Polo del Conocimiento

Pol. Con. (Edición núm. 102) Vol. 10, No 1
Enero 2025, pp. 2251-2267
ISSN: 2550 - 682X
DOI: https://doi.org/10.23857/pc.v10i1.8808

Comparación del Rendimiento y Eficacia de las Herramientas de Análisis Forense en la Recuperación de Datos: Caso de estudio

Comparing the Performance and Effectiveness of Forensic Analysis Tools in Data Recovery: A Case Study

Comparar o desempenho e a eficácia das ferramentas de análise forense na recuperação de dados: um estudo de caso

Luis Fernando Guerrero-Pesantes [I]
luis.guerrerop@ug.edu.ec
https://orcid.org/0009-0008-7899-6270

Héctor Steven Morán-Suarez [II]
hector.morans@ug.edu.ec
https://orcid.org/0009-0001-1989-2235

Fausto Orozco-Lara [III]
fausto.orozcol@ug.edu.ec
https://orcid.org/0000-0003-4872-3702

Janeth Pilar Díaz-Vera [IV]
janeth.diazv@ug.edu.ec
https://orcid.org/0000-0001-8750-0216

Correspondencia: luis.guerrerop@ug.edu.ec

Ciencias Técnicas y Aplicadas
Artículo de Investigación

*** Recibido:** 14 de noviembre de 2024 ***Aceptado:** 11 de diciembre de 2024 *** Publicado:** 23 de enero de 2025

I. Estudiante Universidad de Guayaquil, Ecuador.
II. Estudiante Universidad de Guayaquil, Ecuador.
III. Docente Universidad de Guayaquil, Ecuador.
IV. Docente Universidad de Guayaquil, Ecuador.

Resumen

En este artículo basado de un proyecto de Titulación de la carrera de Tecnologías de la Información de la Universidad de Guayaquil sobre estudio comparativo del rendimiento y eficacia de las herramientas de análisis forense en la recuperación de datos, tiene por objetivo principal evaluar el rendimiento y la eficacia de diversas herramientas de análisis forense digital en la recuperación de datos, con el fin de identificar la más efectiva. La metodología aplicada fue un enfoque mixto que combinó análisis cuantitativos y cualitativos, se evaluó por medio de pruebas controladas a cada una de las herramientas forenses donde se midieron el tiempo, precisión y capacidad de recuperación de datos, se realizaron entrevistas dirigidas a profesionales en el área de la seguridad informática o de las tecnologías de la información. Los resultados revelaron que FTK Imager es la herramienta de análisis forense más efectiva para la recuperación de datos, aunque Autopsy puede ser considerada para investigaciones donde la velocidad no sea un factor importante. A partir de la documentación de los procedimientos y resultados en este estudio comparativo, se publicó un artículo científico que fomenta la participación en el área de la informática forense que es fundamental para el conocimiento de un público interesado en las herramientas de análisis forense.

Palabras clave: eficacia; análisis forense; recuperación de datos; rendimiento; herramientas forenses.

Abstract

This article is based on a thesis project of the Information Technology degree at the University of Guayaquil on a comparative study of the performance and effectiveness of forensic analysis tools in data recovery. The main objective is to evaluate the performance and effectiveness of various digital forensic analysis tools in data recovery, in order to identify the most effective one. The methodology applied was a mixed approach that combined quantitative and qualitative analysis. Each of the forensic tools was evaluated through controlled tests where time, precision and data recovery capacity were measured. Interviews were conducted with professionals in the area of computer security or information technology. The results revealed that FTK Imager is the most effective forensic analysis tool for data recovery, although Autopsy can be considered for investigations where speed is not an important factor. Based on the documentation of the procedures and results in this comparative study, a scientific article was published that encourages

participation in the area of forensic computing, which is essential for the knowledge of an interested public in forensic analysis tools.

Keywords: effectiveness; forensic analysis; data recovery; performance; forensic tools.

Resumo

Neste artigo baseado num projeto de graduação da carreira de Informática da Universidade de Guayaquil sobre um estudo comparativo do desempenho e eficácia das ferramentas de análise forense na recuperação de dados, o principal objetivo é avaliar o desempenho e a eficácia das ferramentas utilizadas a recuperação de dados. A metodologia aplicada foi uma abordagem mista que combinava a análise quantitativa e qualitativa, cada uma das ferramentas forenses foi avaliada através de testes controlados onde foram medidos o tempo, a precisão e a capacidade de recuperação de dados, foram realizadas entrevistas a profissionais da área de segurança informática ou tecnologia da Informação. Os resultados revelaram que o FTK Imager é a ferramenta de análise forense mais eficaz para a recuperação de dados, embora o Autopsy possa ser considerado para investigações em que a velocidade não é um fator importante. Com base na documentação dos procedimentos e resultados deste estudo comparativo, foi publicado um artigo científico que incentiva a participação na área da computação forense, essencial para o conhecimento de um público interessado em ferramentas de análise forense.

Palavras-chave: eficácia; análise forense; recuperação de dados; desempenho; ferramentas forenses.

Introducción

La investigación en análisis forense digital ha adquirido gran relevancia en los últimos años debido al aumento de delitos informáticos. La recuperación de datos se erige como un pilar fundamental para reconstruir eventos y presentar evidencia ante entidades judiciales. Sin embargo, el desempeño y la eficacia de las herramientas utilizadas varían considerablemente, lo que subraya la necesidad de evaluarlas de forma sistemática. Este estudio busca responder a la pregunta: ¿Cuáles son las herramientas más eficaces y de mayor rendimiento en recuperación de datos?

A continuación, se describen las herramientas de recuperación de datos que se eligieron para esta investigación:

- Autopsy: Es una herramienta con interfaz gráfica de usuario que muestra resultados de la búsqueda forense, es muy usada por la policía, militares y empresas cuando necesitan investigar lo ocurrido en algún equipo.
- PhotoRec: Herramienta que recupera datos y archivos perdidos incluyendo videos, documentos y archivos de disco duro.
- Osforensics: Es una herramienta creada por Passmark que se usa en el ámbito forense digital, ya que permite encontrar información visible, oculta o borrada del análisis informático.
- DiskDrill: Herramienta usada para recuperar documentos, archivos de video, imágenes y otros tipos de datos.

El análisis forense se conforma de una disciplina científica organizada que se enfoca más allá del simple análisis técnico de dispositivos electrónicos, su método severo está elaborado de manera que pueda garantizar que toda evidencia digital pueda ser usada de forma efectiva en los procesos judiciales, lo que demanda a seguir protocolos rigurosos en cada fase del proceso investigativo.

Antecedentes

La informática forense es una disciplina fundamental en la investigación de incidentes relacionados con la tecnología de la información de acuerdo a Arqués et al (2020) describen que "la informática forense es la ciencia forense que se encarga de poder asegurar, identificar, recoger, preservar, analizar y presentar la evidencia digital, de manera que la información recopilada sea aprobada en un proceso judicial" (p. 10). Asi también como Tapia (2022) definió la informática forense como una disciplina que aplica métodos científicos y técnicos para salvaguardar evidencia digital, garantizando su integridad y admisibilidad legal. Para Espinoza (2019) señala que el área de la informática forense ha tenido un aumento considerable en los últimos años, junto con los nuevos profesionales especializados en el campo de la informática forense. Es por ello que utilizar herramientas para desarrollar casos forenses ha sido clave, pero hay gran variedad en el mercado, según el autor Espinoza (2019), la selección adecuada de herramientas es crucial para garantizar el éxito en el procesamiento de evidencia digital. El estudio pone de manifiesto que no existe una "herramienta universal" que cubra todas las necesidades del análisis forense. Las decisiones deben basarse en factores como el tipo de sistema de archivos, la cantidad de datos a procesar y el nivel

de experiencia del analista. De esta forma el comparar herramientas comparar herramientas es el eje central de este estudio tal como Costa (2019) que realizó un análisis comparativo de herramientas para el examen forense en dispositivos móviles, proponiendo una metodología que abarca las etapas de recolección, examinación, análisis y reporte. Su trabajo concluyó que el conocimiento de múltiples herramientas es fundamental para abordar las necesidades específicas de cada caso. De igual manera MayanKLovanshi (2020) publicó un estudio comparativo sobre herramientas forenses, evaluando su desempeño en tareas como el volcado de RAM y el análisis de registros. Este trabajo se enfocó en parámetros clave como la velocidad de recuperación y la precisión, proporcionando datos útiles para la selección de herramientas. La integridad de la información es esencial al momento de recuperar datos, por lo cual la herramienta seleccionada juega un papel importante. Como lo explica Sabini (2021) que abordó la integridad de los datos en el contexto de las investigaciones forenses, enfatizando la importancia de preservar la calidad de la información durante todo su ciclo de vida. También tomando en cuenta que la cantidad de tipos de archivos que maneja la herramienta la hará sobresalir, Mallón (2024) exploró los sistemas de archivos como mecanismos clave para la organización y recuperación de datos, destacando la importancia de estructuras eficientes en el manejo de grandes volúmenes de información. Por lo cual ,al existir gran variedad de herramientas, la decisión de elegir cual es la mejor puede variar según el caso y el tiempo, ya que el cambio constante de la tecnología la actualización tanto de las herramientas y de los analistas será fundamental para la selección de las mismas es por eso que autores como (Suárez, 2020) y (Mendoza, 2024) coinciden en que la formación continua y la combinación de herramientas son esenciales para maximizar la eficacia en este campo.

Tipos de datos recuperables

En medio de la era tecnológica, la recuperación de datos es como tener un rompecabezas digital y armarlo con mucho cuidado. Los profesionales comienzan con una copia idéntica del dispositivo para no tocar los datos originales, después se tienen que revisar los sistemas de archivos, incluso salvando información que parecía haberse perdido de manera definitiva. No solo se encargan de buscar archivos, sino que también pistas en los registros del sistema que ayuden a detectar actividades sospechosas. (Duriva, 2024).

Entre los datos recuperables se pueden encontrar diferentes tipos:

Archivos eliminados: Son aquellos datos que fueron borrados de manera intencional por parte del usuario o por sistemas operativos, pero que, en la mayor parte de los casos, aún se mantienen en el

almacenamiento físico del dispositivo hasta que pueden llegar a ser sobrescritos, la recuperación de los datos depende del análisis de los metadatos y aunque el archivo esté eliminado, el sistema solo marca el espacio para que sea sobrescrito.

Datos fragmentados: Se refiere a cuando un archivo se almacena en partes separadas o fragmentadas en diversos sectores del disco. Por lo general ocurre cuando no hay suficiente espacio disponible, lo que ocasiona que el archivo se divida por el disco.

Sectores dañados: Los sectores corruptos en los discos duros de almacenamiento tienen un tema complicado, ya que en las áreas del disco duro presentan datos que han sufrido tanto un daño físico como lógico.

Metodología

La metodología aplicada en este estudio fue de modalidad mixta (cuantitativa y cualitativa), con un enfoque aplicado y comparativo. Se emplearon técnicas de investigación exploratoria y experimental para evaluar el rendimiento y la eficacia de cinco herramientas de análisis forense en la recuperación de datos. La fase exploratoria identificó características clave de las herramientas y estableció una base de conocimiento inicial, mientras que la experimental realizó pruebas controladas para comparar aspectos como velocidad, precisión y capacidad de recuperación. La investigación incluyó estadísticas descriptivas y análisis de varianza (ANOVA) para obtener datos objetivos, complementados con entrevistas a tres profesionales que enriquecieron el análisis con perspectivas cualitativas. Este enfoque integral permitió generar resultados prácticos, relevantes y aplicables tanto en el ámbito técnico como académico. “El rendimiento de una herramienta de análisis forense en la recuperación de datos depende de su capacidad para realizar procesos complejos, como el file carving, con alta precisión y en un tiempo razonable” (Precilla, 2019). Además, según (Murudumbay, 2022), “la implementación de una metodología estructurada permite garantizar la integridad de los datos y la validez de la evidencia obtenida”. Así mismo como “El éxito del análisis forense depende en gran medida de la preparación previa y de la selección de herramientas adecuadas” (Guzmán, 2023). Además, (Rada, 2022) subraya que “las herramientas de software deben ser robustas y flexibles para manejar diversos formatos de datos y estructuras de archivos complejas”.

Población

En las herramientas forenses estuvo compuesto por las herramientas que se enfocaran en la recuperación de datos, que estén disponibles en el mercado o en el ámbito académico que puedan cumplir con criterios de relevancia y popularidad.

En el grupo selecto se consideró pertinente la perspectiva de profesionales en áreas relacionadas como la seguridad informática o tecnologías de la información con el fin de obtener información relevante sobre la eficiencia de herramientas de análisis forense y recuperación de datos.

Muestra

La muestra selecciono a 5 herramientas de análisis forense que permita un análisis detallado de cada una, asegurando que se pueda realizar una comparación significativa y practica dentro de los límites del proyecto.

Dentro de la población de profesionales en seguridad informática o tecnologías de la información se considera pertinente la consulta de 3 individuos que posean conocimiento sobre herramientas de análisis forense y se los tomó como parte de la muestra para brindar apoyo en la recolección de información.

Técnicas e Instrumentos

Técnica de Recolección de datos

Se realizó una revisión documental de las herramientas forenses para comprender sus capacidades y limitaciones, se elaboro pruebas controladas para medir el rendimiento y eficacia de las herramientas seleccionadas, evaluando la velocidad, precisión y capacidad de recuperación de datos. Por ultimo se ejecutó tres entrevistas a profesionales en el área de la seguridad informática para obtener una perspectiva cualitativa de las herramientas forenses.

Instrumentos

Se diseño pruebas controladas para medir el tiempo, precisión y capacidad de recuperación de los datos por cada herramienta. Para el guion de la entrevista contó con preguntas dirigidas a los profesionales para complementar los resultados de las pruebas. Se utilizó el software Jamovi para el análisis estadístico, en especial para la aplicación de ANOVA.

Procedimiento

Se preparo la prueba controlada para las 5 herramientas forenses seleccionadas: PhotoRec, Disk Drill, OSForensics, FTK Imager y Autopsy. La entrevista contó con 5 preguntas abiertas a los 3 profesionales en el área de seguridad y tecnologías para saber más acerca de las herramientas evaluadas.

Aplicación de la prueba controlada

La prueba consistió en determinar el rendimiento y eficacia de las herramientas de análisis forense al recuperar 805 MB de datos eliminados en un USB de 8GB, midiendo el tiempo, la precisión y la capacidad de los datos recuperados, donde se realizó por la prueba 3 repeticiones en cada herramienta para poder evaluar mejor cada métrica.

Figura 1. USB para pruebas

Nota. Obtenido de https://www.amazon.com/-/es/SanDisk-Cruzer-Blade-SDCZ50-008G-B35-Unidad/dp/B002U28LZC

En el dispositivo USB se subieron datos para después eliminarlos de manera intencionada y se pueda realizar la prueba de recuperación.

Tabla 1 Archivos a recuperar del USB

Tipos de archivos	Tamaño	Cantidad
Documentos	22,3 MB	20
Imágenes	71,5 MB	20
Música	118 MB	15
Videos	397 MB	14
Otros	195 MB	9
Total de archivos	**805 MB**	**78**

Nota. Datos obtenidos de la prueba

La tabla muestra los datos a ser recuperados en la prueba donde se especifican los tipos de archivos, el tamaño y la cantidad de archivos. Cada herramienta seleccionada para la prueba deberá recuperar esta información, donde se tendrá que medir el tiempo, precisión y capacidad de recuperación.

Resultados

Figura 2. Datos para el análisis de las métricas

	Herramie...	Repeticion	Tiempo de Recuperación (Segundos)	Precisión (Porcentaje)	Capacidad de recuperación (Porcentaje)
1	PhotoRec	1	368	93.51	86.71
2	PhotoRec	2	363	93.59	87.33
3	PhotoRec	3	365	91.03	87.45
4	Disk Drill	1	331	98.72	90.06
5	Disk Drill	2	334	96.15	89.69
6	Disk Drill	3	327	93.59	89.44
7	OSForensics	1	329	97.44	90.47
8	OSForensics	2	331	94.88	88.96
9	OSForensics	3	337	93.58	88.77
10	FTK Imager	1	332	98.72	90.06
11	FTK Imager	2	324	97.44	93.79
12	FTK Imager	3	326	96.15	91.93
13	Autopsy	1	554	97.44	93.17
14	Autopsy	2	565	98.72	90.68
15	Autopsy	3	558	96.15	92.55

Nota. La tabla muestra los resultados de las métricas de las herramientas de recuperación de datos. Obtenido del software de Jamovi.

De estos datos se obtuvieron los resultados de las siguientes pruebas estadísticas:

Estadística Descriptiva

El análisis descriptivo es una herramienta importante en la investigación y la interpretación de los datos, ya que proporciona una visión general y comprensible de los datos obtenidos de las pruebas realizadas, se lo aplicó por medio del software Jamovi, donde nos presentó tablas de las métricas evaluadas de cada herramienta forense.

Tabla 2. Datos descriptivos de las métricas evaluadas

	Herramienta	N	Perdidos	Media	Mediana	DE
Tiempo de Recuperación (Segundos)	**PhotoRec**	3	0	365.3	365	2.517
	Disk Drill	3	0	330.7	331	3.512
	OSForensics	3	0	332.3	331	4.163
	FTK Imager	3	0	327.3	326	4.163
	Autopsy	3	0	559.0	558	5.568
Precisión (Porcentaje)	**PhotoRec**	3	0	92.7	93.5	1.455
	Disk Drill	3	0	96.2	96.2	2.565
	OSForensics	3	0	95.3	94.9	1.964
	FTK Imager	3	0	97.4	97.4	1.285
	Autopsy	3	0	97.4	97.4	1.285
Capacidad de recuperación (Porcentaje)	**PhotoRec**	3	0	87.2	87.3	0.397
	Disk Drill	3	0	89.7	89.7	0.312
	OSForensics	3	0	89.4	89.0	0.932
	FTK Imager	3	0	91.9	91.9	1.865
	Autopsy	3	0	92.1	92.5	1.296

Nota. Tabla de los datos obtenidos de las métricas de cada herramienta forense. Obtenido del software Jamovi.

Interpretación:

La tabla muestra en el tiempo de recuperación, FTK Imager cuenta con el promedio mas bajo seguido de OSForensics y Disk Drill, mientras que Autopsy es significativamente mas lenta. En términos de precisión, FTK Imager como Autopsy tiene un promedio de 97.4%, mientras que PhotoRec es la menos precisa con un 92.7%. En la capacidad de recuperación, Autopsy sobresale

con un 92.1%, seguido de FTK Imager con 91.9%, mientras que PhotoRec tiene el porcentaje mas bajo con un 87.2%. La mediana confirma que los resultados son consistentes con los promedios en gran parte de las métricas.

Análisis comparativo de medias

Para este análisis comparativo de medias se utilizó el software Jamovi que nos permitió realizar el análisis de varianza ANOVA de un factor. En primer lugar, se aplicó la prueba de normalidad y homogeneidad para verificar si los datos cumplen con los supuestos necesarios para poder ejecutar un ANOVA. Los resultados mostraron que en la prueba de normalidad las tres métricas evaluadas presentan valores de p mayores a 0.005. Lo que indica que no hay evidencia suficiente para rechazar la hipótesis nula de normalidad en los datos, sugiriendo que las métricas siguen una distribución normal. En la prueba de Levene para homogeneidad de varianzas muestra que los valores p para las métricas son mayores a 0.05. Esto significa que no hay evidencia suficiente para rechazar la hipótesis nula de igualdad de varianzas entre los grupos, indicando que las varianzas son homogéneas para las métricas. Por lo que el supuesto de homogeneidad de varianzas para aplicar ANOVA se cumple.

Tabla 3. Datos del ANOVA de Un Factor

	F	gl1	gl2	p
Tiempo de Recuperación (Segundos)	1764.99	4	10	<.001
Precisión (Porcentaje)	3.61	4	10	0.045
Capacidad de recuperación (Porcentaje)	9.98	4	10	0.002

Nota. Tabla de los resultados de las métricas del ANOVA de Un factor. Obtenido del software de Jamovi.

Interpretación:

La tabla del análisis ANOVA de un factor muestra diferencias significativas entre las herramientas de análisis forense en las métricas evaluadas. En el tiempo de recuperación, el valor de F (1764.99) y el $p < 0.001$ indican una gran variabilidad entre las herramientas. En la precisión, el valor de F (3.61) y el $p = 0.045$ demuestran que, aunque las diferencias son menores en comparación con el tiempo, aun son significativas. Por último, en la capacidad de recuperación, el valor de F (9.98) y el $p = 0.002$ sugieren que hay diferencias evidentes en la métrica entre las herramientas.

La prueba Post-Hoc de Tukey se utilizó para poder realizar diversas comparaciones entre grupos después de obtener un resultado significativo en un análisis de varianza (ANOVA). Esta prueba permitió identificar a los pares de grupos que tienen diferencias significativas en sus medias.

Tabla 4. Prueba Tukey Post-Hoc – Tiempo de recuperación (Segundos)

			PhotoRec	Disk Drill	OSForensics	FTK Imager	Autopsy
PhotoRec	**Diferencia de medias**		—	34.7	33.00	38.00	-194
	valor p		—	<.001	<.001	<.001	<.001
Disk Drill	**Diferencia de medias**			—	-1.67	3.33	-228
	valor p			—	0.986	0.852	<.001
OSForensics	**Diferencia de medias**				—	5.00	-227
	valor p				—	0.590	<.001
FTK Imager	**Diferencia de medias**					—	-232
	valor p					—	<.001
Autopsy	**Diferencia de medias**						—
	valor p						—

Nota. Tabla de los resultados de la prueba Tukey Post-Hoc del tiempo de recuperación. Obtenido del software Jamovi.

Interpretación:

La tabla del análisis Post-Hoc de Tukey demuestra que Autopsy tiene un tiempo de recuperación significativamente más lento que las demás herramientas forenses, con diferencias de medias de -232 comparado con FTK Imager, y valores p menores a 0.001, lo que es estadísticamente significativo. FTK Imager, destaca como la herramienta más eficiente, siendo veloz y consistente en la recuperación de datos. No se encontraron diferencias significativas entre Disk Drill, OSForensics y FTK Imager, esto sugiere que estas herramientas cuentan con un rendimiento similar. Por otro lado, PhotoRec se revelo significativamente más lento que Disk Drill,

OSForensics y FTK Imager. Estos resultados demuestran que FTK Imager es superior en términos de tiempo de recuperación.

Tabla 5. Prueba Tukey Post-Hoc – Precisión (Porcentaje)

			PhotoRec	Disk Drill	OSForensics	FTK Imager	Autopsy
PhotoRec	**Diferencia de medias**		—	-3.44	-2.590	-4.73	-4.73
	valor p		—	0.201	0.433	0.053	0.053
Disk Drill	**Diferencia de medias**			—	0.853	-1.28	-1.28
	valor p			—	0.974	0.897	0.897
OSForensics	**Diferencia de medias**				—	-2.14	-2.14
	valor p				—	0.602	0.602
FTK Imager	**Diferencia de medias**					—	0.00
	valor p					—	1.000
Autopsy	**Diferencia de medias**						—
	valor p						—

Nota. Tabla de los resultados de la prueba Tukey Post-Hoc de la Precisión. Obtenido del software Jamovi.

Interpretación:

La tabla del análisis de Post-Hoc de Tukey presenta los resultados de la métrica de precisión entre las herramientas de análisis forense. En este caso ninguna de las comparaciones demuestra diferencias significativas, ya que los valores de p son mayores a 0.05. Las diferencias de medias entre las herramientas son parcialmente pequeñas, y los valores de p más cercanos a ser significativos son entre PhotoRec y FTK Imager/Autopsy donde p = 0.053. Esto indica que, aunque hay leves diferencias en la precisión entre las herramientas forenses, no son lo suficientemente grandes como para ser significativas.

Tabla 8 Prueba Tukey Post-Hoc – Capacidad de recuperación (Porcentaje)

			PhotoRec	Disk Drill	OSForensics	FTK Imager	Autopsy
PhotoRec	**Diferencia de medias**		—	-2.57	-2.237	-4.76	-4.970
	valor p		—	0.106	0.181	0.003	0.002
Disk Drill	**Diferencia de medias**			—	0.330	-2.20	-2.403
	valor p			—	0.996	0.192	0.138
OSForensics	**Diferencia de medias**				—	-2.53	-2.733
	valor p				—	0.113	0.080
FTK Imager	**Diferencia de medias**					—	-0.207
	valor p					—	0.999
Autopsy	**Diferencia de medias**						—
	valor p						—

Nota. Tabla de los resultados de la prueba Tukey Post-Hoc de la capacidad de recuperación. Obtenido del software Jamovi.

Interpretación:

La tabla del análisis de Post-Hoc de Tukey muestra los resultados de la métrica de capacidad de recuperación entre las herramientas de análisis forense. Se puede observar diferencias significativas entre PhotoRec y FTK Imager (p = 0.003) y entre PhotoRec y Autopsy (p = 0.002), demostrando que estas herramientas tienen diferencias significativas en su capacidad de recuperación. Las diferencias de medias mas destacables son entre PhotoRec y Autopsy (-4.970) y entre PhotoRec y FTK Imager (-4.76). En cambio, las diferencias significativas entre Disk Drill y las demás herramientas, como Entre OSForensics y Autopsy, no son significativas ya que los valores p son mayores a 0.05. Esto demuestra que FTK Imager y Autopsy resaltan por tener una capacidad de recuperación significativamente mayor en comparación son PhotoRec.

Análisis de las entrevistas

Como podemos notar dos de los expertos mencionan a FTK Imager como una de las mejores, por otro lado uno de los expertos se inclinó hacia Autopsy, también se evidencia que en los criterios coinciden mucho, ya que según sus experiencias el tiempo es un factor importante en la recuperación de datos, adicional de que hubo coincidencia en la herramienta más eficiente, también lo hubo en la herramienta más fácil de usar que es PhotoRec, cabe señalar que esta no está relacionada a la eficiencia, sino más bien a lo amigable que es con el usuario. Esto demuestra que hay coincidencia entre las herramientas populares y ejes en este proyecto de investigación.

Conclusiones

El estudio comparativo revelo que las herramientas de análisis forense digital tienen distintas características y capacidades específicas que las vuelven indispensables dependiendo del caso en que se las utilicen. Las herramientas como FTK Imager y Autopsy sobresalieron por su interfaz gráfica y la capacidad de poder procesar cantidades grandes de datos, pero en el caso de PhotoRec se destacó por contar con la recuperación de particiones y archivos dañados. Estos cambios que presentan las herramientas forenses señalan la importancia de una evaluación cuidadosa al momento de escoger herramientas según las necesidades específicas de requiera cada investigación, ya que una herramienta no puede llegar a garantizar resultados perfectos.

En las pruebas controladas del análisis comparativo se demostró que las herramientas como FTK Imager y Autopsy son bien efectivas por su alta precisión y capacidad de recuperación, mientras que PhotoRec presento limitaciones en la precisión y capacidad de recuperación. Las diferencias en velocidad mostraron que Autopsy cuenta con menos eficiencia en escenarios donde el tiempo es muy importante para las investigaciones, pero las herramientas de análisis forense tuvieron un rendimiento sólido en gran parte de las pruebas, resaltando sobre todo en la herramienta FTK Imager por tener los resultados más favorables en las métricas del tiempo, precisión y capacidad de recuperación, demostrando que es la más efectiva para la recuperación de datos.

El análisis de las entrevistas reveló que herramientas como FTK Imager son muy eficaces en áreas profesionales de análisis forense para la recuperación de datos, en cuanto a PhotoRec sobresalió por la facilidad de uso para principiantes que estén comenzando a trabajar con herramientas forenses. Sin embargo, se presentaron limitaciones enfocadas con la necesidad de capacitación técnica para aumentar su conocimiento en el área forense. En los criterios mencionados los

profesionales están de acuerdo según sus experiencias que el tiempo es un factor muy importante en la recuperación de datos.

Recomendaciones

Se recomienda elaborar una selección completa de herramientas forenses que permitan evaluar sus características específicas según el caso que este investigando. Esto implicaría la creación de una base de datos actualizada sobre las capacidades y limitaciones que tengan cada herramienta, como FTK Imager, Autopsy y PhotoRec, así los profesionales podrán elegir con precisión. También, se podrían realizar metodologías estandarizadas que cuenten con guías prácticas para determinar la herramienta forense más conveniente.

Se recomienda usar FTK Imager como la herramienta principal en investigaciones forenses digitales ya que su notorio desempeño tanto en la velocidad, precisión y capacidad de recuperación, la coloca como la opción más efectiva en escenarios complejos donde se necesita un análisis forense completo. Autopsy con buenos resultados en la precisión y capacidad de recuperación, puede ser utilizado en casos donde la rapidez no sea un factor decisivo. En cambio, PhotoRec es más conveniente para investigaciones que tengan menos exigencias, por lo que seleccionar la herramienta forense correcta según las necesidades que se requieran asegurara buenos resultados en el análisis forense.

Se recomienda para las limitaciones enfocadas en la capacitación técnica, la creación de programas que cuenten con formación especializada en informática forense, que permitan acceder a usuarios con distintos niveles de experiencia. Los programas deben centrase en herramientas forenses como FTK Imager y PhotoRec, para incorporar prácticas en tiempo real y así aprender a utilizar la herramienta. Se puede introducir módulos sobre la gestión del tiempo en la recuperación de datos, un punto importante que los profesionales marcaron como crítico, garantizando así que los profesionales controlen de manera eficiente los desafíos en investigaciones forenses.

Referencias

1. Arqués, J., Colobran, M., & Gargallo, E. d. (2020). Informática forense, febrero 2020. FUOC. http://hdl.handle.net/10609/150231
2. Costa, L. A. (28 de Noviembre de 2019). UJA. https://hdl.handle.net/10953.1/11909

3. Duriva. (2024). Duriva. https://duriva.com/como-la-informatica-forense-ayuda-a-recuperar-datos-y-evidencia-perdida/
4. Espinoza, M. (2019). Desarrollo y aplicación de técnicas forenses.
5. Guzmán, L. (2023). Importancia de la preparación previa en el análisis forense.
6. Mallón , X. (23 de Abril de 2024). KeepCoding. https://keepcoding.io/blog/que-es-un-sistema-de-archivos/#:~:text=Un%20sistema%20de%20ficheros%2C%20sistema,ellos%20de%20una%20forma%20r%C3%A1pida.
7. MayanKLovanshi, P. B. (2020). Benchmarking of Digital Forensic Tools. https://doi.org/10.1007/978-3-030-41862-5_95
8. Mendoza, M. d. (2024). nterpretación y Desafíos de la Evidencia Digital en la Investigación Criminal. Código Científico Revista De Investigación,5(E3), 480–498. https://doi.org/https://doi.org/10.55813/gaea/ccri/v5/nE3/328
9. Murudumbay, M. J. (2022). Marco de trabajo y herramientas para el análisis forense en la atención de los delitos informáticos de Cibergrooming bajo los dispositivos móviles Android. Pro Sciences: Revista De Producción, Ciencias E Investigación. https://doi.org/https://doi.org/10.29018/issn.2588-1000vol6iss43.2022pp280-296
10. Precilla, J. (2019). Eficiencia en la recuperación de datos forenses.
11. Rada, M. (2022). Importancia de las herramientas de software en el análisis forense.
12. Sabini, J. (19 de Enero de 2021). Estudio desde Casa. https://estudiodesdecasa.com.ar/dispositivos-de-almacenamiento/
13. Suárez Bohórquez, W. (2020). Utilización de herramientas informáticas FTK Imager y Autopsy para el análisis forense de evidencia digital a una memoria USB [Trabajo de grado, Universidad Tecnológica de Bolívar]. Repositorio UTB. https://hdl.handle.net/20.500.12585/11413
14. Tapia, J. (2022). Origen de la Informática forense. https://doi.org/10.13140/RG.2.2.18012.97927