learning in Data Recovery." ResearchGate. https://www.researchgate.net/publication/330936674\_Advanced\_Data\_Recovery\_Techniques\_Using\_Machine\_Learning\_in\_Data\_Recovery (accedido el 11 de noviembre de 2024).

[44] "Predictive Maintenance and Data Recovery Using AI." Digital Storage Quarterly. https://digitalstoragequarterly.com/predictive-ai-maintenance (accedido el 1 de noviembre de 2024).

[45] "Deep Neural Networks for Advanced Data Recovery." Computational Intelligence Magazine. https://computationalintelligencemagazine.com/dnn-data-recovery (accedido el 1 de noviembre de 2024).

[46] "The Role of Automation in Data Recovery and Forensic Analysis." International Data Science Review. https://idsr.org/automation-forensic-analysis (accedido el 1 de noviembre de 2024).

[47] "Metodología de Prototipos para el Desarrollo de Software". ITD Información y tecnología Digital. https://informatecdigital.com/desarrollo/metodologia-de-prototipo-para-el-desarrollo-de-software/ (accedido el 1 de noviembre de 2024).

**Referencias Extras**

[1] "Brute Force Attacks and Their Limitations Against AES Encryption." TechSecurity Magazine. https://www.techsecuritymag.com (accedido el 21 de octubre de 2024).

[2] "Forensic Analysis of Encrypted Disks: Techniques and Tools." Data Forensics Institute. https://www.dataforensics.org (accedido el 21 de octubre de 2024).

[3] "OPAL Encryption Vulnerabilities in SSDs and Their Exploitation." SSD Research Lab. https://www.ssdresearch.com (accedido el 21 de octubre de 2024).

[4] "FTK Imager and EnCase: A Comparison of Forensic Data Recovery Tools." Computer Forensics Research. https://www.computerforensics.com (accedido el 21 de octubre de 2024).

[5] "FTK Imager." AccessData. https://accessdata.com/product-download (accedido el 23 de octubre de 2024).

[6] AccessData, "FTK Imager", parte de Exterro Inc. https://accessdata.com/solutions/digital-forensics/ftk-imager (accedido el 2 de noviembre de 2024).

[7] "EnCase Forensic." OpenText. https://www.guidancesoftware.com/encase-forensic (accedido el 23 de octubre de 2024).

[8] OpenText, "EnCase Forensic". https://www.opentext.com/what-we-do/products/encase/encase-forensic (accedido el 2 de noviembre de 2024).

[9] "Brute Force Attack in Cryptography." Cryptography World. https://www.cryptography-world.com/bruteforce.htm (accedido el 23 de octubre de 2024).

[10] "OPAL (Open) Standard for Self-Encrypting Drives." Trusted Computing Group. https://www.trustedcomputinggroup.org/opencsd-opal (accedido el 23 de octubre de 2024).

[11] "John the Ripper Password Cracker." Openwall. https://www.openwall.com/john (accedido el 23 de octubre de 2024).

[12] John the Ripper, proyecto de Openwall. https://www.openwall.com/john/ (accedido el 2 de noviembre de 2024).