UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

ABRIL 2024 – AGOSTO 2024

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERA EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS DE HERRAMIENTAS DE ANÁLISIS FORENSE Y SU APLICABILIDAD EN LA INVESTIGACIÓN DE DELITOS INFORMÁTICOS

ESTUDIANTE:

JULISSA MARIÚ CONTRERAS CONTRERAS

TUTOR:

ING. IVAN RUIZ

AÑO 2024

ÍNDICE

RESUMEN 4
SUMMARY 5
PLANTEAMIENTO DEL PROBLEMA 6
JUSTIFICACIÓN 8
OBJETIVOS 9
OBJETIVOS GENERALES 9
OBJETIVOS ESPECÍFICOS 9
LÍNEAS DE INVESTIGACIÓN 10
MARCO CONCEPTUAL 11
Análisis Forense 11
Vulnerabilidades 11
Delitos informáticos 11
Tipos de delitos informáticos 12
Fraude por manipulación informática 12
Manipulación de entradas 12
Manipulación del software 13
Falsificación informática 13
Dañar o alterar programas o datos de computadora. 13
Sabotaje informático 13
Virus 14
Gusanos 14
Piratas o hackers 14
Reproducción no autorizada de software informático de defensa legal 15
Evidencia digital 15
Auditoria Informática 15
Informática Forense 16
Objetivos de la informática forense 17
Utilidad de la informática forense 17
¿Por qué se necesita información forense digital? 18
Fase de obtención de evidencias digitales 19
Fase preservación de evidencias digitales 19
Fase de análisis de evidencias digitales 19
Fase de documentación de la investigación forense informática 19
Herramientas de análisis forense 20
Autopsy 20

Características:.....20
Ventajas:.....21
Desventajas:.....21
Osforensics.....22
Ventajas:.....22
MARCO METODOLOGICO.....23
Revisión de la literatura.....23
ENTREVISTA.....29
RESULTADO.....40
DISCUSION DE RESULTADOS.....42
CONCLUSIÓN.....44
RECOMENDACIONES.....45
BIBLIOGRAFIA.....46
ANEXOS.....48

RESUMEN

La información forense es esencial en la seguridad informática, especialmente con el aumento de la tecnología y los ciberataques. Este campo se dedica a la adquisición, verificación y preservación de información digital en diversos dispositivos y sistemas operativos. Las herramientas forenses permiten recuperar información, restaurar archivos eliminados y verificar acciones específicas, generando informes precisos para uso legal.

La clave de la informática forense es seleccionar la herramienta adecuada para cada investigación, junto con la experiencia del investigador. El incremento en el uso de equipos informáticos y telecomunicaciones con acceso a internet ha elevado los incidentes de seguridad informática, haciendo que la informática forense sea crucial para identificar y analizar los autores de delitos informáticos.

La informática forense utiliza técnicas y métodos para reconstruir la secuencia de eventos basada en hardware o tecnología durante un incidente. Este trabajo pretende demostrar la importancia y la eficacia de las herramientas informáticas forenses evaluando objetiva su impacto en la investigación de delitos informáticos.

Palabras claves: Informática forense, ciberataques, herramientas forenses, delitos informáticos, seguridad informática.

SUMMARY

Forensic information is essential in cybersecurity, especially with the rise of technology and cyberattacks. This field is dedicated to the acquisition, verification and preservation of digital information on various devices and operating systems. Forensic tools allow you to recover information, restore deleted files and verify specific actions, generating accurate reports for legal use.

The key to computer forensics is selecting the right tool for each investigation, along with the experience of the investigator. The increase in the use of computer and telecommunications equipment with Internet access has increased computer security incidents, making computer forensics crucial to identify and analyze the perpetrators of computer crimes.

Computer forensics uses techniques and methods to reconstruct the hardware or technology-based sequence of events during an incident. This work aims to demonstrate the importance and effectiveness of computer forensic tools by objectively evaluating their impact on the investigation of computer crimes

Keywords: Computer forensics, cyber attacks, forensic tools, computer crimes, computer security.

PLANTEAMIENTO DEL PROBLEMA

Actualmente los sistemas informáticos no comprenden la importancia que tienen al ser el principal motor de gestión y procesamiento de la información que posee una organización para cumplir plenamente con su lógica de negocio. Al mismo tiempo todo lo relacionado con la seguridad de la informática está adquiriendo más importancia para las organizaciones. Prácticamente es imposible que una organización no sistematice y debido a ello, no se preocupe por la seguridad de sus activos de información, estos recursos están abiertos a amenazas ocultas, principalmente debido a la conexión de sus redes internas y redes externas facilitadas por el proveedor que les brinda acceso a internet.

El principal problema es la no actualización de las herramientas de análisis forense de acuerdo a los constantes avances tecnológicos, es por esto que surge la interrogante si las herramientas son lo suficientemente flexibles y adaptables para abordar las distintas necesidades de investigación informática. La interoperabilidad entre las diferentes herramientas y compatibilidad en la amplia variedad de plataformas son cuestiones esenciales que afectan a las investigaciones forenses en el ámbito de delitos informáticos.

Es muy importante tener en cuenta que dependiendo del tamaño de la organización en el mercado deberá gestionar el proceso de seguridad en su plataforma tecnológica y reservas de datos. Esto se explica que una organización poco conocida en el mercado no tiene el mismo interés en ser atacada en su plataforma tecnológica que una organización con una imagen sólida.

Desafortunadamente, ningún sistema informático puede proporcionar una seguridad perfecta y siempre habrá vulnerabilidades de seguridad que no se pueden eliminar, en estos casos las organizaciones deben intentar reducirlos tanto como sea posible y esto se logra mediante sistemas de gestión de seguridad de la información.

En la era digital actual, los delitos y abusos cibernéticos se han vuelto cada vez más comunes, con la aparición de la tecnología, han surgido nuevas oportunidades para la delincuencia y para protegernos a nosotros mismos y a nuestro activo. El ciberdelito se refiere a cualquier actividad, la distribución de malware, fraudes en línea y acoso.

Proteger la integridad de la evidencia digital es fundamental para la seguridad forense informática. Por este motivo, se debe considerar una serie de medidas y mejores prácticas para garantizar que sus datos no sean comprometidos ni alterados durante este proceso. Para proteger la privacidad, solo el personal autorizado tiene acceso a la evidencia digital. Es importante establecer restricciones de permisos para que sólo las personas autorizadas tengan acceso.

Estas herramientas forenses deben evaluarse para su empleo eficaz y rápido, es aquí donde entra en juego el campo de la seguridad informática, dado que es un conjunto de técnicas utilizadas para solucionar problemas de seguridad. los profesionales deben estar capacitados y familiarizados con las últimas tecnologías y técnicas para gestionar eficazmente las ciberamenazas.

JUSTIFICACIÓN

La información forense es un campo de la seguridad informática que está evolucionando debido a los avances tecnológicos y ciberataques, para lograr sus objetivos el campo se basa principalmente en software y cuenta con amplia gama de aplicaciones que permiten el estudio de eventos desde múltiples perspectivas. Estas aplicaciones, al igual que las industrias informáticas que respaldan, continúan evolucionando con la tecnología para lograr resultados óptimos.

En la ciencia forense las herramientas son muy esenciales porque permiten la adquisición, verificación, preservación segura y eficiente información digital, estas herramientas están creadas para funcionar con todo tipo de dispositivos y sistemas operativos ya sean computadoras, celulares, discos duros tablets, etc. Las herramientas de análisis forense tienen una diversidad de características que ayudan a la recuperación de información, archivos borrados y la verificación de acciones sospechosas. Estos programas permiten elaborar informes más precisos que puedan usarse como prueba en un caso

Una de las razones por las que la información forense es tan atractiva ya que permite a los investigadores encontrar la herramienta perfecta para su investigación, esto por supuesto debe combinarse con aspectos tan importantes como la experiencia y la iniciativa del investigador. Con este trabajo pretendemos demostrar la eficacia y eficiencia de las herramientas de informática forense más representativo del mercado de la manera más objetiva, clara, detallada y profesional.

OBJETIVOS

OBJETIVOS GENERALES

- Analizar herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos.

OBJETIVOS ESPECÍFICOS

- Identificar las principales herramientas de análisis forense utilizadas en la investigación de delitos informáticos.
- Evaluar la eficacia y eficiencia de las herramientas de análisis forense en la recolección y análisis de evidencia digital.
- Determinar la aplicabilidad de las herramientas de análisis forense en diferentes escenarios de delitos informáticos.

LÍNEAS DE INVESTIGACIÓN

La presente investigación está orientada con la línea de investigación Sistemas de información, comunicación y emprendimiento e innovación. Esta línea de investigación se relaciona directamente con el caso de estudio sobre su aplicabilidad en la investigación de delitos informáticos de las herramientas en análisis forense, ya que ambas están diseñadas para encontrar soluciones tecnológicas avanzadas y promover la innovación de la ciberseguridad.

Redes, tecnologías inteligentes de software y hardware la sublínea de investigación, se relacionan con el caso de estudio ya que ayudará a examinar la interrelación del flujo de datos con herramientas de análisis forense. La tecnología inteligente se enfoca en utilizar métodos y herramientas de aprendizaje que permiten la detección de amenazas para la toma de decisiones en el ámbito de los delitos informáticos.

Un marco teórico y conceptual lo conforman la línea y sub-línea de investigación ideal para el estudio de caso de las herramientas de análisis forense y su aplicabilidad a las investigaciones de delitos informáticos. Permiten evaluar los riesgos en detalle los enfoques multidisciplinarios y tecnológicos, proponer soluciones innovadoras y contribuir de manera importante al fortalecimiento de la protección de los sistemas informáticos.

MARCO CONCEPTUAL

Análisis Forense

La ciencia forense digital es una disciplina en expansión que se centra en la recopilación, análisis y presentación de evidencia digital relacionada con delitos o actos maliciosos. La disciplina tiene sus raíces en la ciencia forense y la informática tradicional, pero ha evolucionado hasta convertirse en una entidad única que abarca aspectos legales, éticos y de seguridad informática. (Rodrıguez, 2023)

Vulnerabilidades

Los piratas informáticos pueden acceder a los activos informáticos a través de agujeros en los sistemas y aprovechar las vulnerabilidades lo que se traduce en importantes pérdidas. En otra definición podemos decir que una vulnerabilidad es cualquier debilidad en cualquier característica que puede de alguna manera afectar el correcto funcionamiento de un sistema informático. Estas debilidades, también llamadas "agujeros de seguridad" pueden estar relacionadas con la implementación del software o la configuración del sistema operativo. (Samaniego, 2021)

Delitos informáticos

El delito cibernético es cualquier uso ilegal, delictivo y fraudulentos de dispositivos electrónicos e Internet con la finalidad de infiltrar, destruir o perjudicar los activos de las organizaciones. También conocido como delito cibernético, abarca muchas actividades ilegales diferentes. ya sea un medio o un fin la tecnología de la información es factor común.

Los delincuentes informáticos son expertos en el uso y conocimiento de la tecnología. Esto no sólo les ayuda a utilizarla, sino que también les brinda una buena oportunidad de lograr sus objetivos. Es por ello que una parte importante de los ciberdelitos contra las empresas son cometidos por empleados. (Seguridad , 2021)

Un agente utiliza la tecnología de la información o las comunicaciones para buscar beneficios ilegales para sí mismo o para otro en perjuicio de un tercero mediante el diseño, adición, modificación, eliminación, copia de datos informáticos o manipulación del funcionamiento de sistema informático. (Perez, 2019)

Según Fernández (2019) define el delito informático como la comisión de un acto que según las características se comete contra los derechos y libertades de los ciudadanos utilizando un elemento informático o telemático.

Tipos de delitos informáticos

Los ciberdelincuentes pueden ser diversos debido a la imaginación y las capacidades técnicas de los delincuentes, así como las vulnerabilidades de seguridad en los sistemas informáticos son delicada. Conozcamos sobre los diferentes delitos informáticos:

Fraude por manipulación informática

Manipulación de entradas

Este tipo de fraude informático, también conocido como robo de datos, es el ciberdelito más común porque es fácil de realizar y difícil de detectar. Este delito no requiere ningún conocimiento técnico informático y puede ser cometido por cualquier persona que tenga acceso a una función normal de procesamiento de datos en la etapa de obtención de la información (Hall, 2021).

Manipulación del software

Esto es muy difícil de detectar y muchas veces pasa desapercibido porque el delincuente necesita conocimientos especiales de informática. El delito consiste en modificar softwares existentes, agregar programas o procesos nuevos a un sistema informático. El llamado caballo de Troya es una técnica común utilizada por programadores informáticos, ocurre cuando se inyectan comandos en secreto en un programa de computadora que facilita realizar funciones no están permitidas durante el funcionamiento normal.

Falsificación informática

Falsificadores de computadoras

Las computadoras también se pueden utilizar para falsificar documentos para uso comercial. Cuando estuvieron disponibles las fotocopiadoras en color computarizadas con láser, apareció una nueva generación de falsificaciones. Estas fotocopiadoras pueden realizar copias de alta resolución, editar documentos e incluso falsificarlos sin depender del original, y los documentos producidos son de tan alta calidad que sólo los profesionales pueden distinguirlos de los documentos genuinos. (Hall, 2021)

Dañar o alterar programas o datos de computadora.

Sabotaje informático

Esta es la eliminación, alteración no autorizada de funciones o datos de la computadora con la intención de interferir con el funcionamiento normal del sistema. Las técnicas que permiten el sabotaje informático incluyen:

Virus

Un virus es un programa malicioso creado por piratas informáticos con una amplia programación para dañar el hardware de una o más computadoras al inyectar código malicioso infecta toda la maquina dejándola desprotegida y en mano de los atacantes.

Otra forma de definirlo es: Un virus informático es un programa o código malicioso y un agente de replicación que se inserta en cualquier dispositivo técnico sin su conocimiento o permiso, causando daños, problemas o interrupciones en la computadora, sistema y por lo tanto al usuario. (Robalino , Yanza , & Montoya, 2022)

Gusanos

Un gusano es un tipo de malware diseñado para propagarse a múltiples dispositivos que puede permanecer activo sin el conocimiento del usuario porque es autónomo y no requiere activación humana. Estos tipos de virus bloquean las computadoras y las redes informáticas, impidiendo que los programas funcionen correctamente. Este virus permanece sin ser detectado en el sistema durante un tiempo determinado luego paraliza la computadora e impide que funcione. (Robalino , Yanza , & Montoya, 2022)

Piratas o hackers

El acceso suele realizarse desde una ubicación externa ubicada en una red de telecomunicaciones utilizando uno de los diversos métodos siguientes: Medidas de seguridad débiles un atacante puede utilizar para obtener acceso o descubrir fallas en las medidas de seguridad o métodos del sistema existentes. Los piratas informáticos suelen hacerse pasar por usuarios legítimos del sistema. Esto sucede cuando el sistema donde los usuarios pueden usar contraseñas estándar o mantenimiento integradas en el propio sistema. (Hall, 2021)

Reproducción no autorizada de software informático de defensa legal

Esto puede causar graves pérdidas financieras a los propietarios legítimos, algunas jurisdicciones han penalizado este tipo de actividad con sanciones. Con el contrabando de estas copias no autorizadas a través de las modernas redes de telecomunicaciones, el problema ha alcanzado una dimensión transnacional. Por lo tanto, creemos que no es un delito informático la copia no autorizada de programas informáticos porque la propiedad legal que se protege es propiedad intelectual (Hall, 2021).

Evidencia digital

La evidencia digital se puede definir como información y datos almacenados o transmitidos por una computadora o dispositivo electrónico con fines de investigación, En las investigaciones criminales este tipo de evidencia puede ser importante porque puede proporcionar gran cantidad de información que no se obtener de otros medios. (Sosa, 2023)

Características principales de la evidencia digital:

- **Volátil:** Puede perderse si no se recoge a tiempo.
- **Duplicable:** Se pueden realizar varias copias sin identificar el original.
- **Alterable:** Se puede cambiar y/o eliminar sin registrar las acciones relevantes.
- **Anónimo:** En algunos casos no se puede identificar al autor.

Auditoria Informática

Una auditoría de TI es un examen y evaluación realizada sobre el software, hardware, sistemas e información utilizados por una organización para mejorar sus

procesos para medir el rendimiento y la utilización de los recursos de TI de la organización, evaluar su uso adecuado y los resultados que aportan a la organización.

Según Reascos Velastegui (2019), La auditoría informática se determina por un proceso ordenado y preciso enfocado a proteger la integridad, confidencialidad de los sistemas informáticos y computadoras. Esto implica realizar una revisión exhaustiva del sistema de control interno para determinar posibles debilidades y evaluar los riesgos asociados a la tecnología de la información.

En el contexto actual, con el crecimiento exponencial de las redes sociales y su impacto en la vida diaria, la seguridad y protección de los datos personales en estos entornos digitales debe cobrar cada vez más importancia. Las personas, empresas y organizaciones que operan en línea corren el riesgo de sufrir ataques cibernéticos que buscan obtener acceso no autorizado a registros y explotar información con multas maliciosas.

Informática Forense

La informática forense se ocupa de la extracción, preservación y análisis de evidencia cuando se producen violaciones de seguridad en sistemas informáticos, dispositivos móviles, discos duros, correos electrónicos entre otros. Los especialistas también pueden utilizar técnicas informáticas forenses en diversos litigios civiles, incluida la recuperación de datos y registros de auditoría, un analista forense proporciona seguridad de la información y respuestas a preguntas legales. (Herrera, Figueroa, & Lara, 2020)

Según Rodríguez (2024) La informática forense es un campo de la informática que reúne los conocimientos técnicos y científicos tiene como objetivo explicar hechos, acontecimientos concretos del pasado mediante la detección, almacenamiento, análisis y

registro de información relacionada con elementos hardware o software que sean tangibles y derivados de ella.

Objetivos de la informática forense

Cuando se producen brechas de seguridad cibernética por distintos tipos de delitos, la aplicación de la informática forense tiene los siguientes objetivos básicos:

- Facilitar la recuperación, analizar y preservar los equipos informáticos y sus componentes relacionados.
- Establecer la causa del crimen y la identidad del principal culpable.
- Crear un informe de investigación computarizado que proporcione una descripción detallada del proceso de investigación.

Utilidad de la informática forense

La informática forense tiene muchas utilidades, más aun teniendo en cuenta el uso cada vez mayor de la tecnología que se da hoy en día a todos los niveles, y el creciente número de ciberamenazas para empresas y usuarios. He aquí algunas instalaciones relevantes:

Aportación de pruebas en procedimientos judiciales: En casos de manipulación en robo de datos, ataques de malware, discos duros, el análisis forense puede aportar pruebas importantes en procedimientos judiciales físicos.

Aportar pruebas en las negociaciones: En el caso de las negociaciones colectivas, los datos pueden demostrar que los empleados hacen bien su trabajo. Al contrario, también es posible si el análisis forense determina que un empleado actúa encontrar de la empresa.

Seguro de Internet: El seguro contra ciberataques es cada vez más popular. Este contexto, en caso de violación de la seguridad, los expertos tienen que reunir pruebas para determinar si debe proporcionarse cobertura de seguro. Esto es similar a lo que ocurre en la suscripción de seguros de automóviles. (Romero, 2022)

¿Por qué se necesita información forense digital?

A medida que la tecnología se desarrolla y evoluciona cada vez más rápido, se puede transferir más información, como la comunicación, lo que da como resultado que una gran cantidad de información privada se aloje en Internet. La privacidad de cada ciudadano está garantizada por ley, sin embargo, los delitos cibernéticos a menudo violan estos derechos, por lo que se necesitan profesionales calificados que puedan obtener pruebas de la comisión de este tipo de delito. Estos expertos se denominan expertos en informática forense.

Los ciberataques se pueden llevar a cabo contra personas, empresas, organizaciones, etc, por lo que hacer un análisis forense digital es muy útil para saber cuál es el problema. En el caso de una empresa, son principalmente empleados experimentados quienes advierten y detectan los ciberataques, y en otros suele ser la policía. En ambos casos estos profesionales deben averiguar qué métodos y procedimientos utilizaron para identificar qué tipo de datos atacaron. (Borja , 2022)

El análisis forense se divide en 5 fases que ayudan a mantener la investigación en orden, promover la validación y reproducibilidad del análisis:

Fase de obtención de evidencias digitales

La fase de recolección de evidencia digital de la informática forense se determina el objeto de investigación y se obtiene la evidencia digital que se sospecha que está relacionada con el caso de la investigación. (CARVAJAL , 2024)

Fase preservación de evidencias digitales

La fase de preservación de la evidencia digital forense, debe permanecer intacta y poder demostrar que los elementos de la investigación posterior son consistentes durante la fase de adquisición con los resultados.

Fase de análisis de evidencias digitales

La fase de análisis de evidencia digital utiliza las técnicas y herramientas de la informática forense para extraer información relevante sobre los hechos de la investigación a partir de los elementos capturados y almacenados. La información debe estructurarse basándose en la lógica para que se puedan extraer una serie de conclusiones sobre un hecho. (Hidalgo, Yasaca, & Hidalgo, 2019)

Fase de documentación de la investigación forense informática

Durante la fase de documentación de una investigación forense informática se redactará el correspondiente informe informático. Dicho informe reflejará detalladamente la recolección y conservación de cada prueba digital, así como analizará los factores relevantes con suficiente detalle como para que puedan ser reproducidos por terceros en las mismas condiciones de sala. Finalmente, se contendrá las conclusiones de la investigación junto con los argumentos racionales obtenidos a partir de los hallazgos forenses. (CARVAJAL , 2024)

Fase de presentación de la investigación informática forense

El trabajo de informática forense realizado en el juicio debe explicar los hechos con la mayor claridad posible y corroborar a los peritos durante la audiencia. Los expertos deben ser lo más didácticos posible, tratando de hacer que la tecnología compleja sea comprensible para alguien que no sea un especialista en el campo. (CARVAJAL , 2024)

Herramientas de análisis forense

Las herramientas de informáticas forenses suelen estar conectadas a computadores y portátiles para realizar análisis forenses digitales. Estas herramientas pueden ser de duplicación de disco, interconexión, adaptadores y dispositivos de bloqueo que permiten un análisis rápido y sencillo de la evidencia.

Autopsy

Es una interfaz gráfica para análisis forense informático que utiliza herramientas de línea de comandos, esto permite a los investigadores realizar auditorías forenses no intrusivas de los sistemas bajo investigación, puede escanear unidades y sistemas de archivos de Windows y UNIX (NTFS, FAT, UFS1/2, Ext2/3). A continuación, se muestra una descripción de la herramienta. (GUZMÁN, 2023)

Características:

- Compatible con discos de grabación y teléfonos inteligentes.
- Habilita búsqueda de hash MD5.
- Está basado en código fuente abierto para que los usuarios puedan contribuir a su desarrollo.
- Permite la colaboración multiusuario al permitir que se analicen múltiples versiones de datos simultáneamente y se generen en un solo informe cuando se complete.

- Las etiquetas se pueden utilizar para identificar evidencia preservada de casos pasados que pueden volverse relevantes o relevantes para el caso actual.

Ventajas:

- Le permite utilizar palabras clave para realizar búsquedas de forma más eficaces.
- Recuperar datos de parte de ellos.
- Proporciona una interfaz gráfica de usuario.
- Le permite agregar módulos para agregar o automatizar funciones.
- Compatible con Windows, Mac OS y Linux.

Desventajas:

- No tiene una versión portátil.
- Se requiere un examen forense preliminar.
- La interfaz de usuario puede ser compleja.
- Se requieren conocimientos en el campo del disco duro.

Osforensics

OSForensics es una herramienta desarrollada por Passmark que se utiliza en forense digital, porque permite encontrar información visible, oculta o eliminada del análisis informático, la herramienta es muy fácil de usar y permite secuenciar la extracción de datos según sea necesario. investigador. El análisis de datos funciona a través de 3 fases que permiten desarrollarlo adecuadamente. (Villacrese, Chóez, & Figueroa, 2021)

- **Descubrimiento:** Puede descifrar contraseñas, extraer archivos y recuperar elementos eliminados de varios sistemas de archivos: Windows, Mac y Linux.
- **Identificación:** Todos los archivos se analizan y permiten crear una línea de tiempo.
- **Administración:** Permite la organización de la evidencia en una secuencia que abarca datos forenses.

Ventajas:

- Informes cifrados en PDF
- Soporte para OCR en Windows 10
- Incluye la última versión de VolatilityWorkbench y compatibilidad con Mac y Linux.
- Recuperación de clave Bitlocker.
- Función de copia de seguridad Búsqueda automática avanzada.
- Extraer vídeos MP4 de sitios web como YouTube.

MARCO METODOLOGICO

El presente caso de estudio se centra en la identificación de herramientas de análisis forense, la metodología propuesta incluye una revisión de la literatura, se utilizará un enfoque cualitativo para obtener una comprensión integral a través de entrevistas con expertos, con el objetivo de brindar una visión integral e información completa en la investigación de delitos informáticos.

Revisión de la literatura

La tabla presenta un resumen de la búsqueda literaria relacionada sobre la utilización de las herramientas forenses en la actualidad la cual, destacando investigaciones, caso de estudios y revistas sobre la identificación de las herramientas de análisis forense.

Tabla 1 Búsqueda literaria de las herramientas forenses

Fuente	**Enfoque Principal**	**Hallazgos claves**
Carrara, M., & Conti, G. (2020). A Comparative Analysis of Open-Source Digital Forensics Tools.	Herramienta Autopsy,Osforensic, EnCase,Ftk.	El estudio comparó las funcionalidades, rendimiento y facilidad de uso de diferentes herramientas de código abierto.
Granados Muñoz, R. (2020). Theoretical review of methodological tools applied in criminological research.	Herramientas aplicadas en la investigación criminológica	Resumen de diversas herramientas y metodologías utilizadas en investigación criminológica.
Cardozo, M. (2024). Aplicación de herramientas forenses en la recopilación y análisis de evidencia digita.	Aplicación de herramientas forenses	El análisis forense es clave en la lucha contra el cibercrimen, FTK y Autopsy son esenciales para la investigación forense.
Barrios Adrián. (2023). Herramientas de análisis forense digital manual de buenas prácticas	Herramientas de análisis forense digital.	Establecer técnicas y herramientas para obtener copias forenses sin alterar el original.
Hidalgo I, Hidalgo B, Pucuna S, Hidalgo Diego, Ola Jessica. (2020). Evidencia digital en la investigación forense informática	EnCase Forensic, FTK	Estas herramientas permiten a los investigadores forenses recolectar, examinar y documentar de manera exhaustiva la evidencia digital, facilitando la resolución de casos y la administración de justicia
Bebalcazar Nelly, Olmedo Byron, Hidalgo Mesa. (2024). Informática Forense	Caine	Proporcionar una distribución forense completa y gratuita, diseñada para realizar investigaciones informáticas forenses de manera eficiente y reproducible.

Parra Beatriz. (2023), Forensia Digital	Herramientas Autopsy, Encase, OSForensic	Permite obtener evidencia crucial en casos de ciberacoso, extorsión y otros delitos donde la comunicación digital es fundamental.
Smith & Johnson. (2022) Evaluation of Modern Digital Forensic Tools	Revisión y evaluación de las herramientas forenses	Las herramientas basadas en inteligencia artificial mejoran notablemente la precisión en la detección de cibercrímenes.
Brown et al. (2023) Standardizing Digital Forensic Tools: A Comparative Study	Clasificación y evaluación de herramientas forenses	La estandarización de herramientas forenses reduce las discrepancias en los resultados de los análisis.

La tabla comparativa destaca la importancia de las herramientas forenses digitales en la investigación criminal y el análisis forense, tanto de código abierto como comerciales, para la recolección y análisis de evidencia digital. Las investigaciones enfatizan la necesidad de metodologías adecuadas y buenas prácticas para maximizar su eficacia, estas herramientas son cruciales para abordar el cibercrimen y apoyar la justicia, subrayando la importancia de seguir evaluándolas y mejorándolas para satisfacer las crecientes demandas en el campo forense.

Se realizo una revisión exhaustiva de la literatura con lo cual se pudo identificar las herramientas de análisis forense más utilizadas actualmente y se procedió a la elaboración de la tabla.

Tabla 2 Características principales herramientas forenses

Herramienta	Plataforma	Tipo de archivo	Formato de imagen	Interfaz	Costo	Funcionalidades destacadas
Autopsy	Multiplataforma	Amplia variedad	E01, AFF, RAW	Gráfica	Gratuita	Análisis de discos duros, búsqueda de archivos
OSForensic	Windows	NTFS, FAT, EXT2/3/4	E01, AFF, RAW	Gráfica	Comercial	Análisis en profundidad, personalización avanzada
The Sleuth Kit	Multiplataforma	Amplia variedad	E01, AFF, RAW	Línea de comandos	Gratuita	Gran flexibilidad, bajo nivel
Digital Forensic Framework	Multiplataforma	Amplia variedad	Depende de los módulos	Gráfica	Gratuita	Extensible, modular

Magnet AXIOM	Multiplataforma	Amplia variedad	Varios	Gráfica	Comercial	Análisis completo de dispositivos móviles, nube
CAINE	Linux	Amplia variedad	Varios	Gráfica	Gratuita	Sistema operativo forense completo
Helix3	Nube	Amplia variedad	Varios	Web	Comercial	Análisis en la nube, colaboración

En la comparación de herramientas forenses digitales, Autopsy y OSForensics destacan como opciones robustas y accesibles, Autopsy, gratuita y multiplataforma, ofrece una amplia variedad de análisis de discos duros y búsquedas de archivos con numerosos complementos. Su interfaz gráfica la hace accesible para usuarios de distintos niveles de experiencia, siendo una excelente opción integral sin costos asociados, OSForensics también es una herramienta potente, conocida por su rapidez y eficiencia en la adquisición e indexación de datos.

La tabla presenta un resumen sobre las pruebas de rendimiento de las herramientas seleccionadas Autopsy y OSForensic.

Tabla 3 Pruebas de rendimiento de Autopsy y OSForensic

Característica	**Autopsy**	**OSFORENSIC**	**Observaciones**
Velocidad de adquisición	Depende del hardware y tamaño del disco	Depende del hardware y tamaño del disco	Generalmente similar, puede variar según la configuración.
Velocidad de indexación	Rápida, indexación incremental	Rápida, indexación incremental	Ambas ofrecen indexación rápida, lo que permite búsquedas eficientes.
Velocidad de búsqueda	Muy rápida, gracias a la base de datos SQLite	Rápida, pero puede ser más lenta en grandes conjuntos de datos	Autopsy suele destacar en búsquedas complejas.
Uso de RAM	Moderado a alto, dependiendo de la complejidad del caso	Moderado, optimizada para sistemas con menos RAM	OSFORENSIC puede ser más ligera en entornos con recursos limitados.
Uso de CPU	Moderado a alto, durante la indexación y búsquedas intensivas	Moderado, bien optimizada para multi-core	Ambas pueden utilizar la CPU de manera eficiente.
Escalabilidad	Buena, puede manejar grandes imágenes de disco	Buena, diseñada para manejar grandes volúmenes de datos	Ambas escalan bien, aunque Autopsy puede tener una ligera ventaja en casos extremadamente grandes.
Análisis soportados	Amplio rango, desde análisis de archivos hasta análisis de red	Amplio rango, con énfasis en análisis de	Autopsy ofrece una mayor variedad de módulos y plugins.

		sistemas operativos Windows	
Visualizaciones	Excelentes, con timeline interactivo y visualizaciones de archivos	Buenas, con timeline y visualizaciones básicas	Autopsy ofrece visualizaciones más sofisticadas y personalizables.
Reportes	Personalizables, en formato HTML y PDF	Personalizables, en formato HTML	Ambos generan reportes detallados, pero Autopsy ofrece más opciones de personalización.
Facilidad de uso	Interfaz gráfica intuitiva, bien documentada	Interfaz gráfica sencilla, pero puede requerir más conocimientos técnicos	Autopsy es generalmente considerada más fácil de usar.
Soporte técnico	Comunidad activa, documentación extensa	Comunidad más pequeña, documentación menos detallada	Autopsy cuenta con un mayor soporte comunitario.
Costo	Gratuita (open source)	Gratuita (open source)	Ambas son herramientas gratuitas y de código abierto.

La tabla compara Autopsy y OSForensics, destacando la velocidad de adquisición e indexación rápida en ambas, con Autopsy sobresaliendo en la velocidad de búsqueda y uso eficiente de RAM. Autopsia escala mejor en análisis intensivos, ofrece más módulos variados y análisis atractivos, y permite informes personalizables en HTML y PDF. Además, es más intuitivo, fácil de usar y tiene un sólido soporte técnico comunitario,se sugiere considerar estas diferencias al elegir la herramienta adecuada.

La tabla presenta un resumen sobre los diferentes casos prácticos de las herramientas seleccionadas Autopsy y OSForensic.

Tabla 4 Caso práctico de las herramientas Autopsy Y OSForensic

Caso Práctico	Autopsy	OSForensics	Observaciones
Investigación de un dispositivo móvil robado	Excelente para analizar imágenes de dispositivos móviles. Puede extraer datos de aplicaciones, mensajes, historial de llamadas, etc.	Puede ser utilizado, pero Autopsy suele ser más especializado en este tipo de análisis.	Autopsy ofrece una mayor profundidad en el análisis de dispositivos móviles.
Análisis de un sistema comprometido por ransomware	Puede identificar archivos cifrados, cambios en el registro y actividad de red.	Puede realizar un análisis similar, pero Autopsy puede ofrecer más opciones de filtrado y búsqueda.	Ambos pueden ser utilizados, pero la elección dependerá de las preferencias del investigador.
Investigación de fraude interno	Análisis de correos electrónicos, búsqueda de palabras clave, reconstrucción de cronologías.	Análisis de registros de acceso a archivos, detección de anomalías en el uso de recursos.	Ambas herramientas fueron útiles, pero OSForensic proporcionó una mayor profundidad

			en el análisis de registros del sistema.
Análisis de un sistema infectado por malware	Puede identificar archivos maliciosos, analizar el comportamiento del malware y reconstruir la línea de tiempo de la infección.	Puede realizar un análisis similar, pero Autopsy puede ofrecer más opciones de análisis de registro.	Ambos pueden ser utilizados, pero la elección dependerá de la complejidad del malware.

La tabla compara Autopsy y OSForensics en análisis forense digital, Autopsy sobresale en el análisis de dispositivos móviles robados, ransomware, fraude interno y malware, ofreciendo opciones avanzadas y especializadas. OSForensics también es útil, especialmente para búsquedas rápidas y análisis de artefactos específicos, aunque puede ser menos detallado. La elección entre ambas herramientas dependerá de la complejidad del caso y las preferencias del investigador, con utopsy siendo más robusta para investigaciones complejas.

La tabla presenta un resumen sobre benchmarking en las herramientas seleccionadas Autopsy y OSForensic.

Tabla 5 Benchmarking de las herramientas Autopsy Y OSForensic

Característica	Autopsy	OSFORENSIC	Observaciones
Velocidad de Adquisición	Depende del hardware y tamaño del disco. Generalmente rápida, pero puede variar según la configuración.	Similar a Autopsy. Depende del hardware y configuración.	Considerar el tamaño del disco, tipo de sistema de archivos y hardware utilizado.
Velocidad de Indexación	Rápida, indexación incremental. Excelente para grandes imágenes.	Rápida. Puede variar según la complejidad de la imagen.	Evaluar el tiempo de indexación en imágenes de diferentes tamaños y complejidad.
Velocidad de Búsqueda	Muy rápida, gracias a la base de datos SQLite. Permite búsquedas complejas.	Rápida, pero puede ser más lenta en búsquedas muy complejas.	Comparar el tiempo de respuesta en diferentes tipos de búsquedas (por ejemplo, por fecha, extensión, contenido).
Uso de Recursos	Moderado a alto, dependiendo de la complejidad del caso.	Moderado. Optimizada para sistemas con menos RAM.	Evaluar el consumo de CPU y RAM en diferentes fases del análisis.
Escalabilidad	Excelente. Diseñada para manejar grandes imágenes y casos complejos.	Buena. Puede manejar imágenes de gran tamaño, pero puede tener limitaciones en casos extremadamente grandes.	Evaluar el rendimiento con imágenes de varios terabytes.
Análisis Soportados	Amplio rango. Desde análisis de archivos hasta análisis de red.	Amplio rango, con énfasis en sistemas Windows.	Comparar la disponibilidad de módulos y plugins para diferentes tipos de análisis.

Visualizaciones	Excelentes. Timeline interactivo, visualizaciones de archivos y redes.	Buenas. Timeline y visualizaciones básicas.	Evaluar la calidad y cantidad de visualizaciones disponibles para cada tipo de evidencia.
Reportes	Personalizables. Formato HTML y PDF.	Personalizables. Formato HTML.	Comparar la flexibilidad y detalle de los reportes generados.
Facilidad de Uso	Interfaz gráfica intuitiva. Bien documentada.	Interfaz gráfica sencilla. Puede requerir más conocimientos técnicos.	Evaluar la curva de aprendizaje y la documentación disponible.
Costo	Gratuita (open source)	Gratuita (open source)	Ambas son herramientas gratuitas y de código abierto.

A continuación, se presentan en una tabla los Casos reales de delitos informáticos.

Tabla 6 Casos reales de delitos informaticos

Escenario	**Herramientas Utilizadas**	**Acciones Realizadas**	**Resultados Claves**	**link**
Fuga de datos (2022)	Autopsy, The Sleuth Kit	Análisis de imágenes de disco de servidores comprometidos, búsqueda de patrones de acceso no autorizado, recuperación de archivos borrados, análisis de logs de sistema.	Identificación del punto de entrada del atacante, determinación del alcance del compromiso, recuperación de datos sensibles.	https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/11397/CASO%20FUGA%20DE%20DATOS%20SEGUNDA%20PARTE.pdf?sequence=5&isAllowed=y
Caso DFRWS 2008 Rodeo por daños a los sistemas informáticos (2022)	Autopsy, CAINE	Análisis de logs de sistema, análisis de archivos de configuración, búsqueda de conexiones inusuales	Identificación del punto de entrada, determinación del método de intrusión	https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/6041/AdrianBarrios_2023.pdf?sequence=5&isAllowed=y
Ataque ransomware a un hospital (2021)	OSForensic, FTK	Análisis en profundidad de sistemas infectados, recuperación de archivos cifrados, análisis de redes para identificar la propagación del ransomware, búsqueda de vectores de ataque.	Identificación de la variante de ransomware, recuperación parcial o total de datos, determinación del impacto en las operaciones del hospital.	https://prcrepository.org/xmlui/bitstream/handle/20.500.12475/1251/AN%C3%81LISIS%20DE%20CASO%20%20UNITED%20STATES%20VS.%20ZHU%20HUA%20AND%20ZHANG%20SHILONG.pdf?sequence=1

Análisis de fraude en la bolsa de valores en Estados Unidos (2023)	Autopsy, The Sleuth Kit	Análisis de transacciones financieras, búsqueda de patrones de fraude, análisis de logs de sistemas bancarios, recuperación de correos electrónicos fraudulentos.	Identificación de cuentas comprometidas, seguimiento del flujo de fondos, recuperación de evidencia para procesos legales.	https://prcrepository.org/xmlui/bitstream/handle/20.500.12475/1853/Proyecto%20Final%20CPena.pdf?sequence=1

La tabla resume varios escenarios de cibercrimen y los enfoques metodológicos para abordarlos, destacando herramientas como Autopsy, The Sleuth Kit, Caine y OSForensics, estas herramientas son esenciales para analizar dispositivos comprometidos, rastrear actividades maliciosas y mitigar el impacto de los ciberataques. Los resultados subrayan la efectividad del análisis forense digital en la identificación de perpetradores y la protección de datos confidenciales, en última instancia, estas metodologías fortalecen las estrategias de prevención y seguridad digital.

Se realizó la entrevista a los Profesionales que laboran en la Universidad Técnica de Babahoyo, la cual adjuntare en la sección de anexos.

ENTREVISTA

Universidad Técnica de Babahoyo

Facultad de Administración, Finanzas e Informática

Análisis de las herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos

Nombre del Profesional: ING. CARLOS SOTO

Lugar de Trabajo: UTB-FAFI

Cargo: Docente de la Faculta de Administración, Finanzas e Informática

Objetivo: Obtenga perspectivas y experiencias prácticas sobre la eficacia y aplicabilidad de las herramientas de análisis forense digital, Autopsia y Osforensic, en la investigación de delitos informáticos.

1. **¿Conoce usted la herramienta Autopsy o Osforensic?**

   Si

2. **¿Qué tan eficaz ha sido Autopsy en la recolección y análisis de evidencia digital en comparación con otras herramientas que ha utilizado?**

Su eficiencia ha sido del 30% en relacion a otras herramientas

3. **¿Podría describir algún caso específico en el que Osforensic haya demostrado ser particularmente eficiente en la resolución de un delito informático?**

En la recuperación de información en un arreglo de un Disco Dms 1+0 en un sistema operativo Windows del 2019.

4. **¿Cuánto tiempo le toma generalmente completar un análisis forense con Autopsy y cómo se compara esto con otros softwares de análisis forense que ha utilizado?**

18 horas vs otras herramientas en base del tipo de daño.

5. **Si tuviera que elegir una sola herramienta para un análisis forense, ¿optaría por Autopsy u Osforensic? ¿Por qué?**

Si en un 40% no he logrado obtener un poco de éxito

6. **¿Qué mejoras considera necesarias en las herramientas forenses actuales?**

Análisis y extracción heurístico de datos en bajo nivel.

7. **¿Cuáles son las herramientas de análisis forense digital que utilizas con mayor frecuencia y cómo evalúas su eficacia?**

Son varias Recuva, Get Databack, Hd learnnity

8. **¿Cuáles son las características esenciales que deben tener las herramientas de análisis forense?**

Mayor velocidad y mejorar el extremo de ADM.

9. **¿Cómo manejan las herramientas de análisis forense la preservación de la integridad de la evidencia?**

La mayoría toman un control basado en la ISO 9014-27001

10. **¿Cuál es su experiencia con la capacidad de las herramientas forenses para detectar y analizar evidencias en sistemas de almacenamiento no convencionales o en la nube?**

Dependiendo del tipo de datos y del tipo de daño, las experiencias han logrado su satisfacción.

ENTREVISTA

Universidad Técnica de Babahoyo

Facultad de Administración, Finanzas e Informática

Análisis de las herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos

Nombre del Profesional: ING. RAUL RAMOS

Lugar de Trabajo: UTB-FAFI

Cargo: Director de la Escuela de Tecnologías de la Información y la Comunicación

Objetivo: Obtenga perspectivas y experiencias prácticas sobre la eficacia y aplicabilidad de las herramientas de análisis forense digital, Autopsia y Osforensic, en la investigación de delitos informáticos.

1. **¿Conoce usted la herramienta Autopsy o Osforensic?**

   Si

2. **¿Qué tan eficaz ha sido Autopsy en la recolección y análisis de evidencia digital en comparación con otras herramientas que ha utilizado?**

Autopsy es muy eficaz en recolección y análisis de evidencia digital, superando a muchas otras herramientas.

3. **¿Podría describir algún caso específico en el que Osforensic haya demostrado ser particularmente eficiente en la resolución de un delito informático?** OSForensics resolvió un delito rápidamente al recuperar archivos eliminados de un servidor.

4. **¿Cuánto tiempo le toma generalmente completar un análisis forense con Autopsy y cómo se compara esto con otros softwares de análisis forense que ha utilizado?** La autopsia toma de 4 a 6 horas para un análisis forense, siendo más rápido que otros softwares.

5. **Si tuviera que elegir una sola herramienta para un análisis forense, ¿optaría por Autopsy u Osforensic? ¿Por qué?** Elegiría Autopsy por su robustez y constante actualización.

6. **¿Qué mejoras considera necesarias en las herramientas forenses actuales?**

Mejoras en automatización y machine learning, integración de herramientas, análisis en tiempo real, manejo de big data, usabilidad, aseguramiento de la cadena de custodia, colaboración y compartición de información, y seguridad.

7. ¿Cuáles son las herramientas de análisis forense digital que utilizas con mayor frecuencia y cómo evalúas su eficacia?

Utilizo EnCase, FTK, Autopsy/Sleuth Kit y X1 Social Discovery. Evalúo su eficacia basándome en precisión, velocidad, facilidad de uso, documentación, flexibilidad y seguridad.

8. ¿Cuáles son las características esenciales que deben tener las herramientas de análisis forense? Las características esenciales abarcan precisión y confiabilidad, capacidad para manejar grandes volúmenes de datos, una interfaz de usuario intuitiva, compatibilidad y flexibilidad, documentación y generación de informes detallados, automatización y análisis avanzado, soporte técnico y actualizaciones continuas, así como robustas de seguridad.

9. ¿Cómo manejan las herramientas de análisis forense la preservación de la integridad de la evidencia? Mediante hashing, mantenimiento de la cadena de custodia, acceso controlado, modos de solo lectura, creación de imágenes forenses, certificación y validación del software, trazabilidad completa, y copias de seguridad y redundancia.

10. ¿Cuál es su experiencia con la capacidad de las herramientas forenses para detectar y analizar evidencias en sistemas de almacenamiento no convencionales o en la nube? Utilizo herramientas especializadas como X1 Social Discovery y Magnet AXIOM Cloud, y técnicas como Volatility, chip-off y JTAG. Los desafíos incluyen cifrado y diversidad de formatos, manejados a través de APIs forenses, instantáneas, SIEM, y análisis de logs y adquisiciones remotas.

Este resumen sintetiza las respuestas clave a cada una de tus preguntas sobre herramientas forenses y sus capacidades.

ENTREVISTA

Universidad Técnica de Babahoyo

Facultad de Administración, Finanzas e Informática

Análisis de las herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos

Nombre del Profesional: ING. OMAR MONTECE

Lugar de Trabajo: UTB-FAFI

Cargo: Docente de la Faculta de Administración, Finanzas e Informática

Objetivo: Obtenga perspectivas y experiencias prácticas sobre la eficacia y aplicabilidad de las herramientas de análisis forense digital, Autopsia y Osforensic, en la investigación de delitos informáticos.

1. **¿Conoce usted la herramienta Autopsy o Osforensic?**

Si

2. **¿Qué tan eficaz ha sido Autopsy en la recolección y análisis de evidencia digital en comparación con otras herramientas que ha utilizado?**

   Autopsy es eficaz y fácil de usar, pero algunas herramientas comerciales ofrecen características más avanzadas.

3. **¿Podría describir algún caso específico en el que Osforensic haya demostrado ser particularmente eficiente en la resolución de un delito**

informático? Osforensic facilitó un caso de intrusión, identificando rápidamente los puntos de acceso y las actividades del atacante.

4. **¿Cuánto tiempo le toma generalmente completar un análisis forense con Autopsy y cómo se compara esto con otros softwares de análisis forense que ha utilizado?** Depende del caso, pero generalmente unas horas a varios días, similar a otras herramientas forenses.

5. **Si tuviera que elegir una sola herramienta para un análisis forense, ¿optaría por Autopsy u Osforensic? ¿Por qué?** Elegiría Osforensic por sus capacidades avanzadas y mayor precisión en la recuperación y análisis de datos.

6. **¿Qué mejoras considera necesarias en las herramientas forenses actuales?**

Mejoras en velocidad, automatización de tareas y uso de IA para identificar patrones serían valiosas.

7. **¿Cuáles son las herramientas de análisis forense digital que utilizas con mayor frecuencia y cómo evalúas su eficacia?**

Utilizo Autopsy, Osforensic y EnCase, cada una eficaz en diferentes aspectos según las necesidades del caso.

8. **¿Cuáles son las características esenciales que deben tener las herramientas de análisis forense?**

Recuperación de datos eliminados, análisis de grandes volúmenes, preservación de evidencia y generación de informes detallados.

9. **¿Cómo manejan las herramientas de análisis forense la preservación de la integridad de la evidencia?** Usan técnicas de hash y creación de imágenes forenses para mantener la evidencia intacta y verificable.

10. **¿Cuál es su experiencia con la capacidad de las herramientas forenses para detectar y analizar evidencias en sistemas de almacenamiento no convencionales o en la nube?**

Herramientas como Osforensic y EnCase manejan bien la nube y almacenamiento no convencional, aunque requieren actualizaciones constantes para superar desafíos de acceso y seguridad.

ENTREVISTA

Universidad Técnica de Babahoyo

Facultad de Administración, Finanzas e Informática

Análisis de las herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos

Nombre del Profesional: ING. ALEXIS CEDEÑO

Lugar de Trabajo: UTB-FAFI

Cargo: Analista de Desarrollo de Proyectos Tecnológicos.

Objetivo: Obtenga perspectivas y experiencias prácticas sobre la eficacia y aplicabilidad de las herramientas de análisis forense digital, Autopsia y Osforensic, en la investigación de delitos informáticos.

1. **¿Conoce usted la herramienta Autopsy o Osforensic?**

   Si

2. **¿Qué tan eficaz ha sido Autopsy en la recolección y análisis de evidencia digital en comparación con otras herramientas que ha utilizado?**

Autopsy ha demostrado ser muy eficaz en la recolección y análisis de evidencias. manejando una variedad de formatos de archivo siendo accesible tanto para profesionales como para principiantes.

3. **¿Podría describir algún caso específico en el que Osforensic haya demostrado ser particularmente eficiente en la resolución de un delito informático?** Un caso específico podría ser una investigación de fraude corporativo en la que OSForensics fue utilizado para analizar grandes volúmenes de datos en múltiples dispositivos.

4. **¿Cuánto tiempo le toma generalmente completar un análisis forense con Autopsy y cómo se compara esto con otros softwares de análisis forense que ha utilizado?** El tiempo requerido para completar un análisis forense con Autopsy puede variar significativamente según el tamaño y la complejidad de los datos a analizar.

En promedio, un análisis de disco completo con Autopsy puede llevar desde unas pocas horas hasta varios días, dependiendo del caso.

5. **Si tuviera que elegir una sola herramienta para un análisis forense, ¿optaría por Autopsy u Osforensic? ¿Por qué?** Si el presupuesto es una limitación, Autopsy sería la opción preferida debido a su naturaleza de código abierto y sin costo. Sin embargo, si se requiere una herramienta con soporte técnico robusto y características avanzadas, OSForensics podría ser la mejor opción.

6. **¿Qué mejoras considera necesarias en las herramientas forenses actuales?**

Algunas mejoras necesarias en las herramientas forenses actuales incluyen:

- Mejor soporte para análisis de datos en la nube y sistemas de almacenamiento no convencionales.

- Integración más profunda con tecnologías de inteligencia artificial y aprendizaje automático para acelerar el análisis y la identificación de patrones sospechosos.

- Mejoras en la interfaz de usuario para facilitar el uso por parte de investigadores con diferentes niveles de experiencia.

- Mayor capacidad para manejar grandes volúmenes de datos y mejorar la velocidad de procesamiento.

- Herramientas más avanzadas para el análisis de dispositivos móviles y datos de aplicaciones.

7. ¿Cuáles son las herramientas de análisis forense digital que utilizas con mayor frecuencia y cómo evalúas su eficacia?

Las herramientas de análisis forense digital que se utilizan con mayor frecuencia incluyen:

- Autopsy: Eficaz y accesible para la mayoría de los casos.

- FTK (Forensic Toolkit): Potente y rápida, ideal para análisis de grandes volúmenes de datos.

- EnCase: Conocida por su robustez y soporte técnico, muy utilizada en entornos corporativos.

- OSForensics: Versátil y rica en características, excelente para análisis profundos y detallados.

- Cellebrite: Especializada en análisis de dispositivos móviles, altamente eficaz en este ámbito.

8. ¿Cuáles son las características esenciales que deben tener las herramientas de análisis forense? Preservación de la integridad de la evidencia

Capacidad de recuperación de datos

Análisis de múltiples formatos de archivo

Búsqueda y filtrado avanzados

Generación de informes

Soporte para análisis de dispositivos móviles y datos en la nube

9. ¿Cómo manejan las herramientas de análisis forense la preservación de la integridad de la evidencia? Uso de imágenes forenses: Crear copias exactas de los medios de almacenamiento para análisis, evitando trabajar directamente con los dispositivos originales.

Cálculo de hashes: Generar y verificar valores hash (MD5, SHA-1, SHA-256) para asegurar que los datos no se alteren durante el proceso.

Registro de auditoría: Mantener un registro detallado de todas las acciones realizadas durante el análisis para asegurar la trazabilidad.

10. ¿Cuál es su experiencia con la capacidad de las herramientas forenses para detectar y analizar evidencias en sistemas de almacenamiento no convencionales o en la nube? Las herramientas forenses están mejorando continuamente en la detección y análisis de evidencias en sistemas de almacenamiento no convencionales y en la nube. Sin embargo, el análisis de estos entornos aún presenta desafíos debido a la encriptación, la dispersión de datos y las jurisdicciones legales. La integración de análisis en la nube sigue siendo un área en evolución, y la capacidad para manejar estos tipos de datos se está convirtiendo en una característica crucial para las herramientas forenses modernas.

RESULTADO

El documento compara herramientas de análisis forense como OSForensic, FTK,Autopsy y CAINE, cada herramienda se especializa en diferentes aspectos del análisis, desde la presentación de informes hasta la recolección de datos, el estudio destaca la importancia de estandarizar las herramientas forenses para reducir discrepancias y mejorar la precisión en los resultados.

OSForensic es más eficiente en la identificación de cifrados, entornos con recursos limitados y análisis de metadatos, su sencilla interfaz también facilita el uso para análisis rápidos en grandes volúmenes de datos. Por el contrario, Autopsy es conocida por su rapidez en la búsqueda y la variedad de visualizaciones que ofrece, es eficiente especialmente en el análisis detallado de dispositivos e incidentes de ransomware, además de contar con documentación extensa y una comunidad activa.

En casos prácticos, en incidentes de ransomware, Autopsy resulta ser una herramienta completa para analizar patrones de cifrado, mientras que OSForensic es eficaz para la identificación inicial de archivos cifrados. Las investigaciones de fraude electrónico, Autopsy permite un análisis más detallado de correos electrónicos y comunicaciones, mientras OSForensic facilita la rápida búsqueda de palabras clave en grandes conjuntos de datos. Para el análisis de dispositivos, Autopsy ofrece soporte para una variedad amplia de dispositivos y sistemas operativos, esencial para investigaciones complejas, mientras OSForensic es adecuado por su interfaz accesible para análisis básicos.

El estudio también incluyó análisis de ciberseguridad utilizando herramientas como Autopsy, OSForensic, estableciendo su capacidad para identificar ataques, métodos de

intrusión y variantes de ransomware en diversos escenarios. Al utilizar Autopsy para examinar un disco local, como una unidad USB denominada VTOYEFI, comenzó seleccionando el dispositivo a analizar, este paso fue crucial para asegurar la evaluación y restauración que se realicen en la unidad correcta, evitando errores que podrían haber alterado datos en otros dispositivos, escoger el dispositivo correcto fue fundamental para mantener la integridad del proceso y recuperar los datos.

Después de seleccionar el dispositivo, se estableció las opciones de restauración según las necesidades específicas, ajustando el proceso de recuperación, para enfrentar diferentes tipos de pérdida de datos y garantizar una restauración efectiva. Luego, el programa procedió a examinar y restaurar la información, analizando detalladamente el contenido de la unidad para identificar y recuperar datos dañados o perdidos, se presentó la información recuperada y se ofreció la opción de generar un informe para analizar los datos de manera profesional y documentar.

El análisis de un USB con OSForensics comienza con la creación de un nuevo caso, que permite registrar la evaluación específica del dispositivo, esta etapa es crucial para mantener la organización y documentación sistemática de toda la información junto con actividades relacionadas en el USB garantizando un análisis efectivo.

Se seleccionó la opción de indexación, seleccionando todas las opciones disponibles para un examen exhaustivo del USB, esta fase organiza y clasifica los datos, facilitando su búsqueda y revisión. Posteriormente, se puede buscar información específica por nombre. Finalmente, el programa genera un informe detallado del análisis, generando una documentada de los datos examinados y una visión completa

DISCUSION DE RESULTADOS

El análisis comparativo de herramientas de análisis forense digital revela varios hallazgos clave, Autopsy y OSForensic destacan significativamente en términos de velocidad, eficiencia y accesibilidad. Mientras Autopsy ofrece rapidez en la búsqueda y una variedad de visualizaciones, OSForensic muestra eficiencia en entornos con recursos limitados, ambos son gratuitos y de código abierto, lo que facilita su adopción por una amplia gama de usuarios.

En la comparación de casos prácticos, Autopsy es más versátil en investigaciones de ransomware, permitiendo identificar archivos cifrados y buscar claves de descifrado, OSForensic, por su parte, se destaca en la identificación inicial de archivos cifrados y en el análisis de metadatos, siendo ideal para recuperaciones rápidas, estas diferencias reflejan las fortalezas específicas de cada herramienta según el tipo de análisis requerido.

El análisis de fraudes electrónicos mostró que Autopsy permite una reconstrucción detallada de líneas de tiempo y análisis de comunicaciones sospechosas, por otro lado, OSForensic es más eficiente en la búsqueda de palabras clave y expresiones regulares en grandes volúmenes de datos, facilitando la identificación rápida de transacciones sospechosas, esta diferencia en enfoque proporciona a los investigadores diversas opciones para abordar distintos tipos de fraude.

En cuanto al análisis de dispositivos, a pesar de tener un soporte de dispositivos limitado, la interfaz de usuario de OSForensic es intuitiva y fácil de navegar, lo que la convierte en un recurso valioso para aquellos con poca experiencia, Autopsy soporta una amplia variedad de sistemas operativos, dispositivos, permitiendo el análisis detallado de datos, mensajes y registros de llamadas.

La investigación sobre seguridad informática que usan herramientas como CAINE, Autopsy Wireshark y FTK estas herramientas demostraron la capacidad de realizar análisis transacciones, registros, analizar variante de ransomware y identificar puntos de ataques, los resultados demuestran un conocimiento profundo de la ciencia forense, enfatiza la importancia de elegir las herramientas adecuadas en función del contexto y necesidades específicas.

CONCLUSIÓN

OSForensics y Autopsy son herramientas destacadas en la recolección de evidencias digitales para investigaciones forenses, Autopsy al ser multiplataforma, gratuito resalta por su amplia variedad de accesibilidad y funcionalidades para el usuario de diversos niveles de experiencia. La rapidez de búsqueda, interfaz intuitiva y el comunitario soporte técnico aumenta su nivel como herramienta privilegiada, OSForensics es conocida por su efectividad y velocidad en la obtención de datos es menos detallada.

Herramientas como Caine, OSForensisc y The SLeuth Kit son importantes para escanear dispositivos, reducir el riesgo de delitos cibernéticos y rastrear actividades maliciosas. Estas herramientas examinan y protegen eficazmente los datos confidenciales, las entrevistas con expertos de la Universidad Técnica de Babahoyo brindaron información útil sobre la evaluación y experiencia de uso de las herramientas, destacando la satisfacción de los usuarios según el tipo de datos y los daños resueltos.

La elección entre OSForensics y Autopsy se necesita examinar la dificultad de caso y prioridad del investigador, para investigaciones complejas Autopsy es más apropiada, por el contrario OSForensics es eficiente para exploraciones de dispositivos específicos y búsquedas rápidas, es importante adoptar metodologías y buenas prácticas para aumentar la eficiencia de las herramientas forenses, en el uso de estas herramientas es importante la actualización de conocimiento para afrontar desafíos de los delitos informáticos.

RECOMENDACIONES

Antes de escoger entre OSForensics y Autopsy evalúa la dificultad del caso que se está investigando, utiliza OSForensic para investigaciones rápidas y análisis específicos de dispositivos, elige Autopsy para búsquedas complejas que necesiten un análisis exhaustivo.

Mantenerse actualizados con formación continua sobre el empleo de herramientas forenses, la tecnología y técnicas de ciberseguridad progresan rápidamente por lo que es importante actualizar los conocimientos para abordar eficientemente los delitos informáticos.

Implementar metodologías y buenas prácticas indicadas durante el análisis forense, implica seguir procedimientos estándar y mantener una documentación rigurosa para asegurar la integridad y validez de las investigaciones.

No te limites solo por OSForensic y Autopsy, ten en cuenta el empleo de otras herramientas forenses como Caine o The Sleuth Kit para asegurar y perfeccionar el análisis de evaluaciones completas en los dispositivos y actividades maliciosas.

BIBLIOGRAFIA

Herrera, S., Figueroa, L., & Lara, C. (2020). *INFORMÁTICA FORENSE: MÉTODOS, HERRAMIENTAS Y TÉCNICAS.*

Hidalgo, I., Yasaca, S., & Hidalgo, B. (2019). *Evidencias Digitales en la Investigación Forense Informática.*

Rodrıguez, R. (2023). *Analisis forense.*

Romero, R. (1 de septiembre de 2022). Informática Forense y Seguridad en la Nube. Recuperado el 7 de julio de 2024, de http://redi.ufasta.edu.ar/jspui/bitstream/123456789/1017/1/Romero_IF_2022.pdf

Vargas, D., Quinatoa, D., & Vega, P. (2022). *Ciberseguridad.* Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.uide.edu.ec/bitstream/37000/5605/1/UIDE-Q-TMCSE-2022-3.pdf

Villacrese, C., Chóez, J., & Figueroa, V. (2021). APLICACIÓN INFORMÁTICA FORENSE.

Bermúdez , A., & Saravia , S. (2023). *Informática forense metadatos.* Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://proyectos.uls.edu.sv/wiki/images/5/56/ExifTool.pdf

Borja , B. (2022). *Análisis de delitos forenses con AutoPsy.* Recuperado el 8 de julio de 2024, de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ebuah.uah.es/dspace/bitstream/handle/10017/52510/TFG_Ordonez_Bello_2022.pdf?sequence=1&isAllowed=y

CARVAJAL , A. (23 de Febrero de 2024). Recuperado el 6 de julio de 2024, de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.upse.edu.ec/bitstream/46000/10934/1/UPSE-TTI-2024-0005.pdf

Donadello, B. (2019). *Ingenieria Forense.*

GUZMÁN, A. (2023). *IMPLEMENTACIÓN DE HERRAMIENTAS PARA LA EXTRACCIÓN* .

GUZMÁN, A. (2023). *IMPLEMENTACIÓN DE HERRAMIENTAS PARA LA EXTRACCIÓN DE EVIDENCIA DIGITAL.*

Hall, A. (2021). *Tipos de delitos informaticos*. Recuperado el 29 de junio de 2024, de https://www.forodeseguridad.com/artic/discipl/disc_4016.htm

Perez, J. (2019). *Delitos regulados en leyes penales especiales. Gaceta Jurídica.*

Robalino , A., Yanza , W., & Montoya, J. (2022). *Auditoría Informática.*

Rubio, J. (27 de Noviembre de 2022). Recuperado el 8 de julio de 2024, de https://peritoinformaticocolegiado.es/blog/peritaje-informatico-forense-con-autopsy/

Samaniego. (2021). *Fundamentos de seguridad informática.*

Seguridad . (23 de Diciembre de 2021). Tipos de delitos informáticos más frecuentes. *Seguridad 360*. Recuperado el 28 de junio de 2024, de https://revistaseguridad360.com/destacados/tipos-de-delitos-informaticos/

Sosa, M. (2023). *Evidencia digital Su importancia en la investigación.*

ANEXOS

ENTREVISTA

Universidad Técnica de Babahoyo

Facultad de Administración, Finanzas e Informática

Análisis de las herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos

Nombre del Profesional:

Lugar de Trabajo:

Cargo:

Objetivo: Obtenga perspectivas y experiencias prácticas sobre la eficacia y aplicabilidad de las herramientas de análisis forense digital, Autopsia y Osforensic, en la investigación de delitos informáticos.

1. **¿Conoce usted la herramienta Autopsy o Osforensic?**
2. **¿Qué tan eficaz ha sido Autopsy en la recolección y análisis de evidencia digital en comparación con otras herramientas que ha utilizado?**
3. **¿Podría describir algún caso específico en el que Osforensic haya demostrado ser particularmente eficiente en la resolución de un delito informático?**
4. **¿Cuánto tiempo le toma generalmente completar un análisis forense con Autopsy y cómo se compara esto con otros softwares de análisis forense que ha utilizado?**

5. **Si tuviera que elegir una sola herramienta para un análisis forense, ¿optaría por Autopsy u Osforensic? ¿Por qué?**

6. **¿Qué mejoras considera necesarias en las herramientas forenses actuales?**

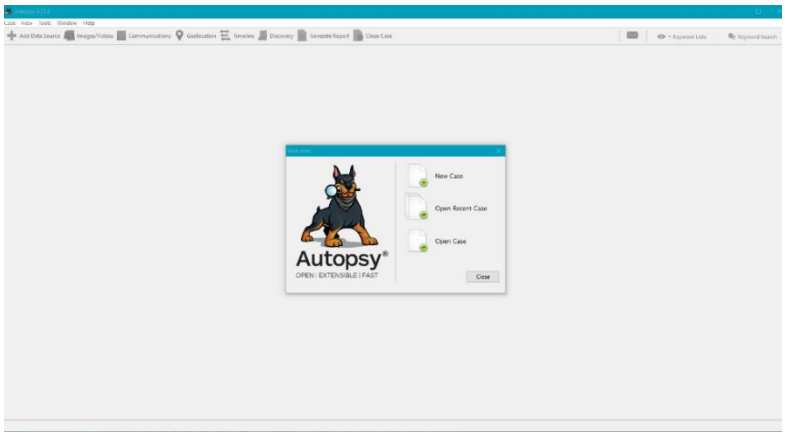
7. **¿Cuáles son las herramientas de análisis forense digital que utilizas con mayor frecuencia y cómo evalúas su eficacia?**

8. **¿Cuáles son las características esenciales que deben tener las herramientas de análisis forense?**

9. **¿Cómo manejan las herramientas de análisis forense la preservación de la integridad de la evidencia?**

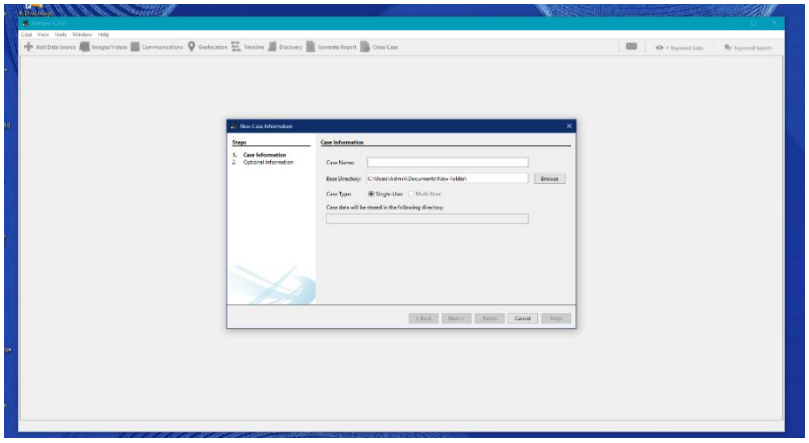
10. **¿Cuál es su experiencia con la capacidad de las herramientas forenses para detectar y analizar evidencias en sistemas de almacenamiento no convencionales o en la nube?**

AUTOPSY



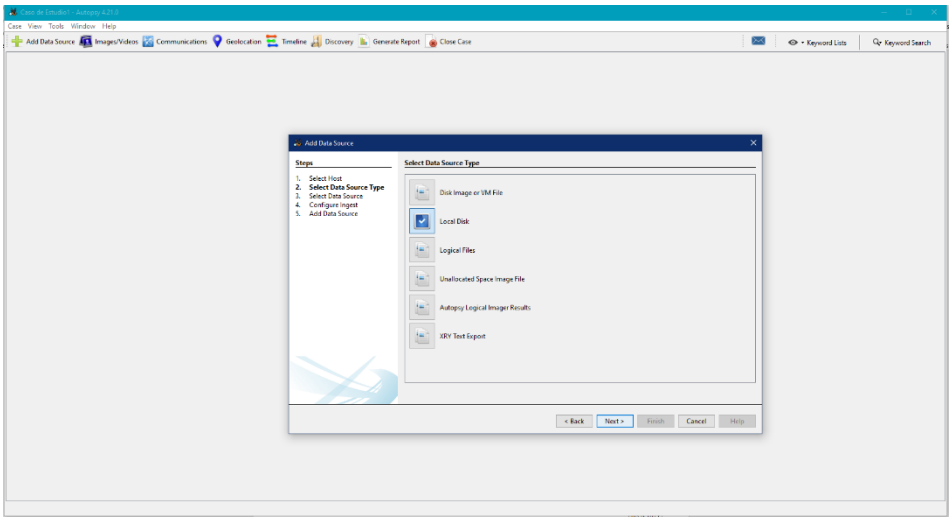
Anexo 1: Al iniciar el programa en el menú aparecerán tres opciones, y seleccionamos la primera opción es para crear un nuevo caso.

Fuente: Elaboración propia



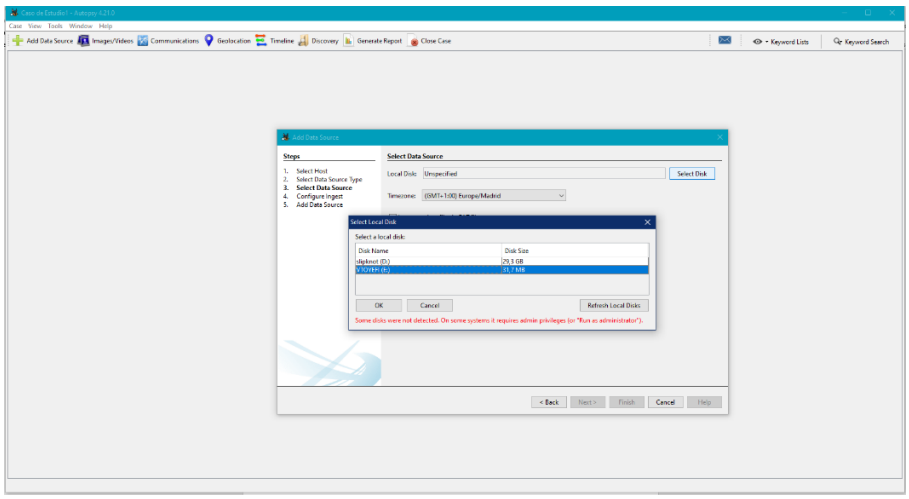
Anexo 2: Aquí damos nombre al caso, también seleccionamos el directorio al que deseamos guardar toda la información por último damos clic en finish.

Fuente: Elaboración propia



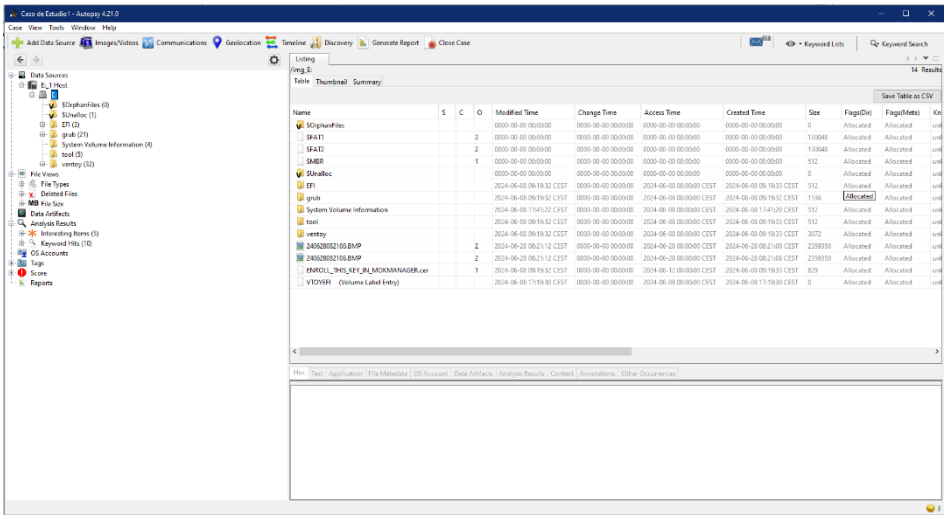
Anexo 3: El siguiente paso es seleccionar la opción que se va a examinar en este caso Local Disk.

Fuente: Elaboración propia



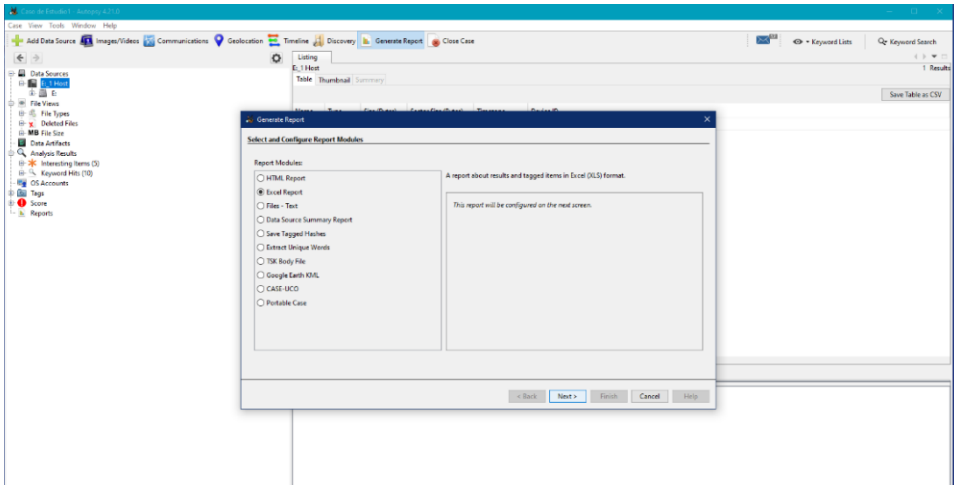
Anexo 4: Aqui nos aparecera los Local Disk disponibles, seleccionamos VTOYEFI que es una USB la que examinaremos por último clic en Ok y Next.

Fuente: Elaboración propia



Anexo 7: Aquí nos muestra toda la información que se recuperó.

Fuente: Elaboración propia

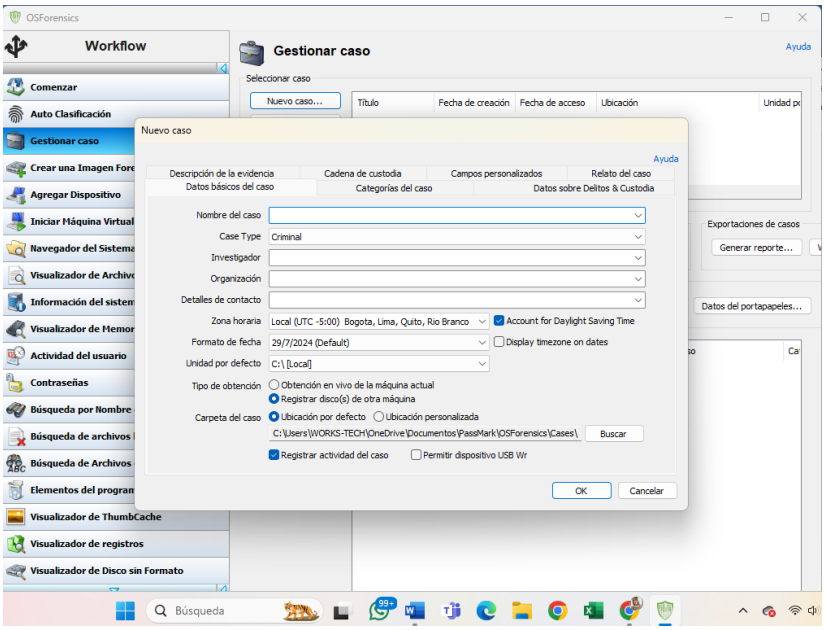


Anexo 8: En la barra del menú nos aparecen diferentes opciones para tener el reporte de lo restaurado damos clic en “Generate Report” y nos da las diferentes opciones de reporte.

Fuente: Elaboración propia

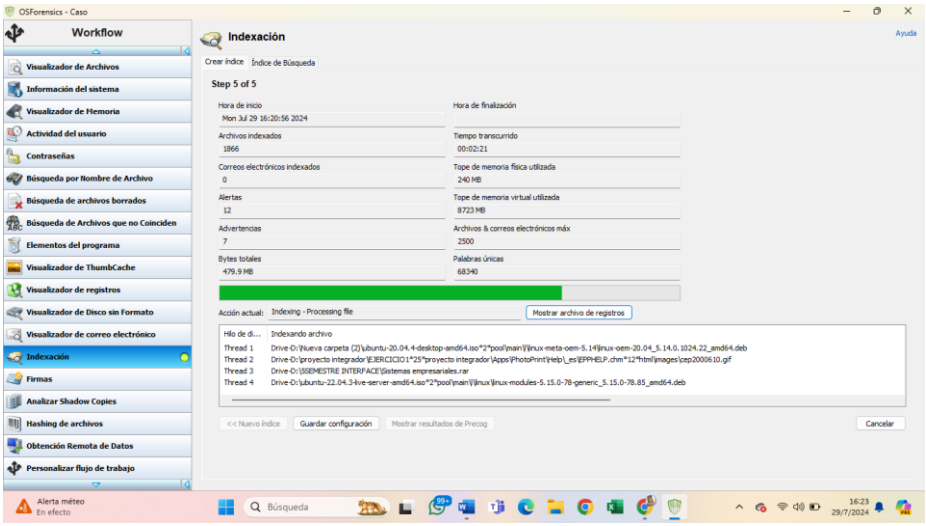
Anexo 1: Creamos un nuevo caso

Fuente: Elaboración propia



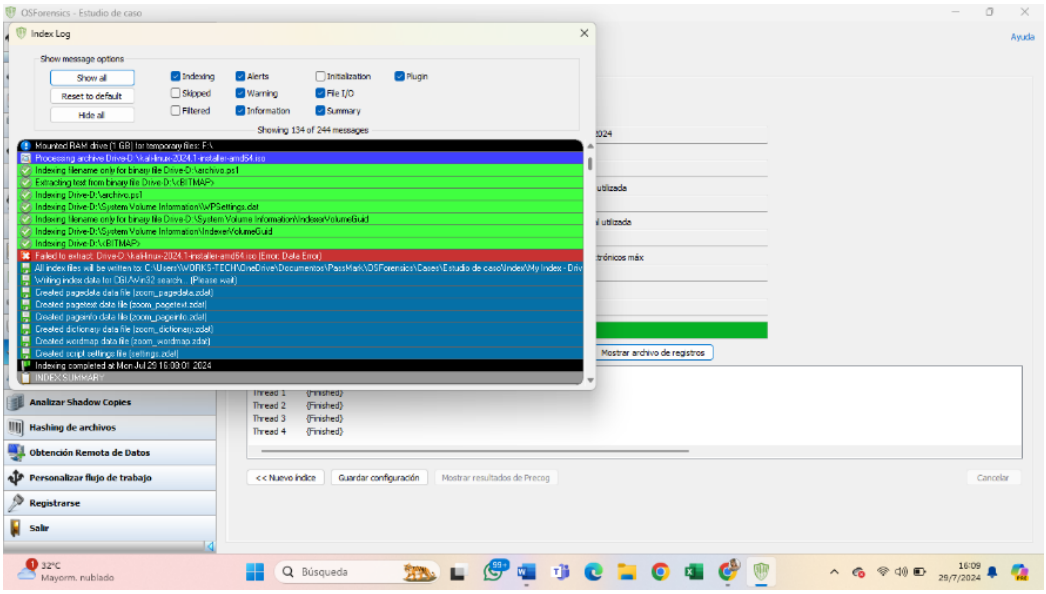
Anexo 2: Agregamos un nombre y clic en ok

Fuente: Elaboración propia



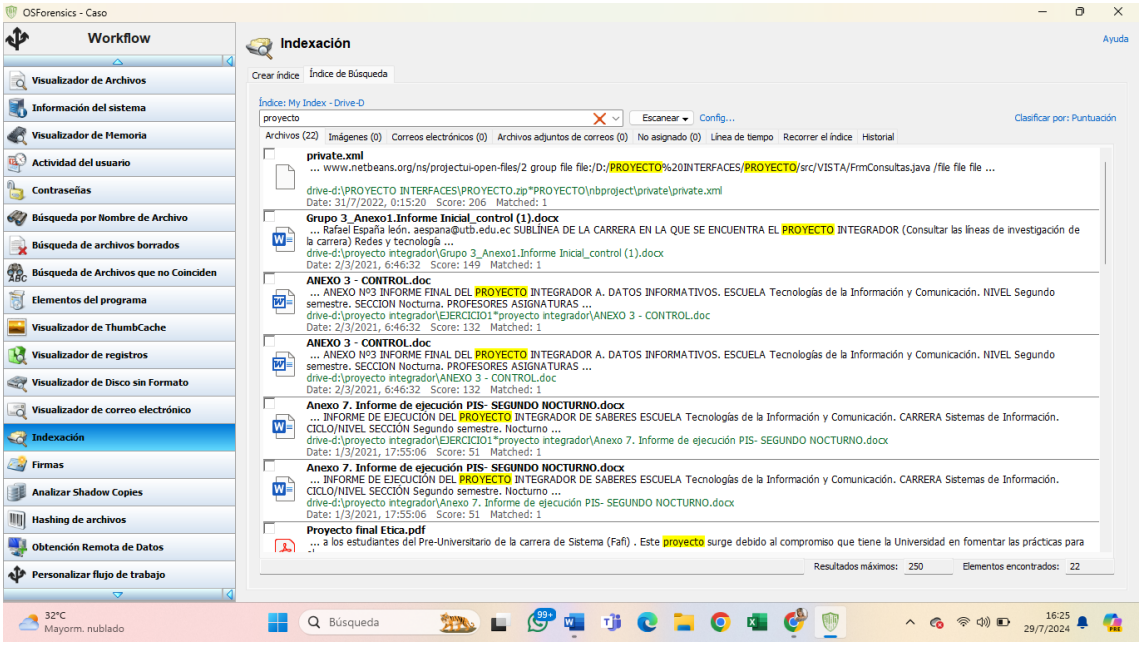
Anexo 5: Aquí comenzara analizar toda la información

Fuente: Elaboración propia



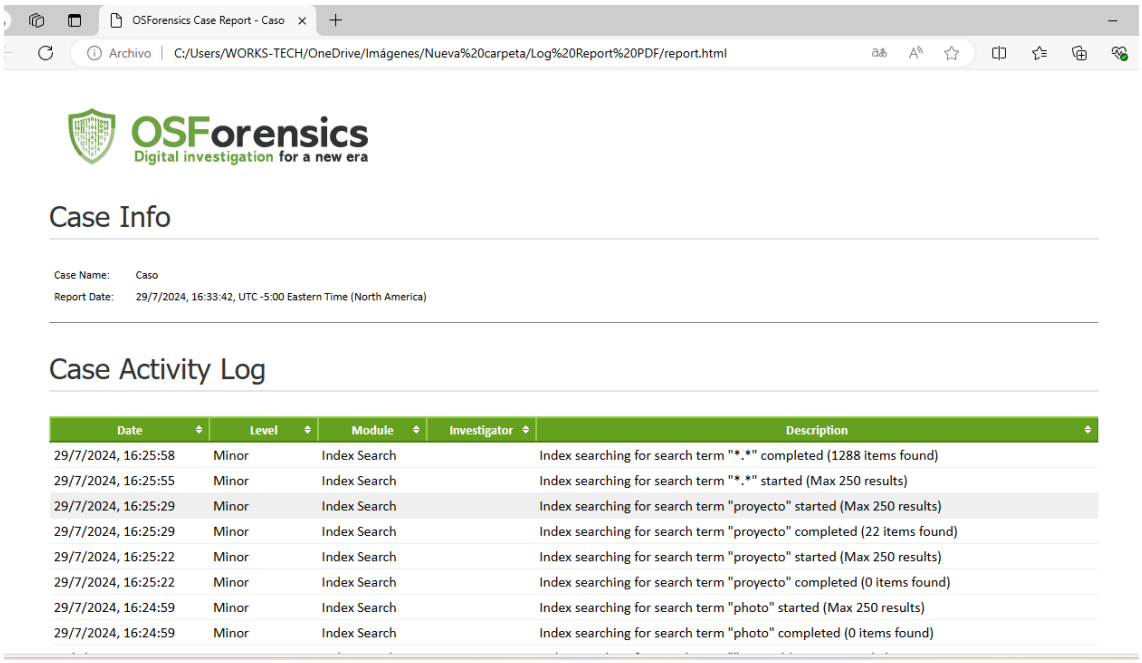
Anexo 6: En este apartado podemos observar lo encontrado del USB

Fuente: Elaboración propia



Anexo 7: Aquí se puede buscar por nombre

Fuente: Elaboración propia



Anexo 8: En este apartado está el reporte de lo analizado

Fuente: Elaboración propia