UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

MAYO 2025 – SEPTIEMBRE 2025

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS COMPARATIVO DE TESTDISK, PHOTOREC Y FOREMOST COMO HERRAMIENTAS FORENSES DE CÓDIGO ABIERTO EN LA RECUPERACIÓN DE DATOS CON KALI LINUX

ESTUDIANTE:

YOELY LIZBETH PAREDES ALAVA

TUTOR:

ING. ENRIQUE ISMAEL DELGADO CUADRO

AÑO 2025

RESUMEN

Este caso de estudio tiene la finalidad de realizar un análisis comparativo entre las herramientas TestDisk, PhotoRec y Foremost las cuales están integradas en Kali Linux y se enfocan en la recuperación de datos, es importante compararlas porque se evalúan aspectos como la eficiencia, facilidad de uso, velocidad y capacidad para recuperar archivos ya que se trata de una investigación de tipo descriptiva con un enfoque tanto documental como práctico, lo que permite comprender mejor los conceptos, funciones, ventajas y desventajas de cada herramienta considerando que cada una trabaja con un estándar de archivos específicos al momento de recuperar información, en la parte práctica se obtuvo varios resultados TestDisk alcanzó un 85% de eficiencia, siendo muy útil para recuperar particiones o tablas dañadas de un disco, aunque tardó aproximadamente dos horas en completar el proceso, por otro lado PhotoRec logró un 90% de eficiencia y se destacó por recuperar la mayoría de archivos firmas mediante un análisis profundo del sistema en solo media hora, finalmente Foremost presentó un 80% de eficiencia con un tiempo estimado de una hora y media, siendo ideal para recuperar archivos a través de cabeceras y extensiones, cabe resaltar que esta investigación no busca demostrar cuál herramienta es la mejor en general, sino identificar cuál es la más adecuada según la situación que se presenta al momento de recuperar la información.

Palabras Claves:

Kali Linux, información, recuperación, herramientas, informática forense.

ABSTRACT

This case study aims to perform a comparative analysis between TestDisk, PhotoRec and Foremost tools which are integrated in Kali Linux and are focused on data recovery, it is important to compare them because aspects such as efficiency, ease of use, speed and ability to recover files are evaluated, speed and capacity to recover files since it is a descriptive research with a documentary and practical approach, which allows to better understand the concepts, functions, advantages and disadvantages of each tool considering that each one works with a specific file standard when recovering information, in the practical part several results were obtained TestDisk reached an 85% of efficiency, being very useful to recover damaged partitions or tables of a disk, although it took approximately two hours to complete the process, on the other hand PhotoRec achieved 90% efficiency and stood out for recovering most signature files through a deep analysis of the system in just half an hour, finally Foremost presented 80% efficiency with an estimated time of an hour and a half, being ideal for recovering files through headers and extensions, it should be noted that this research does not seek to demonstrate which tool is the best in general, but to identify which is the most appropriate according to the situation that arises at the time of recovering the information.

Keywords:

Kali Linux, information, recovery, tools, computer forensics.

ÍNDICE

PLANTEAMIENTO DEL PROBLEMA

La pérdida de datos es un problema muy común tanto en el ámbito personal como institucional, la recuperación de información con herramientas forenses de código abierto son una opción accesible para cualquiera que desee realizar este tipo de proceso, el objetivo es intentar recuperar la mayor cantidad de información posible debido al creciente uso de los dispositivos digitales que ha generado la necesidad de utilizar herramientas especializadas en estos casos.

La pérdida de datos genera un daño crítico, que puede ser desde la interrupción de procesos, la pérdida de evidencias donde afecta la toma de decisiones en las empresas e incluso la imposibilidad de mostrar el rastreo de los hechos de un delito, por eso el campo de la informática forense ha ido adquiriendo cada vez más protagonismo, sobre todo ofreciendo soluciones que permiten la recuperación de la información con precisión, seguridad y trazabilidad.

En el contexto económico y las particularidades del mercado, se puede afirmar que existe una fuerte presencia de herramientas comerciales especializadas para estos casos, muchas de las cuales requieren licencias costosas, teniendo presente que suelen ofrecer interfaces más intuitivas, soporte técnico y funciones avanzadas, no siempre son accesibles para estudiantes, instituciones educativas, pequeñas empresas o equipos de respuesta a incidentes con presupuestos limitados más aún agregando que aquellas dificultades limitan a estas herramientas.

A raíz de esta situación, existe una apertura tecnológica donde las organizaciones que aún están en pleno crecimiento y desarrollo tienen la opción de trabajar con herramientas de código abierto ya que son una alternativa que favorece la ideología de que lo gratis es peor, a pesar de esto las herramientas TestDisk, PhotoRec y Foremost han demostrado en diferentes situaciones ser tan efectivas como sus equivalentes comerciales.

Urge evaluar el verdadero valor técnico y funcional de estas herramientas gratuitas frente al dominio de las soluciones pagadas, no solo para democratizar el acceso a la informática forense, sino también para motivar a usuarios y profesionales a tomar decisiones informadas en base a evidencia, este aspecto del problema plantea una cuestión estratégica teniendo presente la ética en relación con el acceso equitativo de la tecnología especializada en materias consideradas como críticas, por ejemplo la ciberseguridad, la recuperación de datos y la gestión de la prueba digital.

Formulación del problema

¿Cómo las herramientas de código abierto TestDisk, PhotoRec y Foremost, influye en la recuperación de datos con Kali Linux?

JUSTIFICACIÓN

Las herramientas forenses de código abierto son una opción accesible para todos, por tal motivo se seleccionó este tema debido al gran interés que representa en el campo de la informática forense especialmente en la recuperación de datos perdidos o eliminados, en numerosas ocasiones se ha observado cómo las personas pierden información importante y carecen de los conocimientos necesarios para actuar, o asumen que la recuperación de datos ya no es posible, también se definió que las soluciones disponibles en el mercado no están al alcance de todos.

Se decidió investigar las herramientas gratuitas de código abierto ya integradas en Kali Linux, TestDisk, PhotoRec y Foremost dado a la importancia de comprender el funcionamiento, su eficacia y cuándo usar una u otra, además al ser open sources todos pueden usarlas sin pagar licencias lo que las hace mucho más accesibles para estudiantes, técnicos o quienes deseen aprender por su cuenta.

La idea es comparar estas tres herramientas para determinar cuál es la mejor para cada situación, no solo desde una perspectiva técnica, sino también práctica: facilidad de uso, velocidad, tipos de archivos recuperados, de esta manera podemos ayudar a otros a comprender sus opciones si alguna vez necesitan recuperar información y no saben por dónde empezar.

Este análisis también busca contribuir al uso de software libre y demostrar que existen alternativas reales, efectivas y legales para recuperar datos sin recurrir a softwares de alto costo, en este contexto Kali Linux se presenta como un sistema operativo robusto de código abierto con el enfoque en la ciberseguridad y la informática forense, es muy conocido y utilizado por la comunidad de recuperación de datos.

En otras palabras el desarrollo de esta comparativa trata demostrar que estas herramientas no solo sirven para Kali Linux, su amplia compatibilidad con el hardware y el software ayudan a poder trabajar ya sea desde unidades USB e incluso recuperar datos de otros sistemas operativos, como Windows, esta información también es sumamente útil y considerado una forma clara de demostrar que no siempre es necesario invertir dinero para resolver problemas tecnológicos lo que benéfica a todas las herramientas open sources ya que el objetivo de ellas es tratar de brindar su servicio a la comunidad que las rodea.

OBJETIVOS DEL ESTUDIO

1.1 Objetivo General

- Realizar un estudio comparativo de las herramientas forenses TestDisk, PhotoRec y Foremost para la recuperación de los datos.

1.2 Objetivos Específicos

- Analizar la bibliografía de cada una de las herramientas con énfasis en la recuperación de información.
- Hacer pruebas con las herramientas TestDisk, PhotoRec y Foremost para valorar su efectividad en la recuperación de datos.
- Comparar la valorización de las herramientas seleccionadas para la recuperación de información.

LÍNEA DE INVESTIGACIÓN

La línea de investigación: **Sistemas de información y comunicación, emprendimiento e innovación** tiene mucha relación con este estudio en la medida en que trata del uso de herramientas tecnológicas para la recuperación de datos, algo que resulta esencial para la gestión segura de la información digital. Actualmente los datos son uno de los activos más importantes, ya sean documentos personales, archivos de una empresa o incluso evidencias en un proceso judicial. En este sentido este trabajo estudia las herramientas de código abierto TestDisk, PhotoRec y Foremost, a través de la práctica, una forma accesible e innovadora. En este sentido, el hecho de que sean herramientas de código abierto da la posibilidad a la vez de aprender una parte técnica y de ser una base en la que se pueden aplicar emprendimientos, ya sea ofreciendo servicios de recuperación de datos o bien mediante el desarrollo de nuevas soluciones a partir de las infraestructuras que se detallan.

SUBLÍNEA

La sublínea de investigación: **Redes y tecnologías inteligentes de software y hardware** también se encuentra directamente conectada con este caso de estudio, ya que las herramientas analizadas operan a nivel de software e interactúan de forma directa con el hardware del equipo especialmente con los discos duros o unidades de almacenamiento, etc. Estas herramientas permiten recuperar datos incluso cuando el sistema operativo ya no los detecta, lo cual implica un trabajo conjunto entre la lógica del software y el acceso físico a la estructura del disco. Además al desarrollarse en entornos especializados como Kali Linux, este estudio involucra el uso de tecnologías inteligentes aplicadas.

MARCO CONCEPTUAL

Recuperación de datos

Tal y como nos relata Zane Kennedy (2024), en el sector de la informática la recuperación de datos es el conjunto de procesos y técnicas que se realizan para poder acceder a la información que se encuentra almacenada en medio de almacenamiento digital que debido a una avería o defecto del propio medio de almacenamiento no se la puede recuperar de forma habitual.

El proceso de la recuperación de datos puede modularse en función del tipo de medio en el que se almacenen los datos, que sea un disco duro, memorias USB, servidores, cámaras digitales, CD, DVD, etc. La recuperación de datos es necesaria por razones diferentes por ejemplo, por daños físicos en el medio de almacenamiento (averías electrónicas, averías mecánicas, golpes, incendios, inundaciones, etc.) o bien por las averías lógicas (daños en el sistema de archivos, daño en las particiones, archivos borrados, formateos accidentales, etc..).

Por lo tanto, el procedimiento de la recuperación de datos puede ser diverso dependiendo del tipo de medio de almacenamiento y de la naturaleza del daño. Finalmente es bueno hacer notar que no se podrá recuperar los datos perdidos o corruptos dependiendo de cuán fuerte sea el daño.

Según Laboratories (2024), establece que la información que está presente en un dispositivo de almacenamiento intacto se puede recuperar sin la ayuda de un especialista mediante una determinada aplicación. Hay que hacer hincapié, sin embargo en que no se puede recuperar información una vez que haya sido escrita.

Esta es la razón por la que, cuando se desea recuperar un determinado archivo no se debe escribir nada en el dispositivo de almacenamiento hasta haber recuperado todos los archivos que

sea necesario. A la mayoría de las utilidades de recuperación de datos se les aplica el análisis de metadatos y el contenido de recuperación conocido o bien ambos.

Tipos de Pérdida de Datos

Tal como nos refiere tiadmin (2024), existe la pérdida total de datos en el sentido que la información ha desaparecido de forma irrecuperable, lo primero suele estar relacionado con errores en los sistemas de respaldo o en la destrucción física de los medios de almacenamiento a continuación se explican los tipos de pérdidas de datos:

Pérdida temporal: Es la información que está perdida durante un periodo de tiempo corto, pero se puede recuperar no obstante a raíz de esto se lleva a una interrupción muy importante en las operaciones de la empresa.

Corrupción de datos: Los datos no desaparecen por completo, pero la información se convierte en inaccesible y se rompe la relación de los datos con el software o bien con el hardware.

Pérdida parcial: Sólo una parte de la información se pierde o queda inaccesible, este tipo de pérdida puede ser más crítica si existe una relación con información clave, en especial con la base de datos de los clientes o información financiera.

¿Que son los metadatos?

Tal y como indican Laboratories (2024), los metadatos son información de servicio que permanece oculta en el sistema de archivos. Los metadatos nos permiten analizar cómo recuperar las estructuras clave en el almacenamiento donde se almacena la información del lugar donde el contenido de los archivos se encuentra, sus propiedades y la jerarquía de los directorios que van de los subconjuntos de estos archivos a los archivos mismos.

Tal y como indica Docunecta (2021), existen múltiples maneras de clasificar los metadatos la más común y también la más sencilla es la que desarrolla la National Information Standards Organization (NISO). Dicha organización establece tres tipos de metadatos, los metadatos descriptivos que hacen referencia a cómo se identifican y encuentran un archivo a la información que pueden estar representadas por el título, el autor, las palabras o la institución que lo publicó.

A continuación, nos aparecen los metadatos estructurales los cuales son los que nos revelan cuál es la forma de organización de tal información en su interior, como por ejemplo el orden de las páginas de un documento o la forma de un capítulo. Por otro lado tenemos los metadatos administrativos que son los que nos aportan información sobre el origen del recurso, su propiedad intelectual (licencias, derechos de autor, etc) y también como debería conservarse o almacenarse correctamente.

Esta clasificación no solo nos ayuda a gestionar la información digital, sino que también es clave en determinadas ocasiones forenses, como ejemplo de metadatos tenemos Fotografías e imágenes, Materiales escritos, Vídeos, etc.

Métodos comunes de recuperación

Propone Jacob Murel Ph.D (2024), al respecto citando otros de los diferentes métodos de recuperación de datos según la pérdida sufrida. Normalmente cuando un archivo es eliminado o un dispositivo es re-formateado, la información no desaparece en el acto el sistema operativo la marca como espacio disponible. A partir de aquí se pueden aplicar los métodos de recuperación del siguiente modo:

Recuperación desde papelera o historial: Es la forma más básica y acontece cuando los archivos aún no han sido eliminados del todo. En muchas ocasiones se pueden recuperar directamente de la papelera de reciclaje o del historial (versionado) de archivos.

Recuperación mediante escaneo lógico del disco: Utiliza software especializado para analizar los sectores del disco en busca de archivos que aún no han sido sobrescritos (you can use "files not overwritten"). Para ello se usan técnicas como la búsqueda por firmas de archivo (file carving) que admite recuperar archivos de acuerdo a la firma file de los mismos, aunque no existe información sobre su ubicación original.

Recuperación a partir del sistema de archivos: Existen programas que permiten en el caso de que existiera un daño en las estructuras, reconstruir estructuras de bajo nivel, como la tabla de las particiones, el MBR (Master Boot Record) o las tablas FAT/NTFS/ext. Es importante emplear estos tipos de recuperación cuando la pérdida reside en la recuperación de archivos pero no en los mismos.

Recuperación a partir de backup: Si existiesen backups o copias de seguridad (manuales o automáticas) también es posible lograrlo de dicha manera. Esta ejecución de recuperación es útil si la pérdida es absoluta o si el disco está dañado físicamente.

Recuperación en laboratorio (hardware): En situaciones más complejas es posible que el daño esté en el disco, en cuyo caso es preciso dejar el dispositivo abierto en entornos controlados. Se utilizan herramientas que permiten clonar el disco o recuperar datos de componentes internos.

Informática forense

Como pone de manifiesto Kassandra Ortega (2022), la informática forense (también conocida como cómputo forense, computación forense o análisis forense digital o análisis forense informático) es aquella tecnología encargada de abordar la recolección, la preservación y de la observación de evidencias cuando se presenta un fallo de seguridad ya sea en sistemas informáticos, redes de ordenadores, dispositivos móviles, correos electrónicos, discos duros, entre otros sistemas informáticos.

Tal disciplina presenta una combinación de elementos del derecho y la informática a partir de ellos permitir el futuro análisis de datos, siendo también considerada una rama de ciberseguridad que comprendería el hacking ético. Las evidencias detectadas serán una guía para los expertos en seguridad informática permitiendo determinar el origen del ciberataque y a la vez servir como prueba para un futuro proceso judicial.

¿Qué es Kali Linux?

Tal como indican g0tmi1k (2025), Kali Linux (el cual anteriormente era conocido como BackTrack Linux) es una distribución de Linux de código abierto basada sobre Debian que permite realizar concretas pruebas de penetración y auditorías de seguridad muy avanzadas. La distribución funciona de forma muy precisa en diferentes plataformas siendo gratuita y permitiendo así su uso para profesionales en este tipo de práctica de evaluación de seguridad.

En palabras de Morgan (2021), La distribución contiene centenares de herramientas, configuraciones y scripts con modificaciones específicas de la industria para que los usuarios puedan dedicarse exclusivamente a tareas de análisis forense informático, de ingeniería inversa y

de detección de vulnerabilidades, entre otras herramientas y no a todo aquello que no esté relacionado con las pruebas.

Siguiendo la visión de Jafar Hasan (2024), Kali Linux es conocido por estar orientado a la seguridad y por su gran colección de herramientas que aplica. Estas herramientas incluyen utilidades de escaneo de red, marcos de pruebas de penetración, herramientas de evaluación de vulnerabilidades, herramientas de auditoría de redes inalámbricas y además software de análisis forense. Es característico por los siguientes usos que tiene para los usuarios:

Pruebas de penetración: Las pruebas de penetración o hacking ético son unas pruebas que simulan ciberataques para detectar vulnerabilidades en sistemas y redes antes de que sean atacadas por hackers maliciosos. Kali Linux se considera una terminal de interacción para la ejecución de pruebas de seguridad, lo que significa que se puede tener la capacidad de escudriñar la seguridad de la infraestructura de las aplicaciones de una organización

Evaluación de vulnerabilidades: Las vulnerabilidades de la seguridad deben ser identificadas y eliminadas para que se pueda tener seguridad en la organización. Kali Linux es una opción maximizada para la evaluación de vulnerabilidades, ya que permite a los equipos de seguridad examinar redes, aplicaciones web y bases de datos en busca de las vulnerabilidades y las debilidades conocidas.

Análisis forense: El análisis forense es esencial ya que registran el ataque, evalúan y recogen pruebas para identificar su origen cuando el incidente de la seguridad y la filtración de datos se apodera de la organización. Kali Linux proporciona analistas forenses las herramientas y utilidades que les permiten realizar investigaciones forenses extensivas, para agregar la información extraída de artefactos digitales.

Educación y formación en seguridad: Kali Linux se trata de una herramienta educativa increíblemente útil para la formación de los futuros profesionales en ciberseguridad. Proporciona experiencia práctica con herramientas y técnicas auténticas lo cual permite que los alumnos adquieran experiencias prácticas en áreas como pruebas de penetración, seguridad de redes y análisis de malware.

Apoyo y cooperación de la comunidad: Kali Linux se encuentra respaldado por una comunidad activa y vibrante de profesionales, investigadores y entusiastas de la ciberseguridad que contribuyen a su desarrollo, comparten su conocimiento y experiencias. Este entorno colaborativo potencia la innovación, el intercambio de experiencias y el progreso continuo, convirtiendo a Kali Linux en una plataforma dinámica para la ciberseguridad.

Herramientas incluidas en Kali Linux

Tal y como nos indica Daniel (2024) Kali es conocida fundamentalmente por tener una variedad de herramientas las especializadas en la seguridad informática y en el hacking ético. Con más de 600 programas preinstalados, Kali Linux se presenta como una distribución que ofrece un arsenal para cubrir múltiples necesidades en las auditorías de seguridad.

Estas herramientas se distribuyen a través de varias categorías: análisis de red, auditorías de penetración, detección de vulnerabilidades, cracking de contraseñas, etc. Cada una de estas herramientas está preparada para ofrecer resultados certeros, al tiempo para simular un ataque como también para asegurar una red. Además Kali Linux es conocida por la posibilidad de ejecutarse sobre numerosos equipos. Así puede instalarse sobre una máquina virtual, ejecutarse desde una memoria USB, o bien desplegarse en un Raspberry Pi.

De todas las herramientas que contiene Kali nos vamos a centrar en las siguientes 3 de recuperación de datos (información) dónde se analizara cada una de ellas, con la finalidad de conocer más sobre sus funciones.

TestDisk

Según Demian (2021), TestDisk es una herramienta desarrollada por un programador serio y confiable Christophe Grenier, quien comenzó el programa como un proyecto amateur en 1998 y continúa siendo el desarrollador principal en la actualidad. Así mismo es responsable del desarrollo de TestDisk y su herramienta auxiliar, PhotoRec, para diversas plataformas.

Como afirma Rubén Velasco (2023), TestDisk es una herramienta que ayuda a los usuarios a recuperar particiones perdidas o borradas por error y hacer que los discos que han dejado de arrancar, sea por el motivo que sea (mientras no sea un problema físico del disco) vuelvan a funcionar y con todos sus datos intactos. El software analiza la estructura del disco y permite la restauración de tablas de partición eliminadas o corruptas. Igualmente puede reconstruir sectores de arranque y recuperar archivos dañados de los sistemas.

TestDisk es un programa totalmente gratuito y es un software de libre acceso que se encuentra integrado en Kali Linux por lo que también merece la pena destacar la gran compatibilidad que nos presenta esta herramienta gratuita para que la podamos utilizar y obtener provecho de las funciones de esta herramienta en prácticamente la mayoría de los sistemas operativos más populares. Por lo tanto, TestDisk es compatible con los siguientes sistemas operativos:

Tabla 1:

Sistemas operativos compatibles con TestDisk

Sistemas operativos compatibles con TestDisk	
DOS	FreeBSD
Windows (desde Windows NT hasta Windows 11).	OpenBSD
Linux	SunOS
macOS	Y otros sistemas basados en Unix.

Nota. Estos son los diferentes sistemas operativos que se manejan con TestDisk.

A continuación, se muestra la manera en que TestDisk se ocupa de la recuperación de datos al hacer notar su capacidad para detectar particiones perdidas, reparar partes dañadas y acceder a archivos que el propio sistema ya no es capaz de reconocer.

Recuperación de datos con TestDisk

Como dice Demian (2021), TestDisk es una herramienta de recuperación de datos versátil. Le mostramos una lista de lo que promete conseguir:

Tabla 2:

Tipos de recuperación de datos con TestDisk

Tipos de recuperación de datos con TestDisk	
Reparar la Tabla de Particiones, recuperando una partición eliminada.	Recuperar el sector de arranque FAT32 de su respaldo.
Reconstruir el sector de arranque FAT12/FAT16/FAT32.	Arreglar Tablas FAT.
Reconstruir el sector de arranque NTFS.	Recuperar el sector de arranque NTFS a partir de su respaldo.

Tipos de recuperación de datos con TestDisk	
Reparar MFT usando espejo MFT.	Localice el Superblock de las copias de seguridad ext2/ext3/ext4.
Recuperar los archivos de los sistemas de archivos FAT, exFAT, NTFS y ext2.	Copiar archivos de particiones FAT, exFAT, NTFS y ext2/ext3/ext4 eliminadas.

Nota. Estas son las propuestas de recuperación de datos que ofrece TestDisk.

TestDisk se centra sobre todo en problemas de particiones y del sector de arranque si ha perdido una partición TestDisk puede ser una buena opción también permite recuperar particiones eliminadas, reparar tablas de particiones corruptas y reconstruir un sector de arranque en discos dañados es un programa especialmente útil en las situaciones en las que el sistema operativo no reconoce un disco o en las que aparecen errores al intentar acceder a una unidad.

TestDisk es una herramienta ampliamente conocida por su gran eficacia en la tarea de recuperación de particiones, así como en operaciones de reparación de sectores de arranque.

El mecanismo de funcionamiento de esa herramienta se basa en una interfaz de línea de comandos, en lo cual reside en gran medida su precisión, si bien la dificultad de manejo puede llegar a ser un reto para personas sin la adecuada experiencia técnica se exponen algunas de sus más relevantes ventajas y desventajas en lo que concierne a la recuperación de datos.

Tabla 3

Ventajas y Desventajas de TestDisk

Ventajas	Desventajas
Es del todo libre y de código abierto.	Interfaz en modo texto: no recomendable para gente sin conocimientos.
Potente en reparación de particiones y recuperación del sector de arranque.	No es muy bueno para recuperar archivos individuales borrados.

Ventajas	Desventajas
Multiplataforma Windows, macOS, Linux.	Sin la función de guardar la sesión, reanudar el escaneo.
Funciona bien incluso en unidades RAW o no montables.	Requiere conocimientos técnicos para trabajar con soltura.
Admite un número elevado de sistemas de ficheros y tipos de particiones.	Es fácil cometer errores críticos si no se tiene conocimiento de la estructura de la unidad.

Nota. La información que se me muestra en la tabla es del autor Kourafalos (2021).

PhotoRec

Según lo que señala Alfonso Cervera (2025), PhotoRec es un software de recuperación de archivos que te permite recuperar casi cualquier tipo de archivo multimedia como fotos o vídeos, así como documentos, archivos de distintos tipos de dispositivos de almacenamiento (discos duros, cd-roms, pen-drives, tarjetas de memoria, etc.). También restaura fotos de una cámara digital (es compatible con las marcas más comunes de cámaras: Canon, Nikon, Olympus, Pentax y otras).

También trabaja con los principales tipos de sistemas de almacenamiento: FAT, NTFS, HFS+, exFAT, ext2/ext3/ext4. Incluso si ha perdido su sistema de archivos o lo ha formateado, puede recuperar los archivos con PhotoRec por cierto es gratuito y puedes recuperar más de 440 tipos de archivos (270 familias de archivos más o menos). PhotoRec tiene un acceso en modo sólo de lectura, así que los archivos son preservados durante cada uno de los procesos de recuperación.

Tabla 4:

Sistemas operativos compatibles con PhotoRec

Sistemas operativos compatibles con PhotoRec	
DOS	FreeBSD

Sistemas operativos compatibles con PhotoRec	
Windows (desde Windows NT hasta Windows 11).	OpenBSD
Linux	SunOS
macOS	Y otros sistemas basados en Unix.

Nota. Estos son los diferentes sistemas operativos que se manejan con PhotoRec

Tabla 5:

Ventajas y Desventajas de PhotoRec

Ventajas	Desventajas
Recuperación de todo tipo de datos de manera profesional.	PhotoRec no incluye una interfaz intuitiva o gráfica: carece de una interfaz gráfica y tan solo proporciona la interfaz básica de línea de comandos, que se volvería muy difícil de manipular para aquellos que no son expertos informáticos.
PhotoRec permite una recuperación de tipo avanzada.	
Soporta todos los sistemas de ficheros: NTFS, FAT32, HFS+.	Hay acciones del software que son irreversibles, de forma que cualquier mala actuación podría tener un efecto desastroso en los datos del usuario.
Recuperación de archivos gratuita.	PhotoRec destaca por ser software libre, así como por ser convertido en mucho más susceptible al malware y virus en ciertos casos.

Nota. La información que se me muestra en la tabla es del autor Taylor Clark (2023).

Foremost

Según menciona Cervera (2025), Foremost es un software sin costo que ha sido creado por agentes del gobierno de los Estados Unidos que se puede descargar de la red, Foremost intenta recrear los ficheros tal y como se encuentran en disco, en lugar de intentar recuperarlos directamente del sistema de ficheros de su unidad.

La mayor parte de los sistemas operativos eliminan parcialmente los ficheros del sistema de archivos. Eliminan los metadatos y permiten que los datos subyacentes sean sobrescritos. Foremost va a copiar y escanear la unidad para buscar esos datos tal y como se encuentran en disco, puesto que lo que realmente se está haciendo es escanear todos los ficheros.

Utilizará la memoria interna de su ordenador como almacenamiento temporal. Luego buscará segmentos de fichero determinados, los identificará con otros y juntará nuevos ficheros, como si juntara piezas de un rompecabezas.

Recuperación de datos con Foremost

La herramienta hace uso de la técnica llamada minería de datos, por la cual recuperar los elementos mediante los mismos encabezados pies de página y escritura interna de estos, así como por la recuperación de cada una de las entradas en los cuales se recupera una larga lista de formatos que por defecto son:

- jpg, gif, png, bmp, avi, tiff, mp4, exe, mpg, wav, asf, wma, mp3
- fws, riff, wmv, mov, pdf, ole, doc, docx, xls, xlsx. ppt, pptx, zip
- rar, html, cpp, java, art,pst, ost, dbx, idx, mbx, wpc, pgp, txt,
- rpm, dat, etc.

De nuevo, esta herramienta a la cual se puede considerar aplicar los sistemas operativos ya mencionados, está destacada por su utilización en todos los entornos ya sean personales o profesionales. Por su filosofía técnica y por los múltiples usos que tiene en el campo de recuperación de datos, en su aplicabilidad nos interesa tener en cuenta sus puntos fuertes y sus limitaciones por ello se refieren a continuación las características de sus principales ventajas y desventajas.

Tabla 6:

Ventajas y Desventajas de Foremost

Ventajas	Desventajas
Se puede recuperar archivos importantes. Fácil de usar Disponible para varios sistemas operativos.	No se puede recuperar todo tipo de archivos.

Nota. Se presenta las diferentes ventajas y desventajas de Foremost para evaluar su efectividad.

Con toda la información detallada en las hojas anteriores se procederá a hacer la parte práctica donde se evaluarán diversos criterios de las 3 herramientas que se han seleccionado esto se hará con la finalidad de poder hacer la o las tablas comparativas de las herramientas ya mencionadas.

Tabla 7:

Comparación de herramientas forenses

Herramientas	¿Para qué se utiliza normalmente?	¿Cómo realiza la recuperación?	¿Qué tan fácil es de usar?	¿Dónde suele usarse más?
TestDisk		Restauración de estructuras como	Tiene menús en la terminal lo	En la exploración de discos

Herramientas	¿Para qué se utiliza normalmente?	¿Cómo realiza la recuperación?	¿Qué tan fácil es de usar?	¿Dónde suele usarse más?
	Para recuperar particiones inexistentes o discos que no arrancan más.	particiones y sectores de arranque.	cual es fácil para usuarios intermedios.	completos o de discos con daños severos.
PhotoRec	Para recuperar fotos, vídeos y documentos eliminados.	Busca las firmas internas de los archivos y los reconstruye.	Muy fácil de usar con su asistente paso a paso.	En la recuperación de archivos eliminados si el sistema está roto.
Foremost	Para recuperar archivos eliminados en el análisis forense.	Usa cabeceras y extensiones conocidas para identificar archivos.	Requiere saber y conocimientos técnicos, solo utiliza comandos.	En análisis forenses o en análisis automáticos de discos.

*Nota. S*e compara las diferentes herramientas para poder saber cuál es la función de cada una.

La Tabla 7 está bien detallada indicando para qué sirve cada herramienta por ejemplo, TestDisk es bastante adecuado para la recuperación de particiones o de discos que ya no inician, mientras que PhotoRec está centrado en archivos eliminados como fotografías o documentos y Foremost se utiliza más en el ámbito forense porque encuentra los archivos por cabeceras, aunque esto requiere conocimientos más técnicos.

Tabla 8:

Compatibilidad con sistemas y archivos

Herramienta	¿Con qué sistemas operativos funciona?	¿Necesita un tipo específico de sistema de archivos?	¿Qué tipo de archivos puede recuperar?
TestDisk	Funciona con Windows, Linux, macOS, BSD, etc.	Sí con NTFS, FAT, ext, HFS+, etc.	Recupera estructuras del disco y no archivos
PhotoRec	También funciona con los principales sistemas operativos.	No depende del sistema de archivos.	Recupera más de 480 tipos de archivos (imágenes, documentos, vídeos, etc.).
Foremost	Compatible con Linux, macOS, BSD, etc.	No depende del sistema de archivos.	Recupera archivos como JPG, PDF, DOC, XLS, etc.

Nota. Compatibilidad de sistemas operativos con los tipos de ficheros en cada herramienta

La Tabla 8 destaca la compatibilidad todas funcionan en los sistemas operativos más habituales, aunque la diferencia es que TestDisk necesita conocer el sistema de archivos y que PhotoRec y Foremost trabajan sin condiciones, lo cual les otorga mayor versatilidad.

Tabla 9:

Funcionalidades útiles y tiempo de demora en recuperar la información

Herramienta	¿Recupera particiones?	¿Recupera archivos borrados?	¿Funciona con discos dañados?	¿Genera informes de recuperación?	¿Tiempo que demora en recuperar?
TestDisk	Sí	Solo archivos del sistema	Sí, muy bien	Sí, genera logs detallados	2h

Herramienta	¿Recupera particiones?	¿Recupera archivos borrados?	¿Funciona con discos dañados?	¿Genera informes de recuperación?	¿Tiempo que demora en recuperar?
PhotoRec	No	Sí, muy buena recuperación	Sí	Sí, guarda un registro de todo	30 mts
Foremost	No	Sí	Sí, aunque depende de la configuración	Sí, genera archivos de reporte	1:30 h

Nota. Se demuestra las funcionalidades de cada herramienta agregando en tiempo de demora en la recuperación de la información.

En la Tabla 9 se identifican sus funciones más significativas TestDisk se ocupa más de estructuras como particiones, por el contrario PhotoRec y Foremost están pensadas para la recuperación de archivos más concretos, a su vez las tres herramientas logran sacar reportes que es de gran utilidad en análisis forense y también tienen presente el tiempo de demora.

Tabla 10:

Facilidad de uso y perfil del usuario ideal

Herramienta	¿Qué tan fácil es usarla?	¿Para qué tipo de usuario es mejor?	¿Cuál es su punto fuerte?	¿Qué limitación tiene?
TestDisk	Sencilla para quien sabe organización de discos.	Personas con conocimientos intermedios.	Restaurar particiones completas.	No le da alternativa a la hora de recuperar archivos personales en concreto.

Herramienta	¿Qué tan fácil es usarla?	¿Para qué tipo de usuario es mejor?	¿Cuál es su punto fuerte?	¿Qué limitación tiene?
PhotoRec	Muy bien guiada y amigable.	Cualquier usuario, aunque sea inexperto.	Estupendo para recuperar fotos y documentos.	No conserva los nombres originales de los archivos.
Foremost	Solo por comandos. No es tan intuitiva.	Personas con experiencia técnica.	Personalizable y potente para el análisis forense.	Sin interfaz y con el requerimiento de editar ficheros para añadir funcionalidades.

Nota. Se presenta todos los puntos a favor teniendo presente el perfil de usuario ideal.

La Tabla 10 se centra comparando la facilidad de uso, aquí observa que PhotoRec es la más útil para la gente con poca experiencia, TestDisk es para los usuarios intermedios y Foremost es mucho más compleja y tiene un enfoque para expertos.

Tabla 11:

Rendimiento y eficiencia

Herramienta	¿Es rápida analizando?	¿Soporta discos muy grandes?	¿Funciona bien con discos dañados?	¿Necesita instalación aparte?
TestDisk	Muy rápida para reparar particiones.	Sí, sin problemas.	Sí	No, ya viene en Kali
PhotoRec	Rápida, pero puede tardar si hay muchos archivos.	Sí	Sí, incluso en discos RAW	No, ya viene en Kali

Herramienta	¿Es rápida analizando?	¿Soporta discos muy grandes?	¿Funciona bien con discos dañados?	¿Necesita instalación aparte?
Foremost	Puede ser más lenta si hay muchos tipos archivo.	Puede volverse lento.	Sí	No, ya viene en Kali

Nota. Se presenta la eficiencia y rendimiento de cada herramienta desde el punto practico.

En lo que respecta al rendimiento, se puede ver desde el análisis de la tabla 11 TestDisk es ágil y eficaz reparando particiones, PhotoRec también presenta buen rendimiento pero puede ser lento dependiendo de la cantidad de archivos, mientras que Foremost puede convertirse en un programa algo más lento dado la cantidad de tipos de archivo que tiene que trabajar.

Tabla 12:

Legalidad y confiabilidad en contextos forenses

Herramienta	¿Guarda registros de lo que hace?	¿Modifica el disco analizado?	¿Es código abierto?	¿Ha sido usada en investigaciones reales?
TestDisk	Sí, todo queda registrado	No, trabaja en solo lectura	Sí	Sí
PhotoRec	Sí	No	Sí	Sí
Foremost	Sí	No	Sí	Sí

Nota. Se presenta la confiabilidad y legalidad de cada herramienta teniendo presente los contextos forenses.

La Tabla 12 presenta el punto de vista de la legalidad y la confiabilidad, puesto que las tres herramientas trabajan en modo solo lectura hecho que es idóneo para no modificar la evidencia,

además de ser todas de código abierto lo que genera transparencia y uso libre en las investigaciones en la práctica.

Tabla 13:

Instalación y soporte

Herramienta	¿Viene ya con Kali Linux?	¿Se actualiza con frecuencia?	¿Tiene comunidad de soporte?	¿Es fácil mantenerla?
TestDisk	Sí	Sí, se mantiene activa	Muy activa	Sí
PhotoRec	Sí	Sí	Activa (comparten desarrollador)	Sí
Foremost	Sí	No muy frecuente	Comunidad más pequeña	Puede requerir ajustes manuales

Nota. Se presenta la eficiencia del soporte y la instalación de cada herramienta.

Finalmente, en la Tabla 13 se analizan temas de la instalación y el soporte, las tres herramientas vienen ya instaladas en Kali Linux por lo que resulta sencillo utilizarlas no obstante TestDisk y PhotoRec cuentan con comunidades bastante activas y actualizaciones frecuentes, en tanto que Foremost tiene una actualización más limitada y puede requerir ajustes manuales.

Las tablas muestran que TestDisk, PhotoRec y Foremost emplean enfoques diferentes en función del tipo de recuperación que requiera el usuario, TestDisk puede llegar a ser muy útil para arreglar particiones dañadas, PhotoRec tiene un buen funcionamiento para tratar de recuperar archivos eliminados de manera rápida y Foremost es para el análisis forense donde el usuario tiene que poseer más conocimiento tecnológico.

Las tres son del tipo de software libre y funcionan en diferentes sistemas operativos, generan reportes y están incluidas en la distribución de Kali Linux. La elección de cualquier solución dependerá del tipo de recuperación que desee realizar el usuario.

MARCO METODOLÓGICO

Esta investigación tiene como propósito principal recolectar la información de documentos escritos por otros autores, los cuales tengan investigaciones similares o que estén relacionados con el tema a tratar en este estudio teniendo presente el análisis comparativo de las herramientas forenses para la recuperación de información.

Enfoque de la Investigación

El presente trabajo utiliza un enfoque cuantitativo con aplicación práctica, ya que el objetivo de la metodología es el análisis objetivo y medible sobre el comportamiento de tres herramientas forenses de código abierto TestDisk, PhotoRec y Foremost, aunque se apoya en fuentes documentales y en técnicas que ya han sido publicadas, también se llevaron a cabo pruebas controladas en un entorno virtual (en Kali Linux), lo cual ha permitido comparar su comportamiento en diferentes situaciones de pérdida de datos, este enfoque no solo busca describir sus características sino también interpretar los resultados en función de su rendimiento real, ya que a su vez permite integrar la teoría con la práctica.

Tipo de Investigación

Esta investigación se considera una investigación descriptiva con enfoque documental y práctica, se cree descriptiva dado que intenta describir, caracterizar y detallar las funciones, beneficios, limitaciones y niveles de eficacia de las herramientas TestDisk, PhotoRec y Foremost también es un estudio con enfoque documental ya que está basado en documentos técnicos, manuales oficiales y trabajos anteriores es un estudio de aplicación práctica porque se llevaron a cabo pruebas controladas permitiendo observar de primera mano el funcionamiento de cada herramienta en diferentes situaciones de pérdida de datos.

Diseño de la Investigación

El diseño de la investigación que se desarrolla es de carácter no experimental y de tipo transversal, no experimental porque no se están manipulando de manera sistemática las variables independientes, ni tampoco se estructuran grupos de comparación bajo condiciones controladas y específicamente estrictas, como en el caso de los experimentos clásicos.

No obstante, hasta cierto punto sí se realizaron pruebas y control en un entorno virtual, específicamente con Kali Linux en el que se hicieron correr las herramientas forenses TestDisk, PhotoRec y Foremost con el fin de adivinar cómo podrían responder en situaciones similares de pérdida de datos reales.

Método de Investigación

El presente estudio de caso se basa en un procedimiento analítico-comparativo, dado que el objeto de estudio no es otro que observar y confrontar el funcionamiento, características y grado de eficacia de tres herramientas forenses de recuperación de datos: TestDisk, PhotoRec y Foremost, este procedimiento permite estudiar adecuadamente el comportamiento de cada una de las herramientas en situaciones similares mediante la observación de sus características, determinando tanto sus aspectos positivos como los negativos.

El análisis se llevó a cabo mediante la combinación de dos vías de estudio, en primer lugar el recurso a fuentes documentales fiables y actualizadas, como los manuales de uso de cada herramienta, así como la consulta de artículos técnicos y aportaciones vertidas por la gran comunidad que posee este sistema operativo y en segundo lugar la realización de pruebas controladas en una máquina virtual con Kali Linux simulando escenarios de pérdida de datos, observando el comportamiento efectivo de las herramientas en el ámbito más forense.

La combinación de la línea de investigación documental y de la práctica de análisis ejecutado de las herramientas proporciona fortaleza al estudio ya que permite comparar no solo la teoría de las herramientas forenses de la recuperación de datos, sino también su experiencia práctica, sirviendo de anexo a una forma de considerar más completa y fundamentada.

Clasificación de la efectividad

La efectividad de las técnicas de recuperación puestas en práctica por cada una de las herramientas forenses queda categorizada de la siguiente manera, en función del resultado aproximado conseguido:

- **Alta (90 - 100%):** Técnicas que permiten una recuperación precisa, inmediata y fiable tal y como puede observarse en las particiones completas o recuperación de cualquier tipo de archivo.
- **Media-Alta (80 - 89%):** Técnicas eficaces en la recuperación de archivos individuales, aunque limitadas ya que la recuperación puede dar lugar a la pérdida de nombres o estructura original.
- **Baja (70 - 79%):** Técnicas útiles en la práctica forense y muy eficaces que ofrecen una capacidad accedida buena pero que dependen del tipo de archivo y configuración técnica.

Fuentes analizadas

El presente estudio de caso es documental; no se ha trabajado con **población**, ni con **muestra**, como seda en las investigaciones tipo de campo. Desde esta perspectiva se ha tomado como referencia, fuentes técnicas y especializadas en su sentido más amplio tales como:

- Manuales oficiales de cada herramienta.
- Artículos académicos y forenses.

- Pruebas prácticas que han realizado en Kali Linux.
- Foros y artículos contrastivos en ciberseguridad.

Estas fuentes fueron elegidas por interés significativo en este caso de estudio dado que son actuales y confiables de manera que alcancen a fundamentar un análisis aceptable de hecho al proceder de ámbitos de conocimiento especializado en informática forense y recuperación de la información, proporciona una base técnica suficiente para poder comparar la capacidad de respuesta de cada herramienta, asimismo su variabilidad asegura un conocimiento más completo del funcionamiento real de las aplicaciones analizadas, lo que enriquece también la interpretación de los resultados alcanzados.

RESULTADOS

Gracias al estudio realizado se han podido identificar las principales características técnicas, ventajas, limitaciones y niveles de efectividad de las herramientas TestDisk, PhotoRec y Foremost que se encuentran en un entorno forense de recuperación de datos bajo el sistema operativo Kali Linux, con el propósito de cumplir de forma correcta y bien informada con cada una de los metas planteadas, los resultados obtenidos a través de la investigación se corresponden con los objetivos concretos, cada objetivo se puede presentar a partir de datos verificables extraídos y organizados de las fuentes de información oficiales que se han empleado en la presente investigación.

Identificación de funcionalidades relevantes en base a las pruebas realizadas

Cada una de las herramientas empleadas evidencia diferentes estrategias en la recuperación de datos:

TestDisk obtuvo un 85% de efectividad con una demora de 2 horas y media en recuperar la información, esta herramienta se centró en la reparación de tabla de particiones y sector de arranque, siendo útil cuando el sistema no detecta la unidad o cuando hay daños en las estructuras del disco.

PhotoRec obtuvo un 90% de efectividad con una demora de media hora mostró una gran eficacia en la recuperación de archivos individuales (documentos, imágenes, videos, etc.) esta herramienta fue de mucha ayuda y no fue tan compleja de manejar.

Foremost obtuvo un 80% de efectividad con una demora de 1 horas y media fue valorado por su sencillez y por su buen rendimiento en la recuperación de archivos mediante análisis por

firmas (file carving), siendo útil en situaciones donde se había perdido completamente el sistema de archivos.

Tabla 14:

Estrategia de recuperación utilizada en cada herramienta

Herramienta	Estrategia de recuperación utilizada	Descripción técnica	Efectividad estimada
TestDisk	Reparación de estructuras de partición.	Restaura particiones eliminadas y sectores de arranque dañados (FAT, NTFS, EXT)	Alta (90–95%) en recuperación de particiones.
PhotoRec	Recuperación por firma de archivo.	Escanea sectores en bruto buscando cabeceras de archivos conocidos (file carving)	Media-Alta (80–90%) en recuperación de archivos sueltos.
Foremost	Extracción mediante cabeceras y extensiones.	Analiza el contenido del disco para extraer archivos basados en firmas predefinidas.	Baja (70–85%), dependiendo del tipo de archivo y configuración.

Nota. Lo que se presenta en la tabla está basado en la información que se investigó y del punto de vista que nos brindó la comunidad de Kali.

Evidentemente, la tabla pone de relieve a **TestDisk** donde se estima una efectividad del (90–95%) para recuperar particiones y reparar sectores de arranque, siendo el programa adecuado para daños estructurales, gracias a que puede recuperar sistemas de archivos dañados que no pueden ser detectados por otros programas.

En cuanto a la herramienta de recuperación **PhotoRec**, la efectividad se estima en un porcentaje del 80–90% siendo muy interesante para recuperar archivos que no son imágenes aunque, eso sí no identifica el nombre original de cada archivo.

Por su parte, la herramienta **Foremost** obtiene estimación de efectividad del 70–85% y, aunque es menos efectivo que PhotoRec, lo compensa con un modo de detección de archivos mediante cabeceras o extensiones, lo que es útil en la obtención de pruebas en contextos forenses.

Tabla 15:

Comparación de efectividad basado en pruebas realizadas

Herramienta	Tipos de recuperación	Medios de precisión	¿Tiempo que demora en recuperar?	Entorno de Uso Ideal
TestDisk	Particiones, sectores de arranque	85%	2h	Discos dañados, particiones fuera de uso
PhotoRec	Archivos individuales	90%	30 mts	Recuperación profunda de archivos
Foremost	Archivos por firma (carving)	80%	1:30 h	Situaciones de forenses simples

Nota. La información que se presenta en la tabla está basada en la prueba practica que se realizó teniendo presente la efectividad de cada herramienta que se planteó anterior mente.

Después de las pruebas realizadas da como resultado que PhotoRec tiene una muy buena eficiencia en la recuperación de información de archivos individuales con un porcentaje dado del 90%, pasando a la siguiente herramienta esta TestDisk donde se muestra un 85% de eficiencia en la recuperación de particiones y sectores de arranque algo significativo para este tipo de

recuperación de información, por último tenemos a Foremost donde presenta un 80% en la recuperación de archivos por firma esta herramienta también es importante para la sociedad dado que ayuda a recuperar exactamente archivos File Carving.

En resumen, los porcentajes obtenidos permiten ver sin dificultad que cada herramienta posee cualidades propias que no se debe perder de vista, **no se trata de saber cuál es la mejor herramienta**, sino de comprender cuál es la herramienta más adecuada para el tipo de situación que se encuentre ante la pérdida de datos, precisamente en el momento de elegir la herramienta se debe tener en cuenta el tipo de pérdida que se tenga y cuál es el tratamiento que se quiere dar desde el análisis.

DISCUSION DE RESULTADOS

El análisis de los resultados conseguidos en este trabajo se da de acuerdo a los diferentes objetivos específicos que se plantearon al inicio de esta investigación, teniendo presente las pruebas prácticas que se realizaron para evaluar cada una de estas herramientas validando la facilidad de uso, su velocidad, los tipos de archivos y su efectividad en la recuperación de la información.

TestDisk posee el 85% de efectividad al momento de recuperar la información, a pesar de esto en el transcurso de la investigación se creía que era el más fuerte de entre las 3 pero al realizar las pruebas prácticas fue todo lo contrario si bien es cierto su función es arreglar las particiones y restaurar los sectores de arranque, el tiempo en recuperar aquella información es demasiado lento dado que hace un análisis exhaustivo en el disco.

El 90% de efectividad lo mantiene **PhotoRec** dado que logro recuperar múltiples archivos importantes en tan solo media hora eso lo llevo a ser más efectivo, si bien es cierto esta herramienta tiene la función de recuperar archivos individuales algo que es bueno y malo a la vez, se debe tener presente que esta herramienta es un complemento de TestDisk por lo que al unir ambas pueden hacer un mejor dúo recuperando información.

Foremost obtuvo el 80% de eficiencia en recuperar información con una demora de una hora y media, si bien es cierto esta herramienta analiza la búsqueda de archivos de firmas conocidas eso es muy bueno porque extrae la información como tal, la única falla de esta herramienta es que al momento de que extrae los archivos no los recupera con el nombre original por lo que eso retrasa a las personas que usan la herramienta.

De acuerdo con los resultados obtenidos se puede decir que no se busca en este caso la mejor herramienta, sino que simplemente se quiere incentivar a usar estos recursos gratuitos que ofrece Kali Linux dado que muchas veces las equivalentes de estas herramientas son muy costosas lo que genera un problema ante la sociedad en esta circunstancia se ofrece las herramientas TestDisk, PhotoRec, Foremost como una solución que puede recuperar la información ya se sea de manera personal o institucional.

CONCLUSIONES

Al combinar el análisis documental basado en las herramientas que se seleccionó para realizar este estudio comparativo se tiene como conclusión que cada herramienta usa escenarios diferentes, aunque todas tienen el mismo objetivo recuperar la información, a esto se agrega la parte práctica donde se pudo evidenciar de manera clara cómo trabaja cada herramienta.

Al momento de que se realizaron las pruebas mediante el sistema operativo Kali Linux se concluyó que las personas que vayan a usar estas herramientas deben tener presente el tipo de archivo que se desean recuperar, dado que cada herramienta se caracteriza por tener un estándar de archivos específicos basándose en el análisis exhaustivo que le hace ya sea al hardware o software.

Los porcentajes que se obtuvieron a través de la valorización que se realizó en las pruebas da como conclusión que las 3 herramientas se mantiene en un rango de 80 – 90 % de efectividad donde PhotoRec obtuvo como resultado un 90% seguidamente TestDisk con un 85% y por último Foremost presento un 80%, de igual importancia el objetivo de este estudio no es saber cuál es la mejor si no saber cuál es la más adecuada para cada situación donde sea de recuperar información, por lo que al comparar cada herramienta se obtuvo sus conceptos, ventajas, desventajas, características, tipos de archivos, etc.

RECOMENDACIONES

Se recomienda leer información sobre cada una de las herramientas para entender que es lo que hace, saber sus características, ventajas y desventajas para así no ir de vacío directo a manipular el recurso que ofrece Kali Linux ya que eso puede dar problemas al momento de extraer la información que se necesita.

Se sugiere tener presente el tipo de recuperación de datos que se desea realizar ya que todas las herramientas tienen el mismo enfoque, pero cada una tiene un estándar de archivos específicos para recuperar, por lo usar cualquier herramienta sin tener claro que es lo que va a extraer puede generar errores.

Se aconseja tener presente los porcentajes de efectividad de cada herramienta que se definieron en este caso de estudio no es con el énfasis de saber cuál es la mejor si no de tener presente para que situación es adecuada usarla sabiendo el nivel de efectividad que tiene cada una al momento de recuperar la información.

REFERENCIAS

Alfonso Cervera. 2025. «Cómo Usar PhotoRec». https://recoverit.wondershare.es/photo-recovery/how-to-use-photorec.html.

Cervera. 2025. «Cómo Utilizar Foremost para Recuperar Archivos en Linux y su Alternativa». https://recoverit.wondershare.es/file-recovery/foremost-linux.html.

Daniel. 2024. «Kali Linux: todo lo que necesitas saber sobre esta suite de herramientas para pruebas de intrusión». https://datascientest.com/es/kali-linux-todo-lo-que-necesitas-saber.

Demian, Ojash Yadav, Roman. 2021. «TestDisk Review: Scan Results, Pros, Cons & Our Verdict». https://www.handyrecovery.com/testdisk-review/.

Docunecta, Equipo de. 2021. «Qué son los metadatos: definición, tipos y ejemplos». https://www.docunecta.com/blog/que-son-los-metadatos.

g0tmi1k. 2025. «What Is Kali Linux? | Kali Linux Documentation». https://www.kali.org/docs/introduction/what-is-kali-linux/.

Jacob Murel Ph.D., Meredith Syed. 2024. «¿Qué es la recuperación de información? | IBM». https://www.ibm.com/mx-es/think/topics/information-retrieval.

Jafar Hasan. 2024. «What is Kali Linux and Why is it Important in Cybersecurity?» https://appinindore.com/blogs/what-is-kali-linux-and-why-is-it-important-in-cybersecurity/.

Kassandra Ortega. 2022. «¿Qué es la informática forense?» https://worldcampus.saintleo.edu/blog/que-es-la-informatica-forense-analisis-forense-informatico.

Laboratories, LLC SysDev. 2024. «¿Qué es la recuperación de datos y cómo funciona?» https://www.ufsexplorer.com/es/articles/what-is-data-recovery/.

Morgan, Michael. 2021. «Introducing and Install Foremost on Kali Linux». https://blog.eldernode.com/introducing-install-foremost-on-kali-linux/.

Rubén Velasco. 2023. «TestDisk, programa para recuperar datos y particiones». https://www.softzone.es/programas/sistema/testdisk/.

Taylor Clark. 2023. «[2024] Cómo usar PhotoRec y la mejor alternativa». https://www.anyrecover.com/deleted-files-recovery-data/how-to-use-photorec-and-the-best-alternative-of-it/.

tiadmin. 2024. «Perdida de datos: Un riesgo invisible». https://tirescue.com/perdida-de-datos-un-riesgo-invisible.

Zane Kennedy. 2024. «Recuperación de datos». Guía para principiantes sobre cómo recuperar datos con éxito.

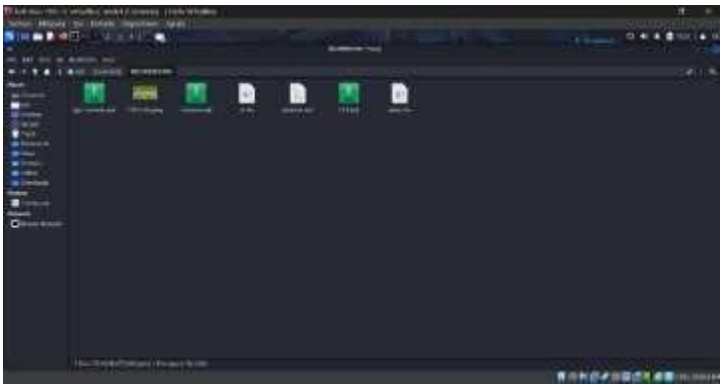
ANEXOS

Recuperación de archivos con la herramienta **TestDisk**

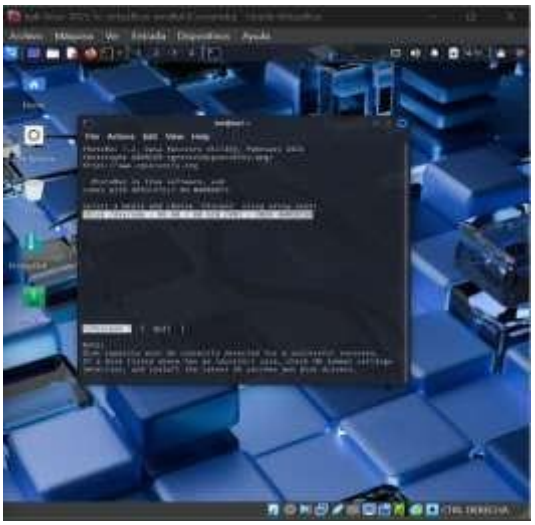






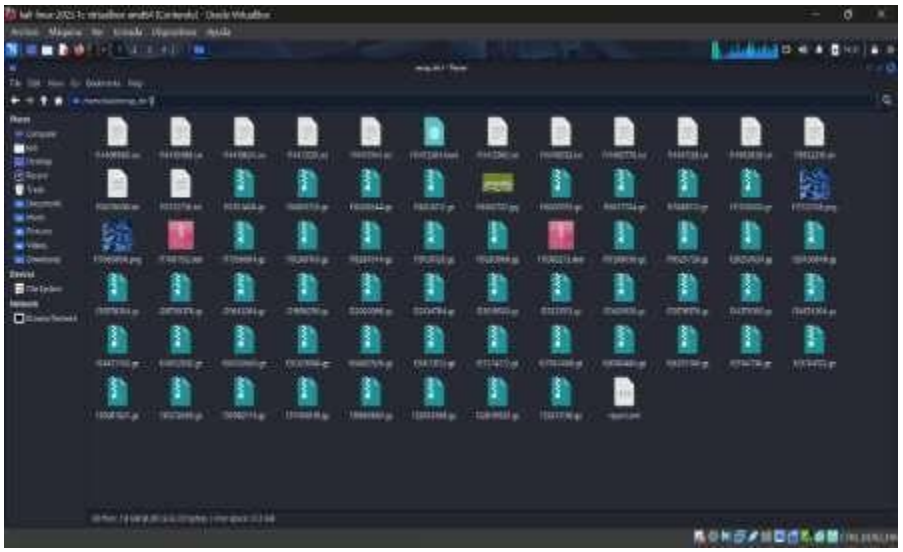



Recuperación de archivos con la herramienta **PhotoRec**

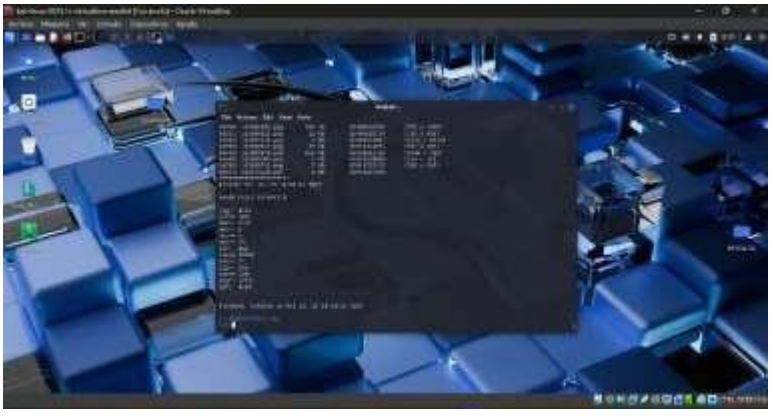


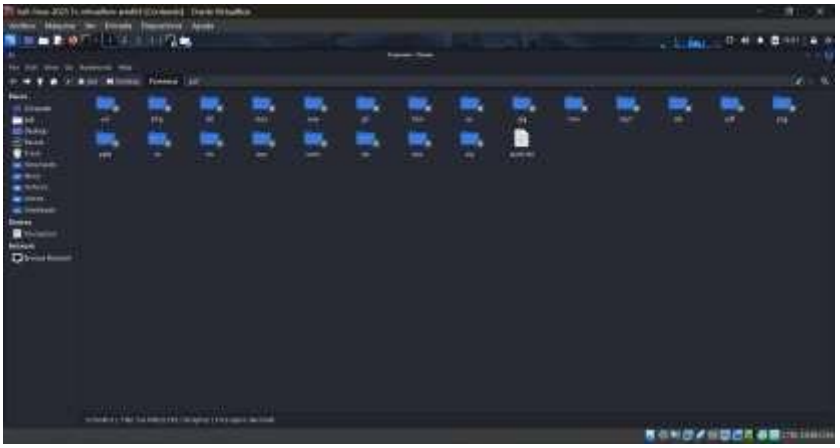




Recuperación de archivos con la herramienta **Foremost**





INFORME DE ANÁLISIS
magister

CASO DE ESTUDIO FINAL COMPILATIO- Yoely Paredes

5% Textos sospechosos

3% Similitudes
0% similitudes entre compilas
0% entre las fuentes mencionadas
2% Idiomas no reconocidos
1% Textos potencialmente generados por la IA

Nombre del documento: CASO DE ESTUDIO FINAL COMPILATIO- Yoely Paredes.docx
ID del documento: c1cf97e4a7d0b0b2481ad1565e628b83d28713d
Tamaño del documento original: 85,88 kB

Depositante: DELGADO CUADRO ENRIQUE ISMAEL
Fecha de depósito: 20/8/2025
Tipo de carga: interface
fecha de fin de análisis: 20/8/2025

Número de palabras: 7962
Número de caracteres: 51.506

Ubicación de las similitudes en el documento:

Fuentes de similitudes

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	es.wikipedia.org	Recuperación de datos - Wikipedia, la enciclopedia libre https://es.wikipedia.org/wiki/Recuperación_de_datos 2 fuentes similares	< 1%	Palabras idénticas: < 1% (52 palabras)
2	www.softzone.es	TestDisk, programa para recuperar datos y particiones https://www.softzone.es/programas/sistema/testdisk/	< 1%	Palabras idénticas: < 1% (54 palabras)
3	www.ochobitshacenunbyte.com	Rescate de datos en Linux con Foremost - oc... https://www.ochobitshacenunbyte.com/2019/04/04/rescate-de-datos-en-linux-con-foremost/	< 1%	Palabras idénticas: < 1% (38 palabras)
4	descargatic.com	TestDisk — Descarga gratuita. Recuperación de datos y particio... https://descargatic.com/testdisk/	< 1%	Palabras idénticas: < 1% (27 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	ESTUDIO DE CASO.pdf | ESTUDIO DE CASO Viene de/en mi grupo	< 1%		Palabras idénticas: < 1% (20 palabras)
2	dspace.utb.edu.ec https://dspace.utb.edu.ec/bitstream/handle/49000/16180/E-UTB-FAFI-SIST-INF-000261.pdf?se...	< 1%		Palabras idénticas: < 1% (17 palabras)
3	tirescue.com | Pérdida de datos: Un riesgo invisible - Ti Rescue https://tirescue.com/perdida-de-datos-un-riesgo-invisible/	< 1%		Palabras idénticas: < 1% (10 palabras)
4	www.filehorse.com | TestDisk Descargar (2025 Última versión) https://www.filehorse.com/es/descargar-testdisk/	< 1%		Palabras idénticas: < 1% (11 palabras)
5	academia-lab.com | Disco de prueba _ Academia Lab https://academia-lab.com/enciclopedia/disco-de-prueba/	< 1%		Palabras idénticas: < 1% (10 palabras)