

Investigación Forense Digital: *análisis de evidencias electrónicas*

IBARRA - ECUADOR

Investigación Forense Digital:

análisis de evidencias electrónicas



ISBN: 978-9942-845-88-7

DOI: 10.53358/libfica/RVSA5180

MSc.

Lidice Haz López.

Universidad Estatal Península de Santa Elena (UPSE)

<https://orcid.org/0000-0003-1291-1875>

lhaz@upse.edu.ec

PhD.

Daisy Imbaquingo Esparza.

Universidad Técnica del Norte (UTN)

<https://orcid.org/0000-0002-6412-6257>

deimbaquingo@utn.edu.ec

MSc.

Jenny Garzón Balcázar.

Universidad Ecotec

<https://orcid.org/0000-0002-9473-902X>

jgarzonb@ecotec.edu.ec

MSc.

Oscar Ibarra Torres.

Universidad Técnica de Ambato (UTA)

<https://orcid.org/0000-0001-7589-2216>

oscar.ibarrat@info.unlp.edu.ar

DIAGRAMACIÓN Y DISEÑO

Lic. Marlon Dario Haro E.

Diseñador Gráfico

PRÓLOGO

En la actualidad, vivimos en un mundo donde la mayoría de los procesos manejan información digitalizada, lo que influye en casi todos los aspectos de nuestra vida diaria. Desde registrar una cita médica hasta realizar transacciones bancarias, estas actividades dejan una huella digital. Con el creciente uso de dispositivos electrónicos conectados a Internet, la información se generaliza y se masifica, dando lugar a delitos cibernéticos en los que la información se convierte en el bien más preciado. Por esta razón, es esencial investigar estos incidentes de manera oportuna y precisa.

El “Manual de Investigación Forense Digital: Análisis de evidencias electrónicas” nace como respuesta a la creciente demanda de conocimientos y habilidades especializadas en el campo de la investigación digital. Este manual se ha concebido como una guía integral tanto para investigadores y profesionales de la seguridad informática como para cualquier otra persona interesada en el análisis de evidencias electrónicas.

La investigación forense digital combina elementos de la tecnología de la información, la investigación criminal y el análisis de datos. A lo largo de este manual, se presentarán herramientas y métodos de recopilación y preservación de datos, con un enfoque paso a paso que facilita la comprensión y aplicación de estas técnicas en situaciones reales. Se pone especial énfasis en que la obtención de estos datos debe realizarse de manera meticulosa y ética, respetando la privacidad de las personas, lo cual es fundamental en este campo.

Finalmente, el objetivo principal de este manual es convertirse en una referencia indispensable para adentrarse en el fascinante y desafiante mundo de la investigación forense digital, donde el conocimiento de herramientas y procedimientos forenses resulta crucial para combatir los delitos digitales, que ya forman parte de nuestra realidad diaria.

ÍNDICE

TEMA 1: PROTOCOLO PARA LA INVESTIGACIÓN FORENSE DIGITAL		13	TEMA 3: FORENSE DIGITAL EN MEDIOS DE ALMACENAMIENTO		37
1.1	Investigación forense digital	13	3.1	Definición y tipos de discos duros	37
1.2	Importancia de cumplir con la cadena de custodia	14	3.2	Tipos de sistema de archivos	38
1.3	Proceso de detección, identificación y registro el incidente de ciberseguridad	15	3.3	Importancia de los metadatos en la investigación forense digital	39
1.4	Recolección de las evidencias digitales según su estado	16	3.4	Práctica 1. Extracción y análisis de evidencia contenida en discos duros	40
1.5	Procedimiento para asegurar la integridad física y lógica de la evidencia digital	17	3.5	Práctica 2. Análisis y recuperación de archivos con data carving	43
1.6	Cuestionario de autoevaluación	19	3.6	Práctica 3. Extracción de la base de datos de una red social almacenada en un dispositivo móvil	45
			3.7	Cuestionario de autoevaluación	48
TEMA 2: LABORATORIO FORENSE DIGITAL		23	TEMA 4: FORENSE DIGITAL EN MEDIOS DE ALMACENAMIENTO VOLÁTIL		51
2.1	Descripción del laboratorio forense digital	23	4.1	Definición y tipos de memoria ram	51
2.2	Características de implementación de un laboratorio forense digital	25	4.2	Memoria física y archivos de paginación	52
2.3	Herramientas de hardware y software para un laboratorio forense digital	30	4.3	Práctica 1. Volcado de memoria ram	53
2.4	Normas y recomendaciones aplicables para un laboratorio forense digital	33	4.4	Práctica 2. Análisis del contenido almacenado en la memoria ram	55
2.5	Cuestionario de autoevaluación	34	4.5	Práctica 3. Análisis del archivo pagefile.sys del sistema operativo windows	61
			4.6	Cuestionario de autoevaluación	62

TEMA 5: FORENSE DIGITAL EN ARCHIVOS MULTIMEDIA	65
5.1 Definición y tipos de archivos multimedia	65
5.2 Ocultamiento de información con esteganografía, y su detección con estegoanálisis.	66
5.3 Manipulación digital con inteligencia artificial (deepfake de voz, texto o video)	70
5.4 Práctica 1. Análisis de la integridad de una fotografía	71
5.5 Práctica 2. Aplicación de esteganografía	73
5.6 Práctica 3. Aplicación de estego-análisis	78
5.7 Práctica 4. Análisis de la integridad de un archivo de audio	80
5.8 Cuestionario de autoevaluación	86

ÍNDICE DE FIGURAS

FIGURA 1.1	
Ejemplo de evidencias no volátiles	16
FIGURA 1.2	
Ejemplos de evidencias volátiles	16
FIGURA 1.3	
Tipos de códigos hash	17
FIGURA 1.4	
Funciones del marco de ciberseguridad del nist	18
FIGURA 2.1	
Laboratorio informático forense de una empresa privada	30
FIGURA 2.2	
Recomendaciones generales en laboratorios forenses digitales	33

ÍNDICE DE TABLAS

TABLA 2.1	
Seguridad de la información en la gestión del laboratorio forense	28
TABLA 2.2	
Gestión del laboratorio forense digital en el área de investigación y desarrollo	29
TABLA 2.3	
Descripción comparativa de software forense	31
TABLA 2.4	
Herramientas portables para análisis forense digital	32
TABLA 3.1	
Comparación de los sistemas de archivos según su tamaño máximo de volumen y tamaño máximo de archivo	38
TABLA 3.2	
Compatibilidad de sistemas de archivos con plataformas de sistemas operativas	39
TABLA 5.1	
Comparación de herramientas para estego-análisis	68



INTRODUCCIÓN

La transformación digital ha traído consigo un creciente avance tecnológico y la digitalización de información que utilizamos comúnmente en nuestra vida cotidiana. En este contexto, la investigación forense digital se ha convertido en un componente indispensable para identificar, analizar y preservar pruebas electrónicas en casos relacionados con la ciberseguridad. Este manual proporciona una guía exhaustiva sobre las técnicas y procedimientos fundamentales en la investigación forense digital. A continuación, se presenta un resumen de los temas abordados en cada capítulo.

En el primer tema, “Protocolo para la Investigación Forense Digital”, se establecen los principios básicos de esta disciplina, subrayando la importancia de seguir protocolos rigurosos para garantizar la validez de las pruebas. Se detallan los pasos iniciales desde la detección hasta la recolección de evidencia, junto con los procedimientos para asegurar su integridad física y lógica. Este capítulo concluye con un cuestionario de autoevaluación.

El segundo tema, “Laboratorio Forense Digital”, explora la creación y operación eficiente de un laboratorio forense. Se discuten las características clave para su implementación, así como las herramientas de hardware y software necesarias. Además, se revisan las

normativas y mejores prácticas relevantes. El capítulo se cierra con un cuestionario de autoevaluación.

El tercer tema, “Forense Digital en Medios de Almacenamiento”, se centra en la investigación de pruebas en discos duros y sistemas de archivos. Se analizan los tipos de discos duros, la relevancia de los metadatos y se incluyen ejercicios prácticos de extracción y análisis de evidencia. Los lectores pueden evaluar su comprensión mediante un cuestionario de autoevaluación. El cuarto tema, “Forense Digital en Medios de Almacenamiento Volátil”, aborda la investigación en memoria RAM. Se explican los diferentes tipos de memoria RAM y cómo se manejan los datos en la memoria física y archivos de paginación. Los ejercicios prácticos incluyen el volcado y análisis de la memoria RAM, seguidos de un cuestionario de autoevaluación.

El quinto tema, “Forense Digital en Archivos Multimedia”, examina las técnicas para analizar y manejar archivos multimedia. Se categorizan los diferentes tipos de archivos multimedia y se estudian las técnicas para ocultar información, como la esteganografía, junto con métodos para detectar deepfakes. Este capítulo también ofrece ejercicios prácticos y un cuestionario de autoevaluación.

- 
- 
- 1.1 Investigación forense digital
 - 1.2 Importancia de cumplir con la cadena de custodia
 - 1.3 Proceso de detección, identificación y registro del incidente de ciberseguridad
 - 1.4 Recolección de las evidencias digitales según su estado
 - 1.5 Procedimiento para asegurar la integridad física y lógica de la evidencia digital
 - 1.6 Cuestionario de autoevaluación

1.1 Investigación forense digital

La investigación forense digital se refiere al proceso de preservar, identificar, extraer y documentar evidencia digital de diversos dispositivos electrónicos y sistemas informáticos. Esta evidencia digital puede ser crucial para resolver delitos cibernéticos, fraudes, violaciones de derechos de autor, amenazas a la seguridad nacional y una amplia variedad de otras actividades ilegales o no autorizadas.

Se define como ciencia y tecnología en la investigación de una escena del crimen, para maximizar la efectividad de demostrar la culpabilidad del autor ante un tribunal de justicia. Las pruebas son esenciales para cualquier investigación de una escena del crimen, conocida como investigaciones de CSI, lo que también incluye los delitos cibernéticos (Gupta et al., 2016).

Este campo en rápida evolución abarca la informática forense, la informática forense móvil, la informática forense en la nube y la informática forense de Internet de las cosas; por esta razón, cuando surge la necesidad de enjuiciar un delito, es necesario

tener mucha evidencia digital. Para que la evidencia digital sea admisible en el tribunal de justicia, debe ser auténtica, precisa, completa y convincente para el jurado (Brown, 2022). La investigación forense digital implica el uso de técnicas y herramientas especializadas para recopilar y analizar datos digitales de manera legal y admisible en los tribunales. Esto incluye la adquisición forense de dispositivos de almacenamiento, como discos duros, unidades USB, teléfonos móviles, cámaras digitales, entre otros. La investigación forense digital se aplica en diversos escenarios, como investigaciones criminales, litigios civiles, auditorías de seguridad, análisis de incidentes de seguridad informática, entre otros. Requiere conocimientos especializados en áreas como sistemas operativos, redes, análisis de malware, recuperación de datos, entre otros, así como el manejo de herramientas y técnicas forenses específicas. Es importante destacar que la investigación forense digital debe llevarse a cabo de manera ética y legal, respetando los derechos y privacidad de las personas involucradas, y siguiendo los procedimientos y regulaciones aplicables en cada jurisdicción.

1.2 Importancia de cumplir con la cadena de custodia

La cadena de custodia es el proceso de control y documentación detallada del rastro de la evidencia digital, desde su adquisición hasta su presentación en un tribunal o informe final. Este proceso garantiza la integridad, autenticidad y confiabilidad de la evidencia digital, lo que es fundamental para su admisibilidad en procedimientos legales (Jawad, 2018).

Cumplir con la cadena de custodia es importante por varias razones:

- **Preservación de la integridad de la evidencia:** la cadena de custodia asegura que la evidencia digital no sea alterada, modificada o contaminada durante el proceso de investigación. Cualquier cambio en los datos podría comprometer su valor probatorio y credibilidad.
- **Admisibilidad en tribunales:** en procedimientos legales, la cadena de custodia es un requisito fundamental para que la evidencia digital sea admitida y considerada válida por los tribunales. Si la cadena de custodia se rompe o no se documenta adecuadamente, la evidencia puede ser descartada o cuestionada.
- **Trazabilidad y transparencia:** la cadena de custodia proporciona un registro detallado de todas las personas que han tenido acceso a la evidencia digital, las acciones realizadas y las fechas y horas correspondientes. Esto brinda trazabilidad y transparencia al proceso, permitiendo identificar posibles problemas o irregularidades.
- **Reproducibilidad de la investigación:** al documentar minuciosamente los pasos seguidos y las herramientas utilizadas, la cadena de custodia permite que la

investigación sea reproducible por otros expertos forenses, lo que refuerza la validez de los hallazgos.

- **Credibilidad del perito forense:** cumplir estrictamente con la cadena de custodia demuestra la competencia y profesionalismo del perito forense, lo que refuerza su credibilidad ante tribunales y autoridades.

Cumplir con la cadena de custodia es de gran importancia en cuanto a pruebas informáticas, han sido muchos los casos donde los tribunales han hecho inadmisibles a las pruebas informáticas, esto se debe a no cumplir con la cadena de custodia, para poder determinar si ha tenido una alteración la prueba informática en una evidencia es cuestión matemática y dicotómica, es decir si la prueba no ha sido alterada desde el momento de su recolección hasta cuando se realiza el estudio forense, se ha cumplido con la cadena de custodia, en cambio, si esta prueba ha sido modificada o contaminada de alguna forma, la cadena de custodia ha sido destruida (Bonomi et al., 2019)

Para que las pruebas sean admisibles en el tribunal, es esencial mantener y evaluar la integridad de las pruebas obtenidas en la escena del crimen, que deben realizarse adecuadamente siguiendo un conjunto de procedimientos. Realizar un seguimiento de las pruebas desde que se recogieron en la escena del crimen hasta que llegan al tribunal es una tarea importante. Para proteger la integridad de la evidencia, el investigador debe estar consciente de cómo, dónde y quién maneja la evidencia durante cada paso del análisis. Se han desarrollado varias herramientas y tecnologías para manejar la evidencia a lo largo del tiempo. Investigadores de todo el mundo han desarrollado una variedad de enfoques para el manejo de la evidencia. Para mejorar el proceso, muchos investigadores han combinado la tecnología blockchain con la cadena de custodia o el ciclo de vida de la evidencia (Banwani & Kalra, 2021).

1.3 Proceso de detección, identificación y registro del incidente de ciberseguridad

Para reducir el impacto de los incidentes, se debe realizar una detección temprana, identificación y registro adecuados. Para ello, el proceso de detección, identificación y registro es crucial para reducir su impacto y tomar acciones apropiadas en respuesta a él. Las organizaciones necesitan entender la naturaleza del incidente, identificar los activos afectados y contener cualquier daño mientras se esfuerza por restablecer la normalidad.

Incidente de ciberseguridad. Es un evento o una serie de eventos inesperados o no deseados que ocurran dentro de los sistemas de información o la red de una empresa y que podrían resultar en una violación de la confidencialidad, integridad y disponibilidad de la información. Hay varios factores que contribuyen a que ocurran estos incidentes, entre ellos:

- **Ataques cibernéticos:** Los hackers, los ciberdelincuentes o incluso los estados nacionales pueden llevar a cabo estos ataques. Códigos maliciosos, phishing, ataques de denegación de servicio (DoS) y el ransomware son algunos ejemplos comunes de ataques cibernéticos (Tatar, 2021).

- **Errores humanos:** una de las principales causas de incidentes de ciberseguridad son los errores humanos. Estos errores pueden incluir hacer clic en un enlace malicioso, abrir un archivo adjunto infectado o ingresar datos confidenciales en un sitio web no legítimo.

- **Fallos del sistema:** los incidentes de ciberseguridad también pueden ser el resultado de fallas del sistema. Estos errores pueden ser causados por desastres naturales, hardware o software defectuosos.

Proceso de detección. - La detección de un incidente de ciberseguridad es el primer paso crítico en la respuesta a incidentes. Este proceso implica identificar indicios o señales de actividad sospechosa o no autorizadas en los sistemas y redes. Algunas técnicas y mecanismos utilizados para la detección incluyen:

- Monitoreo y análisis de registros de eventos (event logs) en sistemas operativos, aplicaciones, dispositivos de red y herramientas de seguridad.
- Implementación de sistemas de detección de intrusos (IDS/IPS) para monitorear el tráfico de red y detectar patrones de ataque conocidos o anomalías.
- Análisis de cambios no autorizados en archivos,

- configuraciones o líneas base de sistemas.
- Revisión periódica de informes de vulnerabilidades y amenazas publicados por fuentes confiables.
- Recepción de informes o alertas de usuarios, personal de TI o proveedores de servicios sobre actividades sospechosas.

Proceso de identificación. - Una vez detectado un posible incidente, es necesario identificar su naturaleza, alcance y posibles causas. Este proceso implica recopilar y analizar información relevante, como:

- Revisar registros de eventos (event logs) en sistemas operativos, aplicaciones y dispositivos de red.
- Analizar archivos de registro (log files) de firewalls, sistemas de detección de intrusos (IDS/IPS), servidores web, entre otros.
- Realizar capturas de tráfico de red (network traffic captures) y analizarlas en busca de actividades sospechosas.
- Examinar los procesos en ejecución y las conexiones de red activas en los sistemas comprometidos.
- Identificar cambios no autorizados en archivos, configuraciones o líneas base de sistemas.
- Utilizar herramientas forenses para obtener información adicional, como timestamps, metadatos, entre otros.

Proceso de registro. - El registro y documentación detallada de todas las acciones y hallazgos relacionados con un incidente de ciberseguridad es fundamental para respaldar cualquier acción legal o disciplinaria posterior. Este proceso implica:

- Mantener un registro preciso de las fechas, horas, personas involucradas y acciones realizadas durante la detección, identificación y respuesta al incidente.
- Documentar de manera clara y concisa los hallazgos, decisiones tomadas y justificaciones correspondientes.
- Incluir capturas de pantalla, diagramas, copias de registros y cualquier otra información relevante que respalde los hallazgos.
- Seguir estándares y mejores prácticas de documentación forense para garantizar la admisibilidad de la evidencia.
- Almacenar y proteger adecuadamente la documentación generada para preservar su integridad y confidencialidad.

1.4 Recolección de las evidencias digitales según su estado

Evidencias no volátiles. - Las evidencias informáticas no volátiles son todos los datos almacenados en medios físicos como discos duros, discos sólidos, memoria USB, estos son cruciales para la investigación forense digital, ya que estos pueden tener las pruebas relevantes para crímenes o delitos cometidos. Para cumplir con la cadena de custodia es fundamental documentar y registrar cada paso del manejo de la evidencia para garantizar su autenticidad e integridad. El proceso de recolección de evidencias no volátiles es:

- Realizar una adquisición forense de los medios de almacenamiento utilizando herramientas específicas para crear imágenes forenses bit a bit.
- Calcular y documentar los valores hash de las imágenes forenses adquiridas para verificar su integridad.
- Recolectar archivos de interés, registros de actividad, correos electrónicos, documentos y cualquier otra evidencia relevante.
- Mantener una cadena de custodia estricta y documentar todos los pasos del proceso.

Es importante tener en cuenta que, aunque las evidencias no volátiles son menos susceptibles a perderse, se deben tomar precauciones para evitar su modificación o alteración durante el proceso de recolección. Algunos ejemplos de evidencias no volátiles son:

Figura 1.1 Ejemplo de evidencias no volátiles

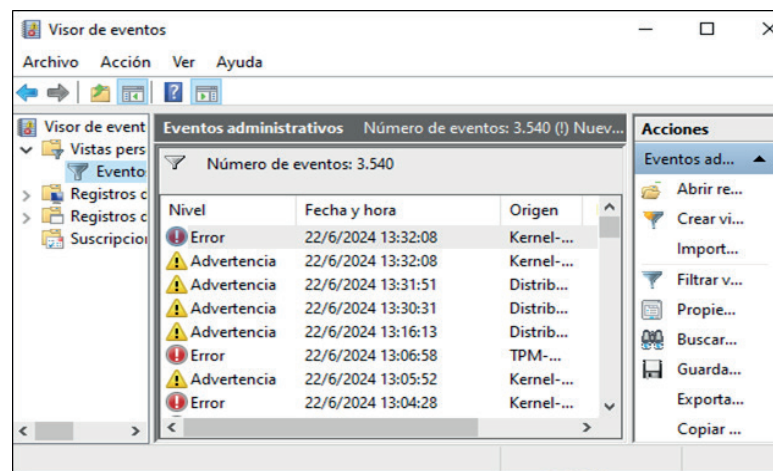


Evidencias informáticas volátiles. - Las evidencias informáticas volátiles son los datos almacenados en sistemas remotos, discos duros remotos, servidores, que solo pueden acceder a través de la red, su naturaleza las hace más propensas a cambios o eliminaciones, así que dificulta su integridad a largo plazo también es importante generar código hash. Ejemplos son páginas web, mensajes en redes sociales, archivos multimedia y software alojados en la nube. El proceso de recolección de evidencias volátiles es:

- Adquirir una imagen forense de la memoria RAM (memoria volátil) utilizando herramientas específicas para este fin.
- Capturar y almacenar registros de eventos (event logs) de los sistemas comprometidos.
- Recolectar información sobre procesos en ejecución, conexiones de red activas y otros datos volátiles relevantes.
- Documentar cuidadosamente cada paso del proceso y calcular valores hash para verificar la integridad de las evidencias recolectadas.

Es importante actuar rápidamente en la recolección de evidencias volátiles, ya que estas pueden perderse al reiniciar o apagar los sistemas.

Figura 1.2 Ejemplos de evidencias volátiles



Código hash.-El objetivo principal del código hash es garantizar la integridad y autenticidad de las pruebas informáticas, evitando cualquier modificación o manipulación. Se crea mediante algoritmos matemáticos como MD5 o SHA-256 (Kakunuri & Subhadra, 2021). Es esencial para mantener la cadena de custodia y la integridad de las pruebas porque permite detectar cambios en dispositivos móviles, memorias USB, discos duros, páginas web y archivos de texto, entre otros.

Figura 1.3 Tipos de códigos hash

Name	Length	Hash
md2	16	5CCF1F0592D8F1FBF7957EC95F96A9AC
md4	16	36BD43C9419F931E49AD9869BF16209C
md5	16	D43EDEDCEE20F3FBAA2550E451311586
sha1	20	74B612D43EC54446058EBB14A41ADA0BFEC0A19
sha224	28	CC0CD42C99B1468AA7811FA6A8154B6ED37EF3244BD8EF32CF
sha256	32	A06F3DE4C5F0A4892A6109587A5B2C3D4EAD1F935FC5745F0D
sha384	48	340FECA21FA9C1CB4FA32209840B4696F801493BEABE4A54E4E
sha512/224	28	75ADC6DE4163C788E15A7A76594780767E80F8724D67A08275
sha512/256	32	9C0B1C32CB18D67311079912BE2E6C8002085A50CE460C59C7

1.5 Procedimiento para asegurar la integridad física y lógica de la evidencia digital

La evidencia digital se refiere a cualquier información que esté disponible en formato electrónico y pueda usarse en procedimientos legales. Garantizar la integridad física y lógica de las pruebas digitales es fundamental para mantener su confiabilidad y confiabilidad en los tribunales (OSCO ESCOBEDO MIGUEL ANGEL et al., 2023).

La integridad física se refiere al estado físico de la evidencia

digital, mientras que la integridad lógica se refiere a su contenido.

Para garantizar ambas cosas, se deben seguir procedimientos rigurosos, desde identificar y preservar pruebas hasta analizarlas y presentarlas en un entorno legal.

Integridad física de la evidencia digital:

- **Manejo adecuado:** manejar la evidencia digital con sumo cuidado, evitando cualquier manipulación o exposición a condiciones que puedan dañarla o alterarla físicamente.
- **Empaquetado:** empaquetar la evidencia digital en contenedores seguros y sellados, utilizando materiales antiestáticos y etiquetarla adecuadamente con información relevante, como el caso, fecha, ubicación y responsable.
- **Cadena de custodia:** implementar una cadena de custodia estricta, documentando cada transferencia, manejo y ubicación de la evidencia digital, incluyendo fechas, horas y personas responsables.
- **Almacenamiento:** almacenar la evidencia digital en un ambiente controlado y seguro, con temperatura, humedad y protección contra campos electromagnéticos adecuados.

Integridad lógica de la evidencia digital:

- **Adquisición forense:** realizar la adquisición de la evidencia digital utilizando herramientas y métodos forenses aprobados, como la creación de imágenes forenses bit a bit, para preservar la integridad lógica de los datos.
- **Cálculo de valores hash:** calcular y documentar los valores hash (como MD5, SHA-1, SHA-256) de la evidencia digital adquirida, para verificar su integridad y detectar cualquier modificación posterior.
- **Uso de herramientas confiables:** utilizar herramientas forenses confiables y validadas, que cumplan con los estándares y prácticas recomendadas en la industria.
- **Acceso restringido:** restringir el acceso a la evidencia digital únicamente al personal autorizado y capacitado, evitando cualquier manipulación o alteración no autorizada.
- **Documentación detallada:** documentar exhaustivamente todos los pasos, herramientas y métodos utilizados durante la adquisición, análisis

y manejo de la evidencia digital, para garantizar la reproducibilidad y transparencia del proceso.

Framework de investigación forense digital NIST. - El Marco de Investigación Forense Digital del National Institute of standards and Technology (NIST, por sus siglas en inglés) puede ayudar a una organización a comenzar y mejorar su ciberseguridad. Este marco proporciona una estructura para que los investigadores forenses digitales realicen investigaciones de manera consistente, eficiente y efectiva. El objetivo principal del marco es ayudar a las organizaciones a gestionar de manera más efectiva la respuesta a incidentes de seguridad informática y las investigaciones forenses digitales (Soto & Olier, 2023). El NIST Digital Forensic Framework está estructurado por tal como se muestra en la Figura 1.4.

Figura 1.4 Funciones del marco de ciberseguridad del NIST

Primeros pasos de NIST Marco de ciberseguridad: Guía de inicio rápido	
IDENTIFICAR	- Identifique los procesos y activos críticos empresariales -Flujos de información de documentos -Mantener el inventario de hardware y software - Establecer políticas para la ciberseguridad que incluyan roles y responsabilidades -Identificar amenazas, vulnerabilidades y riesgos a activos
PROTEGER	- Gestionar el acceso a activos e información -Proteger los datos sensibles
DETECTAR	-Probar y actualizar los procesos de detección -Hacer respaldos con regularidad -Proteger sus dispositivos -Gestionar las vulnerabilidades de los dispositivos -Capacitar a los usuarios - Conocer los flujos de datos esperados de su empresa -Mantener y monitorear los archivos de registro
RESPONDER	-Asegurarse de que los planes de respuesta sean probados -Asegurarse de que los planes de respuesta sean actualizados
RECUPERAR	-Comunicarse con las partes interesadas internas y externas -Asegurarse de que los planes de recuperación sean actualizados -Gestionar las relaciones públicas y la reputación de la compañía

1.6 Cuestionario de autoevaluación

1. **¿En dónde se almacenan las evidencias informáticas no volátiles?**
 - a. Páginas web
 - b. Discos sólidos
 - c. Discos remotos
 - d. Memorias USB
2. **¿Qué es un código hash?**
 - a. Un código hash es un número secreto que se utiliza para proteger la información.
 - b. Un código hash es un tipo de código de barras.
 - c. Un código hash es un virus informático.
 - d. Un código hash es una representación matemática única y compacta de un conjunto de datos como MD5 o SHA-256
3. **¿Cuáles son los 5 primeros pasos de NIST Marco de ciberseguridad?**
 - a. Identificar, Proteger, Detectar, Responder, Recuperar
 - b. Identificar, Investigar, Detectar, Responder, Recuperar
 - c. Investigar, Proteger, Detectar, Responder, Recuperar
 - d. Identificar, Corregir, Recuperar
4. **¿Qué significa NIST?**
 - a. North Indian Standard Time
 - b. National Institute of standards and Technology
 - c. National Institute and Technology
 - d. National service
5. **¿Cuál es el primer paso en el proceso de investigación forense digital?**
 - a. Análisis
 - b. Preservación
 - c. Identificación
 - d. Presentación
6. **¿Qué técnica se utiliza para verificar la integridad de la evidencia digital?**
 - a. Empaquetado
 - b. Cadena de custodia
 - c. Almacenamiento seguro
7. **¿Cuál de los siguientes NO es un tipo de evidencia volátil?**
 - a. Memoria RAM
 - b. Registros de eventos
 - c. Discos duros
 - d. Conexiones de red activas
8. **¿Qué implica mantener una cadena de custodia adecuada?**
 - a. Calcular valores hash
 - b. Documentar cada transferencia y manejo de la evidencia
 - c. Utilizar herramientas forenses confiables
 - d. Restringir el acceso a la evidencia
9. **¿Cuál es el objetivo principal del registro y documentación durante una investigación forense digital?**
 - a. Preservar la integridad física de la evidencia
 - b. Respaldar cualquier acción legal o disciplinaria posterior
 - c. Realizar la adquisición de la evidencia
 - d. Calcular valores hash
10. **¿Qué tipo de evidencia digital se encuentra almacenada en medios de almacenamiento persistentes?**
 - a. Volátil
 - b. No volátil
 - c. Física
 - d. Lógica
11. **¿Cuál de las siguientes NO es una técnica utilizada para la detección de incidentes de ciberseguridad?**
 - a. Monitoreo de registros de eventos
 - b. Análisis de tráfico de red
 - c. Revisión de informes de vulnerabilidades
 - d. Cálculo de valores hash
12. **¿Qué implica el proceso de preservación de la evidencia digital?**
 - a. Adquirir imágenes forenses de los sistemas comprometidos
 - b. Analizar la evidencia digital recolectada
 - c. Identificar las causas raíz del incidente
 - d. Preparar informes de los hallazgos

13. **¿Qué se debe hacer para asegurar la integridad lógica de la evidencia digital?**
 - a. Empaquetar y etiquetar la evidencia
 - b. Realizar la adquisición forense utilizando herramientas y métodos aprobados
 - c. Almacenar la evidencia en un ambiente controlado
 - d. Implementar una cadena de custodia estricta

14. **¿Cuál es la importancia de cumplir con la cadena de custodia en una investigación forense digital?**
 - a. Preservar la integridad física de la evidencia
 - b. Garantizar la admisibilidad de la evidencia en procedimientos legales
 - c. Calcular valores hash de la evidencia d) Restringir el acceso a la evidencia

15. **¿Tipos de investigación forense digital?**
 - a. Investigación Forense móvil
 - b. Investigación de la escena del crimen
 - c. Investigación forense en dispositivos de almacenamiento.
 - d. Investigación analítica.



- 
- 
- 2.1 Descripción del laboratorio forense digital
 - 2.2 Características de implementación de un laboratorio forense digital
 - 2.3 Herramientas de hardware y software para un laboratorio forense digital
 - 2.4 Normas y recomendaciones aplicables para un laboratorio forense digital
 - 2.5 Cuestionario de autoevaluación

2.1 Descripción del laboratorio forense digital

El laboratorio forense digital es esencial para mantener la integridad del proceso de análisis de la evidencia digital. Dada la rápida expansión de las tecnologías digitales y la ciberdelincuencia, ha habido un aumento en la demanda de especialistas forenses competentes, lo que se ha traducido en un aumento significativo de la educación y la formación en materia forense digital (Molina, 2017).

El laboratorio forense digital es una instalación equipada con hardware y software de última generación, supervisada por profesionales expertos con amplia experiencia en el campo de la informática forense. Su función implica la recuperación y el examen de datos de diversas plataformas digitales, como dispositivos de almacenamiento, redes y sistemas informáticos. El objetivo principal es validar la integridad de los datos adquiridos para garantizar su idoneidad como prueba en los procedimientos legales, respetando las normas legales (El nuevo Laboratorio Forense de Evidencia Digital de la Defensoría del Pueblo, 2024).

Se ha reconocido que existen obstáculos para establecer laboratorios forenses digitales prácticos y eficientes, lo que subraya la necesidad de contar con directrices que ayuden a los

educadores a establecer laboratorios educativos. Estos laboratorios son cruciales para dotar a los profesionales de las habilidades necesarias para abordar los desafíos técnicos, como la generación de archivos de imágenes de gran tamaño, y para proporcionar información que agilice el proceso de creación de laboratorios. Al integrar los elementos de las normas ISO/IEC y las perspectivas de los expertos, los laboratorios forenses digitales son indispensables para las organizaciones que buscan garantizar resultados de análisis confiables y cumplir con los requisitos de competencia en las evaluaciones legales.

Aplicabilidad de los laboratorios forenses digitales. - Los laboratorios forenses digitales se utilizan en una amplia gama de escenarios, como los delitos informáticos relacionados con el fraude electrónico, el robo de identidad, la piratería informática, programa maligno y más. También son fundamentales en las investigaciones penales relacionadas con el homicidio, el robo, el tráfico de drogas y el terrorismo, entre otros. Además, estas instalaciones desempeñan un papel crucial en los casos de litigios civiles, incluidos los casos de divorcio, las disputas por la custodia de los hijos, los asuntos de propiedad intelectual, etc. (Casey, 2011)

Dentro de un laboratorio forense digital, se examinan una variedad de categorías forenses distintas, lo que lleva a la presentación de hallazgos que son admisibles en un entorno legal. Estos procedimientos permiten identificar las posibles actividades delictivas, los métodos y los plazos de ocurrencia, los recursos afectados y la posible culpabilidad.

Para este objetivo, un laboratorio forense digital emplea sofisticadas herramientas de hardware y software diseñadas explícitamente para la recuperación, el examen y la exposición de pruebas digitales de manera forense. Además, se siguen protocolos estrictos para mantener la integridad de los exámenes y garantizar la precisión de los hallazgos (Di Lorio et al., 2016).

Dentro del laboratorio forense digital también presentamos el abanico de dispositivos y medios digitales, tales como:

- Computadoras y laptops
- Dispositivos móviles (celulares, etc.)
- Unidades de almacenamiento (HDD, SSD, memorias USB)
- Servidores y redes informáticas
- Evidencia en la nube (correos electrónicos, redes sociales)

Los laboratorios forenses digitales desempeñan un papel crucial en varios contextos, como las investigaciones penales, los incidentes de violaciones de la ciberseguridad, las auditorías de cumplimiento y la recuperación de datos. En el ámbito de las investigaciones penales, son fundamentales para resolver los casos de engaño, robo de identidad y explotación de menores.

Por motivos de ciberseguridad, estas instalaciones son indispensables para examinar y gestionar las infracciones resultantes de la piratería informática, las filtraciones de datos y los ataques de denegación de servicio distribuida. También se utilizan para garantizar el cumplimiento

de los protocolos de seguridad y las leyes legales, así como para recuperar datos cruciales tras fallos técnicos o intrusiones cibernéticas (Calderón Valdiviezo et al., 2011).

Los laboratorios forenses digitales se utilizan en varios escenarios:

- **Investigaciones penales:** relacionadas con delitos informáticos, el fraude cibernético, el robo de identidad y la pornografía infantil.
- **Litigios civiles:** desempeñan un papel en los casos de propiedad intelectual, las disputas contractuales y los divorcios.
- **Investigaciones internas:** incluidas las investigaciones corporativas y las auditorías de seguridad informática.
- **Aplicación de la ley:** desempeñan un papel decisivo en la realización de investigaciones relacionadas con el tráfico de drogas, el terrorismo y el lavado de dinero.

Importancia de tener un Laboratorio Forense Digital. - La importancia de poseer un laboratorio forense digital competente reside en su capacidad para realizar investigaciones forenses digitales con eficiencia y seguridad. Estas instalaciones desempeñan un papel vital en la lucha contra las actividades ciberdelictivas al facilitar la identificación, el examen y la protección de las pruebas procedentes de eventos relacionados con la informática para su utilización en los procesos judiciales. Además, ayudan a las organizaciones a cumplir con los protocolos de seguridad y confidencialidad, al tiempo que mejoran su capacidad para abordar los problemas de ciberseguridad, mitigando así los daños adicionales (Choji, 2021).

2.2 Características de implementación de un laboratorio forense digital

En este discurso profundizaremos en los atributos fundamentales que delinear el establecimiento de un laboratorio forense digital, enfatizando su marco tecnológico especializado, los estrictos procedimientos de manejo de evidencia, las medidas de protección física y lógica, la educación del personal, el trabajo en equipo interdisciplinario y el cumplimiento de los marcos y directivas legales. Estos aspectos son imprescindibles para garantizar la autenticidad y la fiabilidad de las investigaciones forenses digitales, reforzando así la administración de justicia en el ámbito digital. (Appendino et al., 2015) , (A. Di Iorio et al., 2019).

Planificación estrategia. - En primer lugar, es imperativo delinear claramente el alcance y las capacidades del laboratorio, teniendo en cuenta los análisis forenses específicos que se llevarán a cabo y las áreas de especialización requeridas. Esto servirá de base para la adquisición de equipos, la contratación de personal y el diseño de las instalaciones. Otro enfoque fundamental consiste en forjar asociaciones y colaboraciones con otras entidades forenses, académicas y gubernamentales.

Estas alianzas pueden facilitar el intercambio de conocimientos, el intercambio de recursos y la implementación de las mejores prácticas, mejorando así la credibilidad y la posición del laboratorio. Es crucial desarrollar una estrategia integral de recursos humanos, que abarque la contratación de personal competente en diversas disciplinas forenses y la implementación de iniciativas de capacitación continua para mantener la relevancia de las habilidades. Estos protocolos deben alinearse con las mejores prácticas y regulaciones mundiales. En esencia, la planificación estratégica desempeña un papel fundamental en el establecimiento exitoso de un laboratorio forense, ya que abarca análisis de necesidades, la definición de la capacidad y objetivos claros, la gestión de los recursos humanos y físicos, la adquisición de equipos, la estandarización de los protocolos y la obtención de acreditaciones y certificaciones acreditadas (Palacios Carvajal, 2020).

- **Definición de objetivos claros:** establecer el propósito y el alcance del laboratorio forense digital implica tener en cuenta la naturaleza de las investigaciones que se llevarán a cabo, el grupo demográfico objetivo y los recursos disponibles.

- **Análisis de las necesidades:** la evaluación de los requisitos específicos del laboratorio abarca los tipos de dispositivos y sistemas que deben analizarse, el volumen de evidencia digital que debe gestionarse y las competencias que se esperan del personal.

- **Asignación eficiente de los recursos:** la distribución adecuada de los recursos financieros, humanos y tecnológicos es crucial para garantizar el cumplimiento de los objetivos definidos y el funcionamiento eficiente del laboratorio

Infraestructura segura. - La infraestructura del laboratorio forense digital es la piedra angular para desarrollar las capacidades de investigación. Un plan de infraestructura complejo y confiable garantiza la autenticidad de las pruebas digitales, la eficacia de los procedimientos forenses y la protección de los datos confidenciales (A. Di Iorio et al., 2019) .

- **Espacio físico adecuado:** garantice un espacio físico que cumpla con las condiciones ambientales y de seguridad necesarias para proteger la evidencia digital, la integridad del trabajo forense y el bienestar del personal.

- **La implementación de medidas de seguridad físicas y lógicas es esencial:** se deben establecer controles de acceso, vigilancia, firewalls, cifrado de datos, etc., para proteger el laboratorio contra las intrusiones no autorizadas, la pérdida de datos y los daños a la infraestructura (Calderón Valdiviezo et al., 2011).

- **Es imprescindible establecer una red segura y aislada:** crear una red exclusiva para gestio-

nar las pruebas digitales, separada de la red general de la organización, para evitar la contaminación o el acceso no autorizado a la información confidencial.

Personal capacitado. - A continuación, se describen algunas características que deben destacar en los investigadores forenses digitales.

- **Experiencia en informática forense:** la contratación o la formación del personal de laboratorio en informática forense es esencial, ya que abarca una comprensión integral de las herramientas, metodologías y técnicas de investigación forense digital necesarias para el análisis y procesamiento exhaustivos de las pruebas digitales.

- **Familiaridad con las herramientas y metodologías:** es crucial garantizar que el personal esté bien versado en la utilización de las herramientas y metodologías específicas de investigación forense digital que se utilizan en el laboratorio, garantizando su competencia y correcta implementación.

- **Educación continua:** es imperativo fomentar la educación continua entre los miembros del personal sobre los desarrollos, tecnologías y metodologías más recientes en el ámbito de la investigación forense digital para mantener el estado vanguardista del laboratorio y mejorar su eficacia a la hora de abordar los delitos relacionados con la informática.

Procedimientos estandarizados. - A continuación, se describen algunos de los procedimientos que deben seguir los investigadores forenses digitales.

- **Manuales de procedimientos:** deben elaborarse y utilizar manuales de procedimiento detallados para delinear claramente las operaciones que se llevan a cabo en el laboratorio, que abarquen la obtención, el examen, la protección y la exhibición de pruebas digitales, con el objetivo de garantizar la uniformidad, la excelencia y la confiabilidad de los resultados.

- **Pautas de buenas prácticas:** es aconsejable incorporar pautas de buenas prácticas que definan puntos de referencia y sugerencias para ejecutar tareas forenses en el laboratorio, salvaguardando así el calibre y la confiabilidad de

los procedimientos y la autenticidad de las pruebas digitales.

- **Controles de calidad:** la integración de los controles de calidad es esencial para validar la precisión y la confiabilidad de los procedimientos y metodologías aplicados en el laboratorio, manteniendo así el estándar de los resultados y la legitimidad de los esfuerzos forenses.

Cadena de custodia de la evidencia digital. - En la investigación forense digital, la cadena de custodia es crucial para salvaguardar la integridad, la autenticidad y la fiabilidad de las pruebas digitales desde su obtención hasta su visualización en un procedimiento judicial. La cadena de custodia registra meticulosamente cada etapa de la administración de las pruebas, estableciendo una vía rastreable que refuerza su aceptabilidad en un entorno legal. (Valdiviezo et al., s. f.)

El procedimiento de cadena de custodia en un laboratorio forense digital abarca las siguientes etapas:

1. **Etapas de recolección y defensa.** - El proceso de recopilación y preservación de pruebas implica el acto de buscar, identificar y obtener pruebas digitales en la escena del crimen o en posesión del sospechoso.

- En el contexto de Aislamiento y aseguramiento: garantizar la separación de la evidencia digital de su entorno original para evitar cualquier forma de contaminación o alteración, como señaló.

- La etapa de envasado y etiquetado: requiere la utilización de materiales y etiquetas adecuadas que contengan información precisa para salvaguardar e identificar adecuadamente las pruebas.

- Durante la fase de transporte seguro: las pruebas se transfieren al laboratorio forense digital de conformidad con un protocolo predefinido.

2. **Fase de búsqueda y control de la evidencia.** - En esta fase, se procede a identificar la evidencia a analizar, además de su cuidado y debida manipulación.

- La admisión al laboratorio: implica documen-

tar la llegada de la evidencia, anotando la fecha, la hora y la persona responsable.

- **Asignar un identificador:** es esencial asignar un identificador único a cada prueba, ya que este identificador estará vinculado a la evidencia durante todo el proceso.

- **Control de actividades:** debe documentar exhaustivamente todas las medidas adoptadas con las pruebas, especificando la fecha, la hora, la persona a cargo, el tipo de análisis realizado y las herramientas utilizadas.

- **Acumulación segura:** es crucial garantizar el almacenamiento seguro de las pruebas en un lugar de acceso controlado y restringido.

3. Fase de presentar el proceso legal. - En esta fase, se procede a redactar el informe pericial o de los hallazgos obtenidos durante la investigación forense digital, detallando todos los procedimientos realizados.

- **Preparación de informes:** elaboración de informes detallados y completos que describan la cadena de custodia, el análisis forense y los hallazgos obtenidos.

Gestión del laboratorio forense digital. - Como parte de la administración y organización de los elementos del laboratorio forense digital, es importante evaluar y garantizar la calidad de los procesos forenses, así como la seguridad de la información respecto a los datos que se manipularán durante el análisis de la evidencia digital. Respetar la ética profesional manteniendo siempre un criterio objetivo e imparcial en los resultados obtenidos, siguiendo todos los lineamientos de investigación y desarrollo mediante la aplicación de técnicas y herramientas avanzadas según el tipo de delito o incidente de ciberseguridad.

Gestión de la calidad: la gestión de la calidad (QM) es un factor fundamental para garantizar la fiabilidad, la honestidad y la objetividad de los procedimientos y resultados de la investigación. El establecimiento de un laboratorio forense digital (LFD) eficiente incorpora principios, protocolos y metodologías que abarcan su funcionalidad, desde la recepción de las pruebas digitales hasta la presentación de las conclusiones. El Consejo General (GC) de un LFD supe-

ra la mera ejecución de un sistema estructurado de gestión de la calidad (SGC), ya que requiere fomentar una cultura de excelencia en el laboratorio, donde la búsqueda de un rendimiento superior en todas las operaciones y tareas se convierte en un principio fundamental (Parra et al., 2021).

- **Ética profesional:** en la era contemporánea, donde la tecnología digital desempeña un papel cada vez más importante en varios aspectos de nuestra vida cotidiana, el campo de la investigación forense digital se ha convertido en una herramienta indispensable en el ámbito del sistema de justicia penal. Los laboratorios forenses digitales tienen la tarea fundamental de analizar e interpretar las pruebas digitales en el contexto de la ciberdelincuencia, el fraude informático y otros tipos de investigaciones penales. Los resultados de los análisis realizados en estas instalaciones especializadas pueden influir en el destino de las personas; por lo tanto, es imperativo que los profesionales de estos entornos se adhieran a directrices éticas estrictas. El marco ético de los laboratorios forenses digitales se basa en principios fundamentales que abarcan la objetividad, la competencia, la confidencialidad, la transparencia, la responsabilidad y el respeto. Estos principios rectores no son simples sugerencias, sino que sirven como pilares fundamentales que defienden la integridad, la neutralidad y la profesionalidad de las investigaciones forenses digitales.

- **Seguridad de la información:** En el ámbito de la investigación penal, el laboratorio forense digital se ha convertido en un instrumento esencial para analizar las pruebas digitales en casos de delitos informáticos y cibernéticos. La delicada naturaleza de las pruebas digitales, que abarcan la información personal, los datos clasificados y las pruebas de actividades ilícitas, exige el establecimiento de protocolos de seguridad estrictos para protegerlas del acceso no autorizado, la manipulación o la destrucción. La seguridad de la información en la gestión de los laboratorios forenses digitales se refiere a la aplicación de directivas, protocolos y procedimientos tecnológicos para garantizar el secreto, la precisión y la accesibilidad de la evidencia digital en su ciclo de vida, desde su adquisición hasta su eliminación definitiva (cyb_analisis_foren.pdf, s. f.). A continuación, la Tabla 2.1 muestra los criterios de seguridad de la información en la gestión del laboratorio forense digital.

Aspecto	Descripción	Medidas de seguridad
Protección de la Evidencia Digital	Garantizar la integridad y confidencialidad de la evidencia digital.	• Técnicas de adquisición forense seguras. • Almacenamiento de evidencia en entornos controlados y cifrados. • Control de versiones y trazabilidad de la evidencia.
Gestión de Acceso y Control de Usuarios	Restringir el acceso a la evidencia digital y los sistemas forenses a personal autorizado.	• Autenticación multifactorial. • Asignación de roles y privilegios. • Supervisión continua de actividades del usuario. • Registros de acceso y auditoría.
Seguridad de la Red y Comunicaciones	Proteger la infraestructura de red y las comunicaciones del laboratorio forense digital.	• Segmentación de redes. • Cifrado de datos en tránsito. • Monitoreo de la red. • Firewalls y sistemas de detección de intrusiones (IDS/IPS).
Cumplimiento Legal y Regulatorio	Garantizar el cumplimiento de las leyes y regulaciones aplicables.	• Estándares de cadena de custodia. • Privacidad de datos. • Protección de derechos de propiedad intelectual. • Registros detallados y documentación de procedimientos. • Auditorías y revisiones periódicas.
Gestión de Incidentes y Continuidad del Negocio	Establecer planes para responder a incidentes de seguridad y garantizar la continuidad del negocio.	• Plan de respuesta a incidentes. • Procedimientos de recuperación de datos. • Plan de continuidad del negocio. • Pruebas y simulacros de incidentes. • Capacitación en seguridad para el personal.

Tabla 2.1 Seguridad de la información en la gestión del laboratorio forense

Investigación y desarrollo: en la era contemporánea, caracterizada por los rápidos avances tecnológicos y el aumento de las ciberamenazas, la gobernanza eficaz de los laboratorios forenses digitales es fundamental para defender la justicia y la seguridad. Las actividades de investigación y desarrollo en este ámbito son fundamental para impulsar el progreso en este campo y abordar los obstáculos emergentes. Los laboratorios forenses digitales se encargan de recuperar, salvaguardar, examinar y presentar pruebas digitales en las investigaciones penales y civiles. La prueba digital, que abarca documentos informáticos, correos electrónicos, comunicaciones de texto, imágenes y vídeos, es cada vez más crucial para la resolución de casos.

Sin embargo, la naturaleza compleja y la abundancia de la información digital plantean distintos desafíos para los laboratorios. La investigación y el desarrollo en la gestión de los Laboratorio Forense Digital tienen como objetivo diseñar me-

todologías, herramientas y enfoques innovadores para mejorar la eficacia, precisión y confiabilidad de los procedimientos forenses digitales (A. H. Di Iorio et al., 2013). A continuación, se describen algunos criterios necesarios para desarrollar de forma eficiente las investigaciones forenses digitales:

- **Permanecer a la vanguardia de los avances tecnológicos:** La rápida evolución de las tecnologías de la información y la comunicación exige que los laboratorios forenses digitales posean herramientas y métodos de última generación para analizar y extraer eficazmente las pruebas de los dispositivos y sistemas nuevos y emergentes.

- **Abordar las nuevas formas de ciberdelitos:** los ciberdelincuentes están ideando constantemente nuevas estrategias para evitar la detección y las consecuencias legales. La investigación y el desarrollo en la gestión de estos son vi-

tales para reconocer y contrarrestar estas nuevas amenazas.

- **Garantizar la admisibilidad de las pruebas digitales en los entornos judiciales:** las pruebas digitales deben acumularse, preservarse y analizarse adecuadamente para ser aceptadas en los tribunales. La investigación y el desarrollo en la gestión de estos ayudan a establecer principios y protocolos forenses sólidos que garanticen la autenticidad y la fiabilidad de las pruebas digitales.

- **Racionalización de los recursos y mejora de la eficiencia:** la investigación y el desarrollo en la gestión de los laboratorios forense Digital pueden resultar en la creación de herramientas automatizadas y procedimientos simplificados que ahorren tiempo y recursos para los laboratorios forenses digitales (Lerena et al., 2018). La Tabla 2.2, muestra las áreas de investigación y desarrollo relacionadas con su aplicabilidad en el laboratorio forense digital durante investigación de delitos o incidentes de ciberseguridad.



Área de investigación y desarrollo	Descripción
Automatización y Robótica	• Desarrollo de herramientas automatizadas para la adquisición, análisis y presentación de evidencia digital. • Implementación de sistemas robóticos para la manipulación segura y eficiente de dispositivos electrónicos y medios de almacenamiento.
Inteligencia Artificial y Aprendizaje Automático	• Aplicación de técnicas de IA y AA para el análisis de grandes volúmenes de datos digitales. • Desarrollo de sistemas de IA para la detección automática de programa maligno, intrusiones en redes y otras amenazas cibernéticas.
Análisis Forense en la Nube	• Investigaciones sobre técnicas y herramientas para la extracción y análisis de datos de entornos de computación en la nube. • Desarrollo de metodologías para la preservación de la cadena de custodia en entornos de nube.
Análisis Forense de Dispositivos Móviles	• Investigaciones sobre técnicas y herramientas para la extracción y análisis de datos de dispositivos móviles. • Desarrollo de métodos para la recuperación de datos borrados o fragmentados en dispositivos móviles.
Análisis Forense de Big Data	• Investigaciones sobre técnicas para el análisis de grandes volúmenes de datos digitales. • Desarrollo de herramientas para la visualización y correlación de datos forenses de big data.
Ciberseguridad y Protección de Datos	• Investigaciones sobre técnicas para la protección de la confidencialidad e integridad de la evidencia digital.

Tabla 2.2 Gestión del laboratorio forense digital en el área de investigación y desarrollo

2.3 Herramientas de hardware y software para un laboratorio forense digital

Las herramientas de hardware y software de un laboratorio forense digital abarcan los dispositivos y programas empleados para la adquisición, el examen y la demostración de pruebas digitales. Estas herramientas permiten a los profesionales de la ciencia forense digital analizar los delitos relacionados con la informática, recuperar los datos borrados y evaluar las operaciones dentro de los sistemas y redes informáticos (Rivetti et al., 2016).

Figura 2.1

Laboratorio informático forense de una empresa privada

Fuente: <http://hard2bit.com>



Equipos de Hardware:

- Computadoras Poderosas
- Almacenamiento Externo Amplio
- Guardianes del Tráfico de Red
- Protectores de Datos
- Estaciones de Trabajo Forenses Especializadas
- Capturadores de Tráfico de Red en Tiempo Real
- Documentación Fotográfica de la Escena del Crimen

Equipos del Software:

- EnCase Forensic
- FTK (Forensic Toolkit)
- Autopsy/Sleuth Kit
- Wireshark
- Volatility
- X-Ways Forensics
- OSForensics

A continuación, en las tablas 2.3 y 2.4, se describen algunas de las herramientas de hardware y software forense que pueden utilizarse durante el proceso de investigación digital.

Funcionalidad	Softwares Forenses							
	Encase	Deft Extra	Caine	Digital Forensics Framework	Forensics Toolkit	Easy Recovery Professional	Fox	Chrome Analysis
Clonación de discos	x	x			x			
Comprobar integridad criptográfica	x	x		x	x			
Información del sistema	x	x	x		x			
Adquisición en vivo	x	x	x		x			
Recuperación de contraseñas	x	x	x		x			
Recuperación de archivos borrados	x			x	x	x		
Recuperación de emails borrados	x				x			
Análisis forense en redes	x	x	x					
Análisis forense en navegadores	x	x	x				x	x
Análisis de dispositivos móviles	x			x			x	
Análisis de firmas de archivos	x							
Búsqueda de archivos	x	x			x			
Utilitarios extras		x	x					
Reporte manual		x						
Reporte automático	x				x			
Volcado de memoria RAM			x					
Adquisición de evidencia RAM	x							
Herramientas de automatización	x							

Tabla 2.3 Descripción comparativa de software forense

Montaje y virtualización de unidades	
ImDisk	Controlador de disco virtual. Versión actual 2.0.9 16 diciembre 2015 http://www.ltr-data.se/opencode.html
OsfMount	Montar imágenes de discos locales en Windows Versión 1.5.1015 7 febrero de 2014 http://www.osforensics.com/tools/mount-disk-images.html#downloadosfm-32

FTK Imager	Montar imágenes de discos, volcado de memoria, entre otras funciones. Versión 3.4.2 23 febrero de 2016 http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.4.2
LiveView	Crear una máquina virtual VMware de la imagen del disco Versión 07b http://liveview.sourceforge.net/
MountImagePro	Montar imágenes de discos locales en Windows Versión v6.1.3.1626 http://www.mountimage.com/
Raw2vmdk	Permite montar raw disk image creados por “dd” usa VMware Versión 0.1.3.1 https://sourceforge.net/projects/raw2vmdk/
Análisis y adquisición de la memoria	
Dumplt	Vuelca el contenido de la memoria a un fichero Versión 2.0 http://www.moonsols.com/windows-memory-toolkit/
Process Dumper	Convierte un proceso de la memoria a fichero Versión 1.1 14 de julio de 2006 http://www.trapkit.de/research/forensic/pd/
Responder CE	Captura y analiza el contenido de la memoria Versión Pro trial 30 días http://www.countertack.com/
RedLine	Entorno gráfico para capturar y analizar la memoria Versión 1.14 de 12 de junio de 2015 https://www.fireeye.com/services/freeware/redline.html
Memorize	Captura la memoria en entorno Windows y OSX Versión 3.0 de 23 de julio 2013 https://www.fireeye.com/services/freeware/memorize.html
Volatility	Extrae y analiza los procesos para su análisis Versión Volatile Systems - Volatility Framework v1.3 https://www.securitybydefault.com/2013/07/analisis-forense-en-linux-analizando-la.html

Tabla 2.4 Herramientas portables para análisis forense digital

2.4 Normas y recomendaciones aplicables para un laboratorio forense digital

En el ámbito de la investigación forense digital, el cumplimiento estricto de los protocolos y directrices estandarizados es esencial para mantener la excelencia, la confiabilidad y la autenticidad de los procedimientos, resultados y pruebas digitales. Estas directrices establecen una base para las actividades de laboratorio, que abarcan la recopilación y el mantenimiento de pruebas para el escrutinio y la demostración de los descubrimientos en un entorno legal. A continuación, se describen algunos de los estándares internacionales más reconocidos:

- La ISO/IEC 17025 es una norma internacional que se refiere a la acreditación de los laboratorios de pruebas y calibración. Establece los criterios generales de competencia técnica y control de calidad en los laboratorios forenses digitales (Chouliaras, n.d.).y
- La Norma ISO/IEC 27041 ofrece recomendaciones para mantener la integridad de la cadena de custodia y la confiabilidad de las pruebas electrónicas en el contexto de las investigaciones forenses (Semprini, 2016).
- La ISO/IEC 27001 Seguridad de la información, esta norma proporciona un marco para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI). La aplicación de ISO/IEC 27001 en un laboratorio forense digital ayuda a proteger la confidencialidad, integridad y disponibilidad de la información sensible, incluyendo la evidencia digital (Universitat Politècnica de València, 2014).

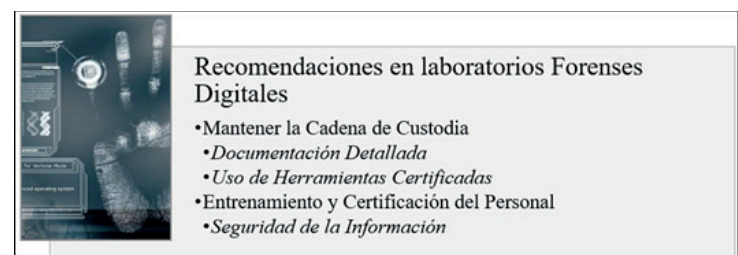
La promulgación de normas y recomendaciones específicas a nivel nacional es imperativa para garantizar la integridad, validez y admisibilidad de las pruebas digitales en los procedimientos legales. Diversas entidades nacionales, como el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos y organizaciones profesionales como la Asociación de Investigación Criminal de Alta Tecnología (HTCIA), han formulado directrices y han sugerido protocolos para la recopilación, el examen y la conservación de las

pruebas digitales. Estos criterios garantizan que los laboratorios forenses digitales funcionen con los más altos estándares de precisión técnica y ética, lo que aumenta la confianza en los hallazgos obtenidos durante las investigaciones

- NIST SP 800-57 Pt 1 Rev. 4: guía del Instituto Nacional de Estándares y Tecnología (NIST) para la gestión de medios digitales con fines forenses, que proporciona recomendaciones sobre la Cadena de Custodia, la preservación de la evidencia y el control de calidad.
- HTCIA recomendaciones y mejores prácticas: la Asociación de Investigación de Delitos de Alta Tecnología ofrece recomendaciones y mejores prácticas formuladas por especialistas en la materia. Estas directrices abarcan diferentes aspectos de la investigación forense digital, desde la recopilación de pruebas hasta la presentación de las conclusiones en un entorno legal.

Recomendaciones generales para utilizar los laboratorios forenses digitales. - Los laboratorios forenses digitales son cruciales para garantizar la integridad, la seguridad y la autenticidad de las pruebas digitales durante el procedimiento de investigación. El espectro de estos protocolos varía desde la recopilación y el mantenimiento precisos de las pruebas hasta su examen y exhibición en entornos judiciales. La adopción de estas sugerencias no solo mejora la confiabilidad de los hallazgos forenses, sino que también garantiza que los protocolos cumplan con los criterios éticos y técnicos reconocidos a nivel mundial.

Figura 2.2 Recomendaciones generales en laboratorios forenses digitales



2.5 Cuestionario de autoevaluación

1. **¿Cuáles son las áreas de aplicación de un laboratorio forense digital?**
 - a. Mantenimiento de dispositivos electrónicos.
 - b. Distribución de software.
 - c. Investigación de delitos cibernéticos.
 - d. Almacenamiento de datos.
2. **¿Cuáles son los beneficios de implementar un laboratorio forense digital?**
 - a. Mejora de la investigación forense.
 - b. Ahorro de tiempo.
 - c. Protección de la evidencia digital.
 - d. Eliminación de errores humanos.
3. **¿Cuáles son los métodos empleados en la adquisición de pruebas digitales?**
 - a. Haga caso omiso de los metadatos asociados a los archivos digitales.
 - b. Simplemente duplique los archivos del dispositivo correspondiente.
 - c. Realice procedimientos forenses de adquisición de imágenes.
 - d. Emplee software de recuperación de datos no forenses.
4. **¿Cuáles son los pasos en el análisis de la evidencia digital?**
 - a. Abstenerse de generar una representación binaria del dispositivo electrónico.
 - b. Realice un examen exhaustivo de los metadatos asociados a la evidencia digital.
 - c. Evalúe la evidencia digital en el propio dispositivo principal.
 - d. Emplee el software forense adecuado para analizar las pruebas digitales.
5. **¿Cuáles son los pasos clave para la implementación de un laboratorio forense digital?**
 - a. Obtener software y hardware forense en ausencia de una planificación estratégica exhaustiva.
 - b. Establecer objetivos inequívocos y delinee la extensión del laboratorio.
 - c. Dejar de instituir protocolos y metodologías.
 - d. Reclutar personal que carezca de la formación suficiente.
6. **¿Qué es la cadena de custodia de la evidencia digital y por qué es importante?**
 - a. Es una cuenta bien documentada que monitorea la transferencia y el manejo de la evidencia digital desde su detección inicial hasta su eliminación final.
 - b. Este procedimiento es exclusivo de las pruebas tangibles
 - c. Constituyen un registro de posesión de pruebas digitales.
 - d. La importancia de esto radica en el valor económico de las pruebas.
7. **¿Por qué es importante la capacitación continua para los profesionales de laboratorios forenses digitales?**
 - a. Para reducir costos operativos.
 - b. Para mantenerse actualizado con las últimas tecnologías y técnicas forenses.
 - c. Para aumentar la carga de trabajo.
 - d. Para disminuir la calidad de las investigaciones.
8. **¿Qué medidas de seguridad son esenciales en un laboratorio forense digital para proteger la integridad de las pruebas?**
 - a. Acceso público a las instalaciones.
 - b. Cifrado de datos sensibles.
 - c. Uso de software desactualizado.
 - d. Compartir contraseñas entre el personal.
9. **¿Cómo se preserva la evidencia digital?**
 - a. Produzca una representación binaria del aparato

- electrónico.
 - b. Documente sistemáticamente el linaje de la evidencia digital.
 - c. Apague la herramienta electrónica en el sitio de la prueba digital.
 - d. Replique los datos del examen digital en una unidad externa sin tener en cuenta el cumplimiento de los protocolos de cadena de custodia.
10. **¿Cómo se documentan y presentan los resultados del análisis de la evidencia digital?**
- a. No incorpore puntos de vista o análisis subjetivos en el informe de resultados.
 - b. Absténgase de especificar las herramientas y metodologías empleadas en el examen.
 - c. Entregue los resultados del escrutinio de la evidencia digital de forma exclusivamente verbal.
 - d. Emplee una estructura estandarizada para registrar los hallazgos del análisis de la evidencia digital.
11. **¿Qué es un laboratorio forense digital?**
- a. Un laboratorio forense digital es una instalación establecida para investigar la biodiversidad de los ecosistemas digitales.
 - b. Se trata de una instalación donde se llevan a cabo investigaciones para desarrollar dispositivos tecnológicos de última generación.
 - c. Un laboratorio forense digital es un establecimiento donde se realizan exámenes de datos para pronosticar las condiciones atmosféricas y los eventos ecológicos.
 - d. Un laboratorio forense digital es una institución que se centra en la adquisición, retención y examen de pruebas digitales para asuntos judiciales, en particular.
12. **¿Cuál es la función principal del software de adquisición de imágenes en la investigación forense digital?**
- a. Facilitar la edición de imágenes digitales.
 - b. Crear copias exactas de dispositivos de almacenamiento para su análisis.
 - c. Mejorar la calidad de las imágenes digitales.
 - d. Ayudar en la creación de gráficos y diagramas forenses.
13. **¿Qué características debe tener un informe forense digital para ser considerado válido en un proceso judicial?**
- a. Incluir opiniones subjetivas sobre la evidencia en contrada.
 - b. Ser breve y generalizado sin detalles técnicos.
 - c. Ser detallado, verificable y basarse en procedimientos forenses aceptados.
 - d. Omitir la metodología utilizada para el análisis.
14. **¿Cuál es el rol de los protocolos de validación en el uso de herramientas forenses digitales?**
- a. Reducir la necesidad de capacitación especializada.
 - b. Garantizar que las herramientas funcionen correctamente y de manera consistente.
 - c. Simplificar el análisis al eliminar la necesidad de herramientas adicionales.
 - d. Permitir la modificación ad hoc de los procedimientos de análisis.
15. **¿Qué es el hashing y cuál es su función en la investigación forense digital?**
- a. Un método de compresión de datos para ahorrar espacio de almacenamiento.
 - b. Un proceso para cifrar archivos y proteger su contenido.
 - c. Un procedimiento para generar un valor único que verifica la integridad de los datos.
 - d. Una técnica para convertir datos en gráficos visuales para análisis rápido.

- 
- 
- 3.1 Definición y tipos de discos duros
 - 3.2 Tipos de sistemas de archivos
 - 3.3 Importancia de los metadatos en la investigación forense digital
 - 3.4 Práctica 1. Extracción y análisis de evidencia contenida en discos duros
 - 3.5 Práctica 2. Análisis y recuperación de archivos con data carving
 - 3.6 Práctica 3. Extracción de la base de datos de una red social almacenada en un dispositivo móvil
 - 3.7 Cuestionario de autoevaluación

3.1 Definición y tipos de discos duros

El disco duro es un componente esencial de una computadora que almacena datos a largo plazo. Además de almacenar archivos personales, el disco duro también contiene el sistema operativo de la computadora, junto con otros programas fundamentales para su funcionamiento, como controladores y marcos de trabajo. La capacidad de un disco duro se mide en megabytes, gigabytes y terabytes, lo que determina cuantos datos puede almacenar. Cuanto mayor sea la capacidad, más archivos podrá guardar. Es importante distinguir entre un disco duro y la memoria RAM (memoria de acceso aleatorio). Mientras que el disco duro almacena datos a largo plazo, la RAM es un tipo de almacenamiento temporal que se utiliza para cargar y ejecutar programas y datos mientras la computadora está encendida. La memoria RAM es temporal, lo que implica que pierde la información almacenada cuando el dispositivo se apaga o reinicia. Se utiliza principalmente para realizar tareas y cambiar entre aplicaciones de manera eficiente, permitiendo trabajar sin problemas, y sin perder el proceso (Dropbox, n.d.). A continuación, se describen los diferentes tipos de discos duros que existen en el mercado:

- **Disco duro (HDD):** son los más comunes y emplean discos magnéticos en rotación para almacenar datos. La lectura y escritura se realizan mediante cabezales móviles que se desplazan sobre los discos. Aunque ofrecen una alta capacidad de almacenamiento a un precio accesible, son más lentos que las unidades de estado sólido (SSD) y pueden ser más propensos a sufrir daños mecánicos debido a sus componentes móviles (Geeksforgeeks, 2020). Algunas de sus características son:

- Utiliza tecnología magnética.
- Tienen partes mecánicas móviles.
- Mayor capacidad de almacenamiento en comparación con la SSD por un costo más bajo.
- **Unidad de disco sólido (SSD):** las SSD utilizan memoria flash NAND para almacenar datos de forma permanente. No tienen partes móviles, lo que las hace más rápidas, silenciosas y duraderas que los HDD. Aunque tienden a ser caras por capacidad de almacenamiento que los HDD. Muchas personas aprecian su velocidad y confiabilidad, especialmente en dispositivos como laptops y computadoras de escritorio de alto rendimiento (Geeksforgeeks, 2024). Entre sus características tenemos:
 - Utilizan memorias flash NAND.
 - No tienen partes móviles.
 - Más rápidas y eficientes en términos de energía que los HDD.
- **Unidad de estado sólido híbridas (SSHD):** estas unidades cambian características de los HDD y las SSD. Integrado como cache para almacenar datos comúnmente utilizados y optimizar el rendimiento, mientras que la mayoría del almacenamiento se basa en discos magnéticos. Esto proporciona un equilibrio entre la capacidad de almacenamiento y el rendimiento, ofreciendo velocidades de acceso más rápido para ciertos archivos mientras una gran capacidad de almacenamiento a un costo más bajo que una SSD pura (Unitel, 2021). A continuación, se describen sus características son:

- Combinan tecnologías de HDD y SSD
- Tienen una pequeña cantidad de memoria flash NAND como cache.
- Ofrecen un equilibrio entre capacidad de almacenamiento y rendimiento.

3.2 Tipos de sistema de archivos

Sistema de archivos. - Los sistemas de archivos son componentes del sistema operativo que gestionan la y el almacenamiento de datos en las unidades de almacenamiento, como discos duros, unidades USB y tarjetas SD. Funcionan como bibliotecarios que organizan los datos en la unidad, asignan espacio para archivos, registran su ubicación física y facilitan un acceso eficiente a los mismos. Cada sistema de archivos tiene sus propias características, ventajas y limitaciones, lo que significa que la elección del sistema de archivo adecuado depende del dispositivo utilizado, su uso previsto y la compatibilidad con diferentes sistemas operativos (Kingston, 2023). A continuación, se describen los sistemas de archivos más utilizados:

- **FAT32 (file allocation table):** desarrollado por Microsoft e introducido con Windows 95B en 1995, es una evolución de los sistemas FAT12 y FAT16. Estos sistemas de archivos, con un ancho de datos de 32 bits, permite la lectura y escritura de datos en una amplia variedad de dispositivos y sistemas operativos, incluidos ordenadores Apple y consolas de videojuegos. Aunque sigue siendo común en dispositivos de almacenamiento extraíbles con USB y tarjetas de memoria debido a su amplia compatibilidad, FAT32 tiene limitaciones en cuanto al tamaño máximo de archivos y particiones (Iosnos, 2020).
- **EXFAT (extended file allocation table):** usa actualización de FAT32 introducida por Microsoft para eliminar la limitación de 4 GB. Compatible con Windows, macOS y algunas distribuciones de GNU/Linux en versión más recientes.

- **NTFS (new technology file sustem):** promovido por Microsoft como alternativa a FAT32, sin los límites de tamaño. Utilizado por defecto en sistemas Windows, pero la compatibilidad con otros sistemas operativos puede ser limitada.
- **HFS+ (hierarchinal file system plus):** desarrollado por Apple para sus dispositivos, pero con compatibilidad limitada fuera del ecosistema de Apple, GNU/Linux puede trabajar con él sin problema, en Windows solo podrá leer el contenido de los discos formateados con él, pero no escribir en ellos.
- **APFS (apple file system):** es el Sistema de archive diseñado por Apple como sucesor del HFS+ e introdujo por primera vez con IOS 10.3. Este sistema está optimizado para dispositivos que usan memorias de estado sólido. Está diseñado para ofrecer un rendimiento óptimo y una mayor eficiencia en dispositivos que utiliza tecnología de almacenamiento flash, lo que incluye una mayor velocidad de lectura y escritura, mejor gestión del espacio y una mayor durabilidad en los datos (Apple, 2021).

A continuación, en la Tabla 3.1 se muestra una comparación de los diferentes sistemas de archivos según las capacidades descritas de acuerdo con su tamaño máximo de volumen y tamaño máximo de archivo.

Sistema de archivo	Tamaño máximo de volumen	Tamaño máximo de archivo
FAT32	8 tb	4
NTFS	16 eib (1,845^7 tb)	16 eib (1,845^7 tb) teóricos en la práctica, alrededor de 256 tb
EXFAT	16 eib (1,845^7 tb)	64 zib (6,4^10 tb)
HFS+	8 eib (9,223^6 tb)	8 eib (9,223^6 tb)
APFS	8 eib (9,223^6 tb)	16 eib (1,845^7 tb)
EXT4	1 eib (1,153^6 tb)	16 tib (17,5921 tb)

Tabla 3.1 Comparación de los sistemas de archivos según su tamaño máximo de volumen y tamaño máximo de archivo

A continuación, la Tabla 3.2 muestra la compatibilidad de los sistemas de archivos con las diferentes plataformas de sistemas operativos.

Sistema de archivos	Windows 8/10	macOS (10.6.5 o posterior)	GNU/Linux		IOS 11 en adelante	Ps4/Ps5	Xbox
FAT32	si	Si	si	Si	No	Si	Si
NTFS	si	Con apps de terceros	Si, aunque puede necesitar drivers	No	No	No	Si
EXFAT	si	Si	Si, aunque puede necesitar drivers	Si	No	Si	Si
HFS+	Con apps de terceros	Si	si	No	No	No	Si
APFS	Con apps de terceros	Si, con macOS 10.13 o posterior	No inicialmente, Aunque hay drivers para intentarlo	no	si	no	no
EXT4	Con apps de terceros	Con apps de terceros	si	no	no	no	Si

Tabla 3.2 Compatibilidad de sistemas de archivos con plataformas de sistemas operativas

3.3 Importancia de los metadatos en la investigación forense digital

Los metadatos son datos que describen otros datos, proporcionando información sobre el origen, la creación, el contenido y las características de un archivo digital. En el caso de las imágenes digitales, los metadatos pueden incluir detalles como la fecha y hora de la captura, el modelo de la cámara, la ubicación geográfica y el autor. Son fundamentales para determinar la autenticidad, la integridad y la procedencia de una imagen digital, lo que puede ser crucial para su valor probatorio en un juicio. Los metadatos deben analizarse con otros elementos de la imagen y complementarse con técnicas forenses para garantizar su validez y confiabilidad como evidencia en un proceso legal.

Los metadatos juegan un papel crucial en la investigación forense al proporcionar información detallada sobre los archivos digitales, incluyendo su contenido y el contexto en el que

se crearon o se almacenaron. Estos datos pueden ser especialmente relevantes en el análisis de archivos multimedia y de oficina, permitiendo a los peritos determinar la autenticidad e integridad de los archivos bajo escrutinio. Los metadatos no son una prueba infalible, ya que pueden manipularse o contaminarse fácilmente.

Para garantizar la fiabilidad de los metadatos en una investigación forense, es fundamental que un perito tecnológico realice la extracción de estos datos con extremo cuidado y atención a los procedimientos técnicos adecuados. Además, los metadatos deben ser evaluados en conjunto con otras evidencias digitales recolectadas durante la investigación, lo que pueden ayudar a corroborar o refutar las conclusiones derivadas de su análisis (Edmonson, 2023) .

3.4 Práctica 1. Extracción y análisis de evidencia contenida en discos duros

El objetivo de esta práctica es facilitar el uso de software especializado para obtener copias o imágenes forenses de las evidencias digitales. A continuación, se describen los recursos requeridos y el procedimiento para generar la imagen forense de un dispositivo de almacenamiento físico.

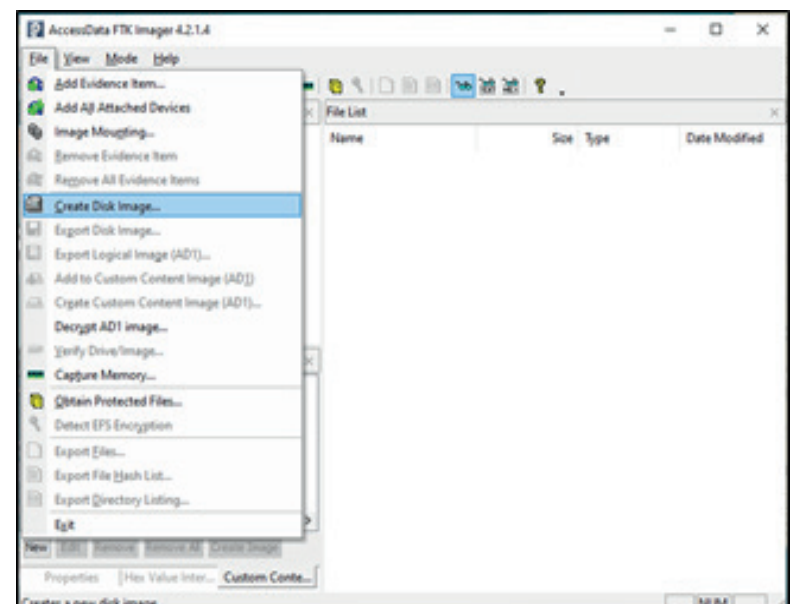
Recursos necesarios:

- Computadora con acceso a internet
- Máquina virtual Oracle VM VirtualBox o VMware Workstation
- Sistemas operativos virtualizados Caine, Santoku.
- Software Access Data FTK Imager, Guymager, Memorize, herramienta Win32dd.exe / win64dd.exe, LiMe.
- Pendrive 2GB o superior
- Dispositivo móvil Android

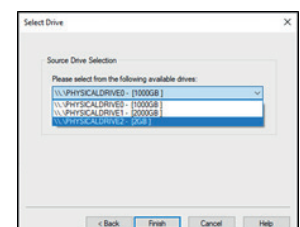
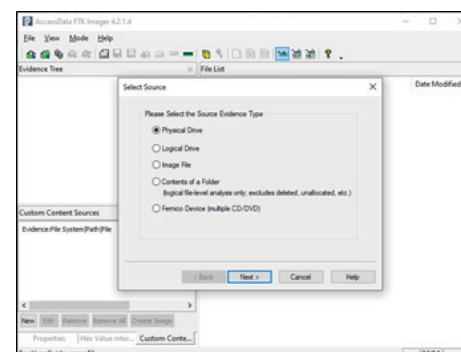
Procedimiento. - Para esta actividad se usará el software Access Data FTK Imager, y luego Guymager. El primero en entorno Windows, y el segundo en entorno Linux. También se requiere del dispositivo de almacenamiento pendrive 2GB o superior.

Primero, se utilizará el software forense **Access Data FTK Imager**.

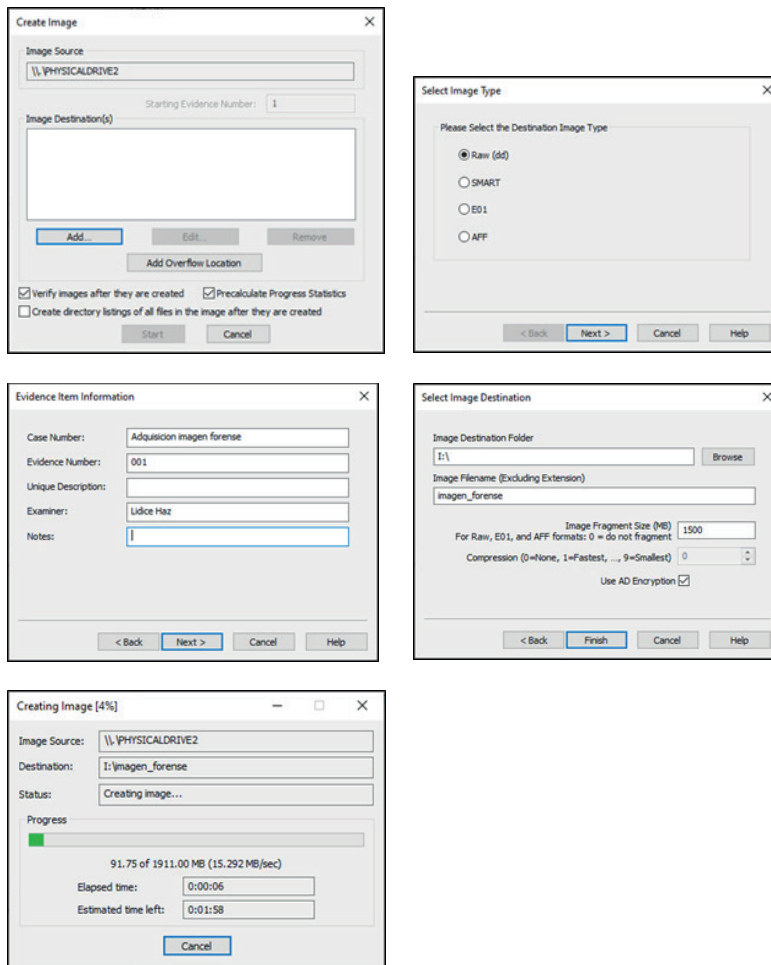
1. Inserte el dispositivo de almacenamiento pendrive en el puerto USB del equipo (evidencia digital).
2. Ejecute el software Access Data FTK Imager como administrador. Seleccione la opción File -> Create Disk Image



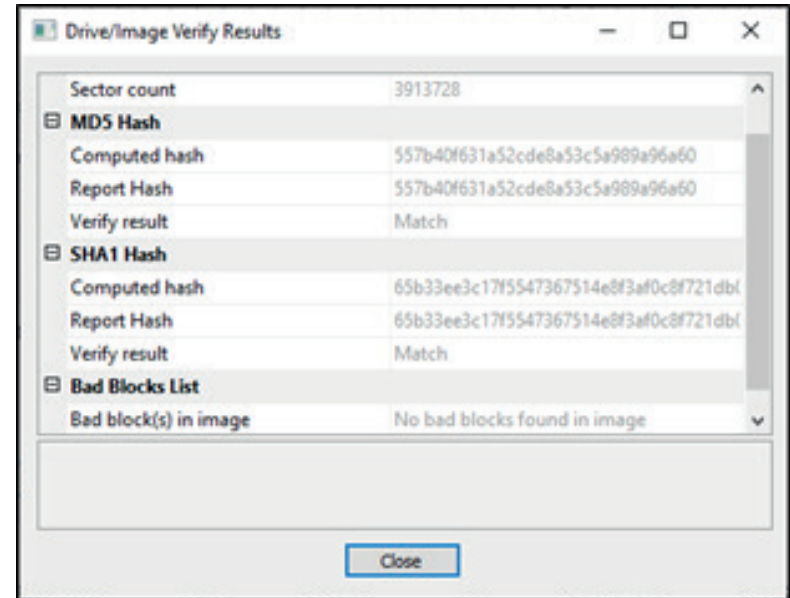
3. Seleccione el origen de los datos que desea extraer como imagen forense. Para el ejemplo, escoja la opción Physical Drive, luego ubique la unidad de almacenamiento pendrive 2GB, y presione el botón Finish.



4. Luego, en la siguiente ventana presione el botón Add, y escoja el tipo de archivo para la imagen forense por defecto se usa el tipo Raw .dd; luego ingresar la información de la evidencia, y por último la ruta de destino donde se guardará la imagen y el nombre del archivo; si se requiere agregar contraseña al archivo se habilita la opción de cifrado y posteriormente el programa le pedirá ingresar la contraseña -para el ejemplo no se usará esa opción-. Clic en Finish para aceptar la información ingresada, y luego clic en Start para que inicie el proceso de copia bit a bit.



5. Proceso concluido con los códigos hash de verificación de la evidencia.



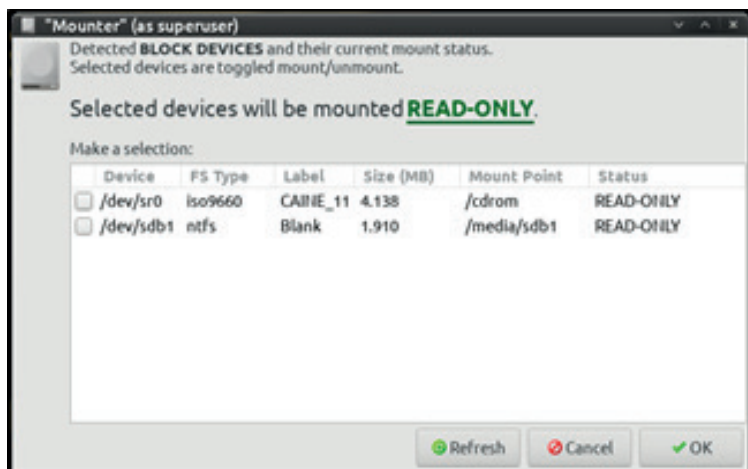
A continuación, se usará **Guymager** desde el sistema operativo Caine:

1. En la máquina virtual inicie el sistema operativo Caine.
2. Inserte el dispositivo de almacenamiento pendrive (evidencia digital) en el puerto USB del equipo anfitrión, y luego habilite el reconocimiento del dispositivo en la máquina virtual. En el sistema operativo Caine no es necesario deshabilitar la lectura de los puertos USB, debido a que el sistema por defecto solo permite la lectura de cualquier medio de almacenamiento.

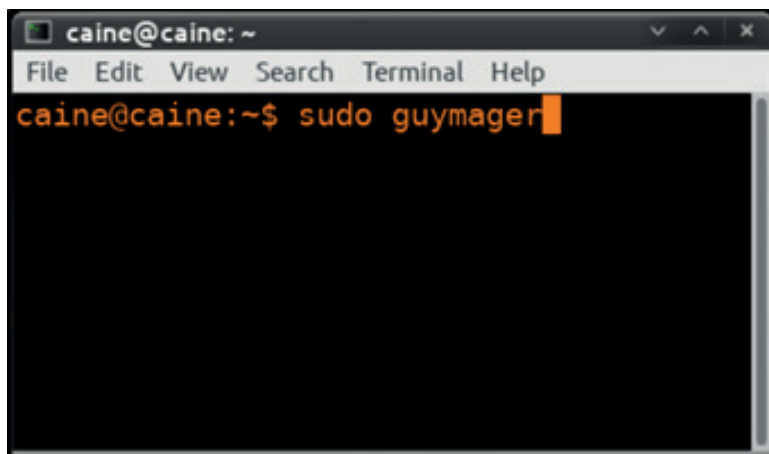


3. En Caine, el software de gestión de dispositivos automáticamente detecta la unidad. Luego habilitar el check de la unidad forense, clic en botón Ok y el sistema procederá a cargar dicha unidad.

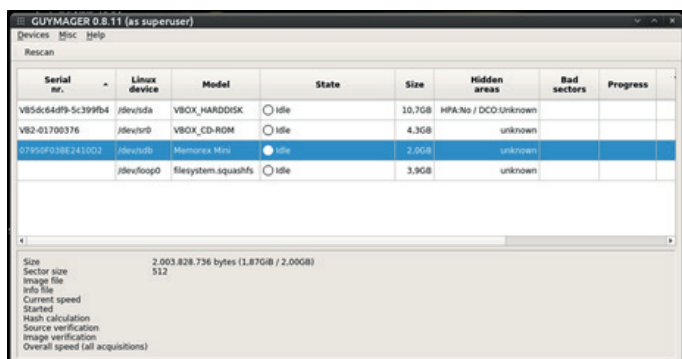
4. La unidad forense ya ha sido cargada y tiene un punto montaje en el sistema Caine.



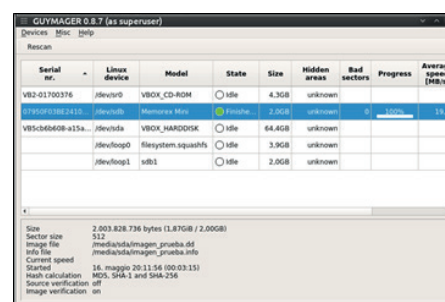
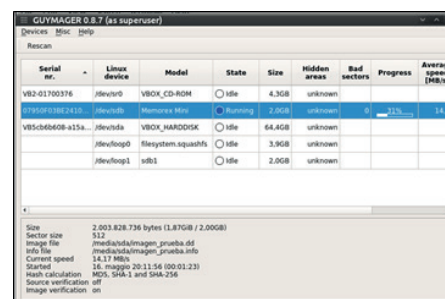
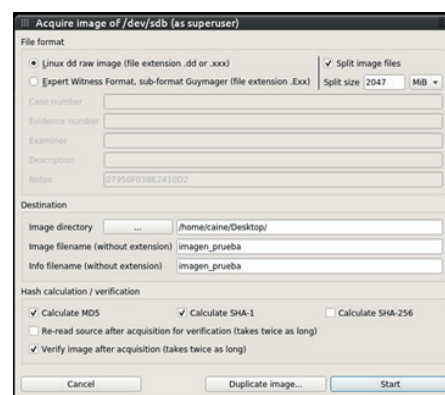
5. A continuación, abrir el software Guymager desde el menú Forensic Tool -> Guymager, ó desde la línea de comandos mediante la instrucción `caine@caine:~$ sudo guymager`



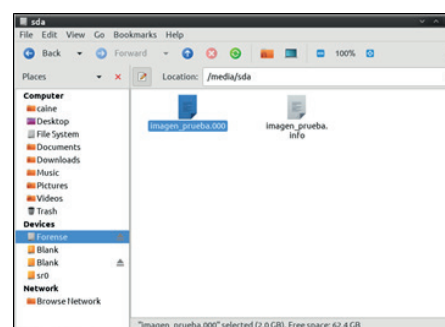
6. Desde la interfaz de Guymager, seleccionar la unidad forense, clic derecho sobre la misma y escoger la opción Acquire image.



7. En la interfaz de Acquire image escoger la opción Linux dd raw image (file extensión .dd or .xxx). Seleccionar el directorio donde se guardará la imagen, y escribir el nombre del archivo. Habilite el cálculo de los hash de verificación. Clic en el botón Start para que inicie el proceso



8. Buscar la ruta donde se grabó la imagen forense. El archivo final tiene extensión .000 para el ejemplo imagen_prueba.000



3.5 Práctica 2. Análisis y recuperación de archivos con data carving

Los objetivos de esta práctica son: (1) analizar la información contenida en una evidencia digital cuyo sistema de archivos haya sido eliminado. (2) Recuperar archivos que han sido eliminados luego de un daño en el sistema de archivos. A continuación, se describen los recursos requeridos, y el procedimiento para recuperar los datos de la evidencia digital.

Recursos necesarios:

- Computadora
- Archivo de evidencia digital
- Sistema operativo Caine
- Software Scalpel
- Archivo de la evidencia digital PracticaCarving.dd

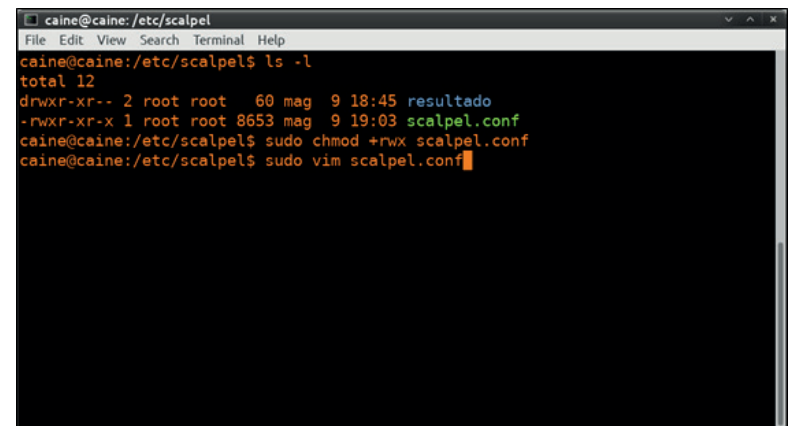
Procedimiento. - Para esta actividad es necesario cargar la evidencia digital en el sistema operativo Caine, para luego recuperar los archivos mediante la herramienta Scalpel.

1. Montar la unidad de almacenamiento que contiene la imagen forense. Para este ejercicio, se utiliza el archivo denominado PracticaCarving.dd, el cual se carga en Caine O.S. Para el ejemplo la unidad montada es Blank.

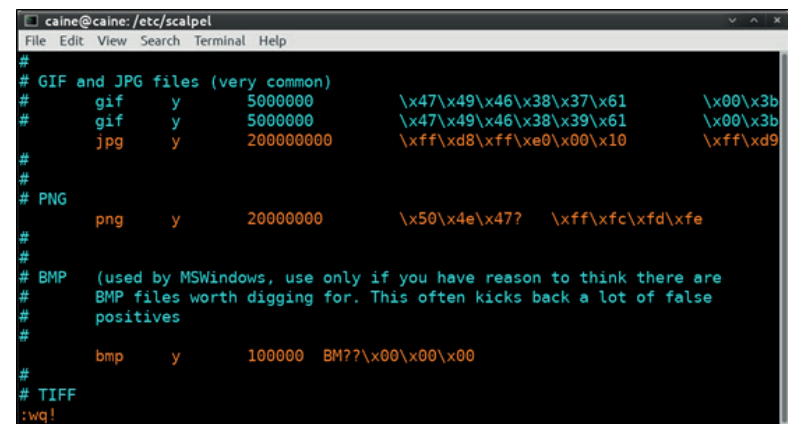


2. Ingrese a la ruta donde se encuentra la herramienta Scalpel digitando la instrucción `caine@caine:~$ cd /etc/scalpel` para verificar el archivo de configuración; luego visualice

el contenido de la carpeta scalpel con la instrucción `caine@caine:/etc/scalpel$ ls -l`. Proceda a modificar los permisos de acceso al archivo `scalpel.conf` para que éste pueda ser modificada por el usuario caine, aplique el comando `caine@caine:/etc/scalpel$ sudo chmod +rwx scalpel.conf`. Luego visualice el archivo digitando `caine@caine:/etc/scalpel$ sudo vim scalpel.conf`



3. Proceda a quitar el comentario para que la herramienta scalpel extraiga los tipos de archivos que presuma se almacene en la imagen forense, al final salga y guarde los cambios del archivo digitando: `wq!`



4. Cargue la imagen forense mediante la instrucción `caine@caine:/etc/scalpel$ sudo scalpel /dev/sdb1 -o resultados`, el contenido de la imagen se almacenará en una carpeta denominada resultados.


```

caine@caine:/etc/scalpel
File Edit View Search Terminal Help
drwxr-xr-- 2 root root 60 mag 9 18:45 resultado
-rwxr-xr-x 1 root root 8653 mag 9 19:03 scalpel.conf
caine@caine:/etc/scalpel$ sudo chmod +rwx scalpel.conf
caine@caine:/etc/scalpel$ sudo vim scalpel.conf
caine@caine:/etc/scalpel$ sudo scalpel /dev/sdb1 -o resultado
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.
ERROR: You have attempted to use a non-empty output directory. In order
to maintain forensic soundness, this is not allowed.
Aborting.

caine@caine:/etc/scalpel$ sudo scalpel /dev/sdb1 -o resultados
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/dev/sdb1"

Image file pass 1/2.
/dev/sdb1: 13.6% |****          | 260.0 MB  06:45 ETA

```

```

root@caine:~
File Edit View Search Terminal Help
Image file pass 2/2.
/dev/sdb1: 100.0% |*****          | 1.9 GB  00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 33, elapsed = 557 seconds.
caine@caine:/etc/scalpel$ cd resultados
bash: cd: resultados: Permission denied
caine@caine:/etc/scalpel$ sudo cd resultados
sudo: cd: command not found
caine@caine:/etc/scalpel$ sudo su -
root@caine:~# chmod +rwx /etc/scalpel/resultados
root@caine:~# ls -l /etc/scalpel/resultados
total 4
-rw-r--r-- 1 root root 2098 mag 9 19:21 audit.txt
drwxr-xr-x 2 root root 420 mag 9 19:21 bmp-2-0
drwxr-xr-x 2 root root 240 mag 9 19:21 jpg-0-0
drwxr-xr-x 2 root root 80 mag 9 19:20 png-1-0
drwxr-xr-x 2 root root 80 mag 9 19:21 tif-3-0
root@caine:~#

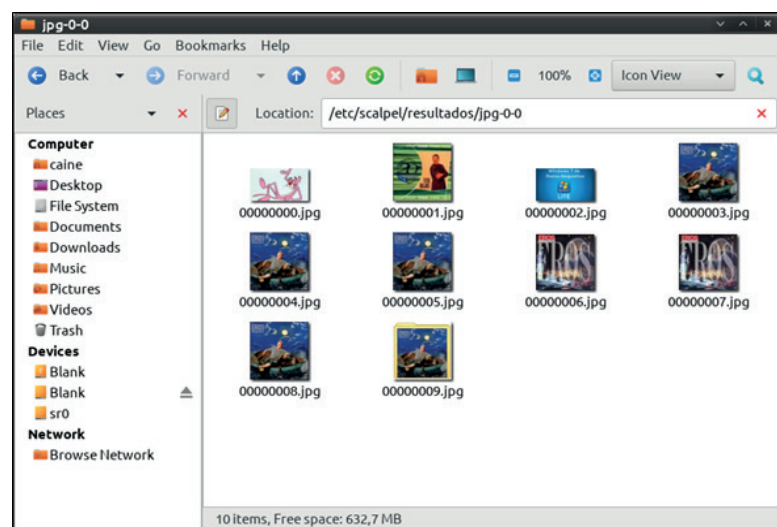
```

```

caine@caine:/etc/scalpel
File Edit View Search Terminal Help
Opening target "/dev/sdb1"

Image file pass 1/2.
/dev/sdb1: 100.0% |*****          | 1.9 GB  00:00 ETA
Allocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built. Workload:
jpg with header "\xff\xd8\xff\xe0\x00\x10" and footer "\xff\xd9" --> 10 files
png with header "\x50\x4e\x47\x3f" and footer "\xff\xfc\xfd\xfe" --> 2 files
bmp with header "\x42\x4d\x3f\x3f\x00\x00\x00" and footer "" --> 19 files
tif with header "\x49\x49\x2a\x00" and footer "" --> 2 files
tif with header "\x4d\x4d\x00\x2a" and footer "" --> 0 files
Carving files from image.
Image file pass 2/2.
/dev/sdb1: 100.0% |*****          | 1.9 GB  00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 33, elapsed = 557 seconds.
caine@caine:/etc/scalpel$

```



5. Para consultar los resultados deberá aplicar permisos de +rwx a la carpeta de resultados obtenido con scalpel. Para esto, debe cambiar su modo de acceso a super administrador digitando la instrucción `caine@caine:/etc/scalpel$ sudo su -`. Luego la instrucción `root@caine:~# chmod +rwx /etc/scalpel/resultados` para modificar los permisos de la carpeta resultados. Luego liste los archivos que han sido extraídos con la herramienta mediante `root@caine:~# ls -l /etc/scalpel/resultados`. Los resultados se presentan clasificados según el tipo de archivo; además se genera el archivo `audit.txt` con el resumen del proceso ejecutado.

```

audit.txt [Read-Only] (/etc/scalpel/resultados) - Pluma
File Edit View Search Tools Documents Help
+ Open Save Undo
audit.txt x
2 Scalpel version 1.60 audit file
3 Started at Sat May 9 19:11:44 2020
4 Command line:
5 scalpel /dev/sdb1 -o resultados
6
7 Output directory: /etc/scalpel/resultados
8 Configuration file: /etc/scalpel/scalpel.conf
9
10 Opening target "(null)"
11
12 The following files were carved:
13 File Start Chop Length Extracted From
14 00000002.jpg 6119424 NO 73500 sdb1
15 00000001.jpg 5849088 NO 2961 sdb1
16 00000000.jpg 5804032 NO 35720 sdb1
17 00000013.bmp 295220486 YES 100000 sdb1
18 00000012.bmp 295220342 YES 100000 sdb1
19 00000015.bmp 332069802 YES 100000 sdb1
20 00000014.bmp 332069658 YES 100000 sdb1
21 00000016.bmp 622065805 YES 100000 sdb1

```

3.6 Práctica 3. Extracción de la base de datos de una red social almacenada en un dispositivo móvil

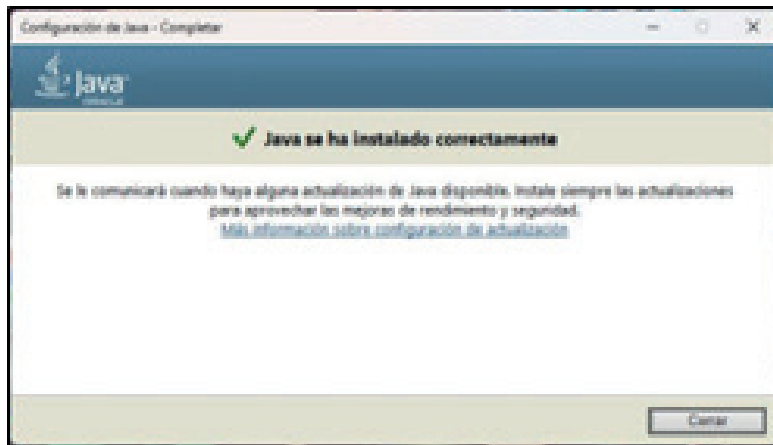
El objetivo de esta práctica es usar software especializado para extraer y analizar la base de datos de una red social almacenada en un dispositivo móvil. A continuación, se describen los recursos requeridos y el procedimiento para generar la extracción, lectura y análisis.

Recursos necesarios:

- Computadora con acceso a internet
- Máquina virtual Oracle VM VirtualBox o VMware Workstation
- Sistemas operativos virtualizados Caine, Windows
- Software ADEL, JAVA
- Dispositivo móvil Android

Procedimiento. - Para esta actividad se extraerá la base de datos de WhatsApp en un dispositivo con plataforma Android.

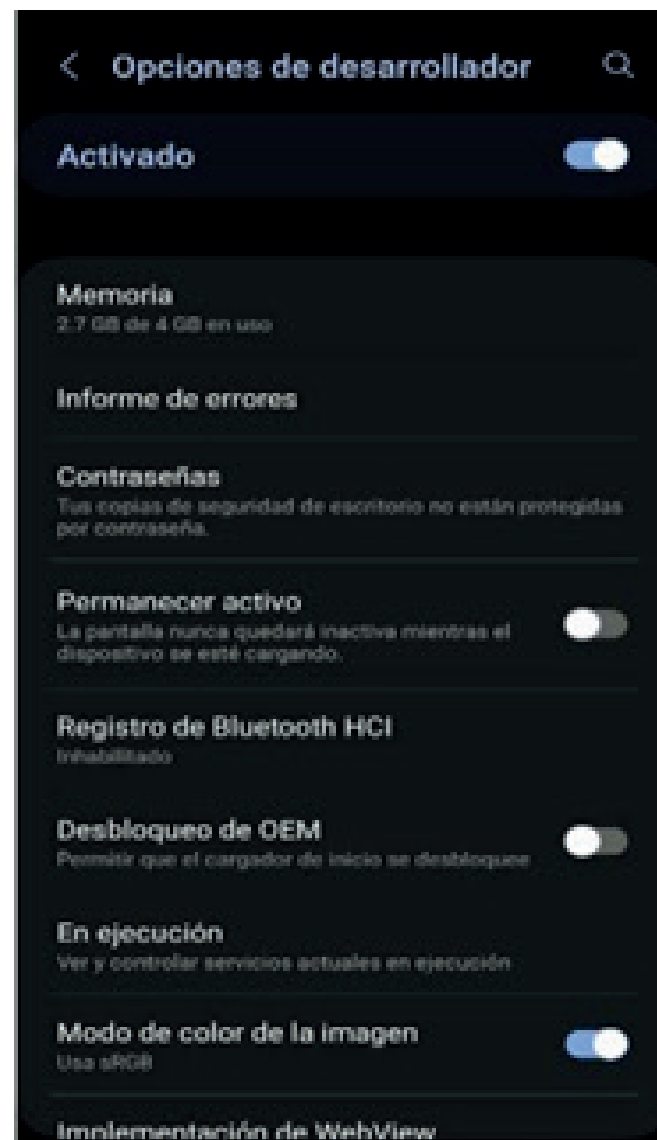
1. Primero, se debe instalar la máquina virtual de JAVA en el sistema Windows como requisito previo. Luego, instalar el programa Android Data Extractor Lite (ADEL) para obtener la base de datos de WhatsApp de un dispositivo Android.



2. Verificar, si es necesario instalar Controladores ADB; ya que, algunos dispositivos no permiten comunicarse con el

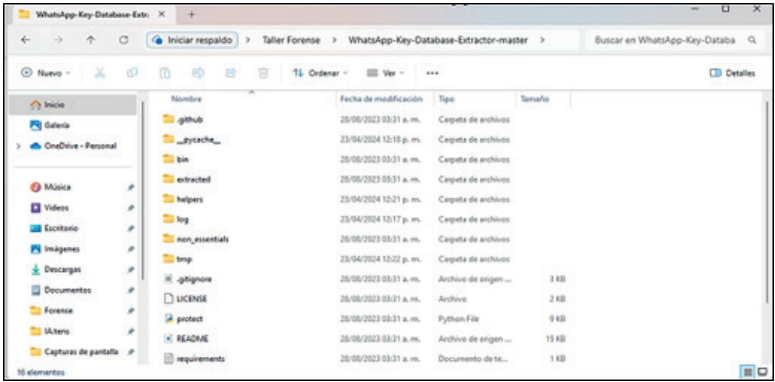
ordenador a través del cable USB activando el modo depurador USB, caso contrario omitir este paso.

3. Luego, active el modo depurador USB en el dispositivo usado en la práctica.

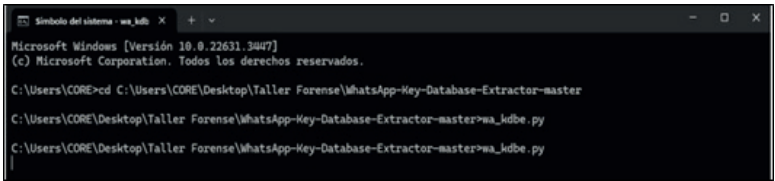


El dispositivo utilizado en este ejemplo es Samsung Galaxy A03 SM-A037M/DS con versión de Android 13.

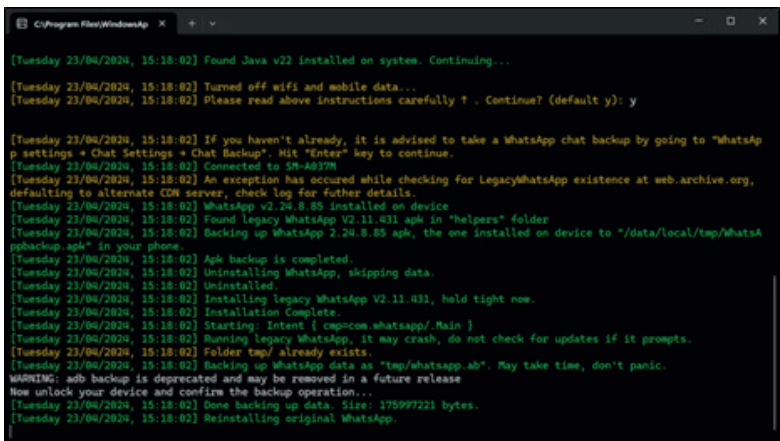
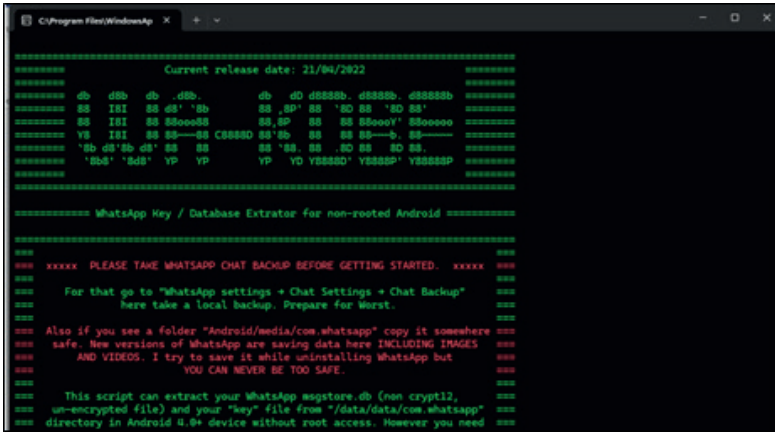
4. Descargar WhatsApp-Key-Database-Extractor del repositorio de GitHub para realizar la extracción de la base de datos de nuestro WhatsApp.



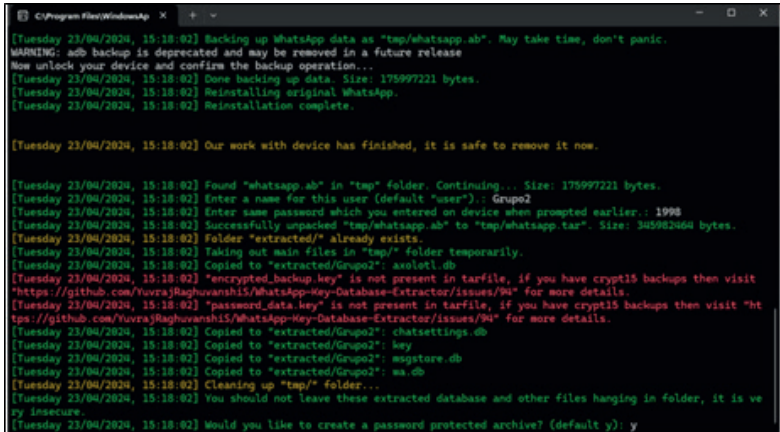
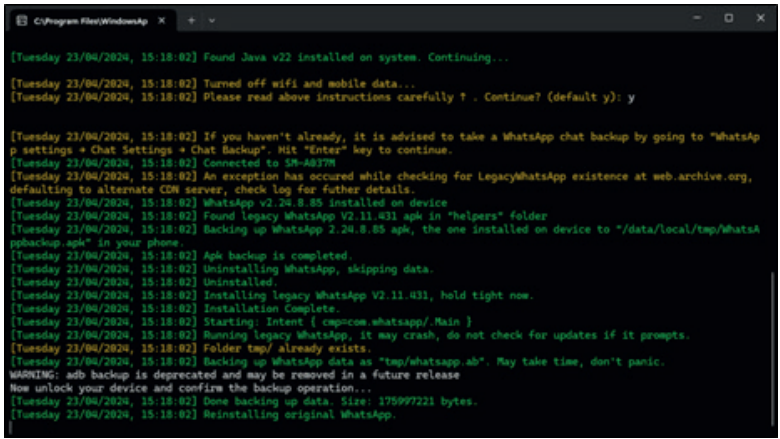
5. Una vez realizado, se procede a cambiar de directorio en el cmd, primero hacia el escritorio y luego a la carpeta \WhatsApp-Key-Database-Extractor-master



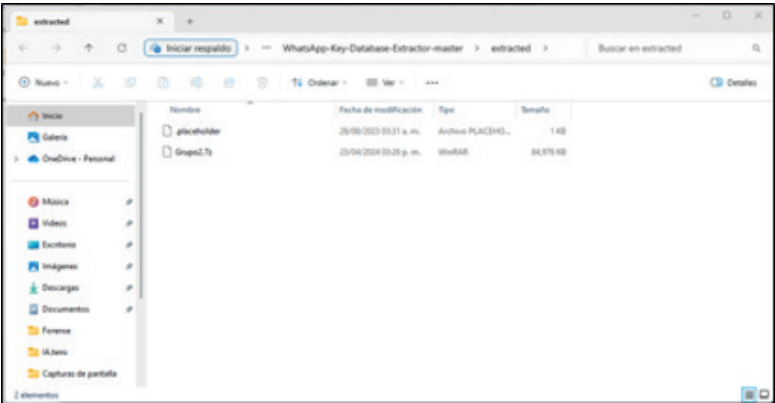
6. Luego, en la carpeta se ejecuta el programa wa_kdbe.py con el teléfono conectado al equipo para proceder con la extracción de la base de datos.



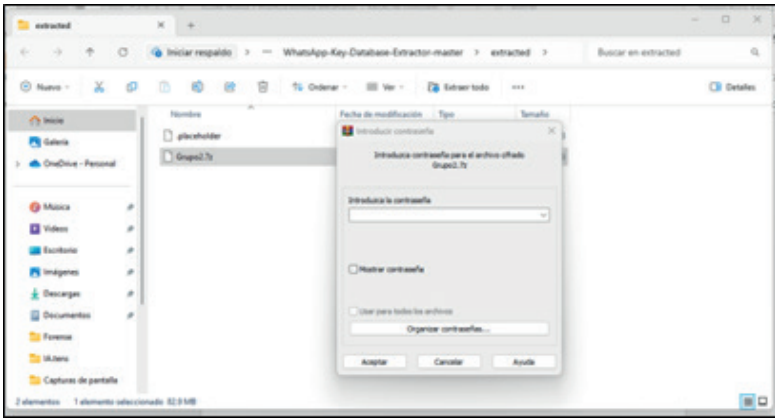
7. Se asigna un nombre a la carpeta.



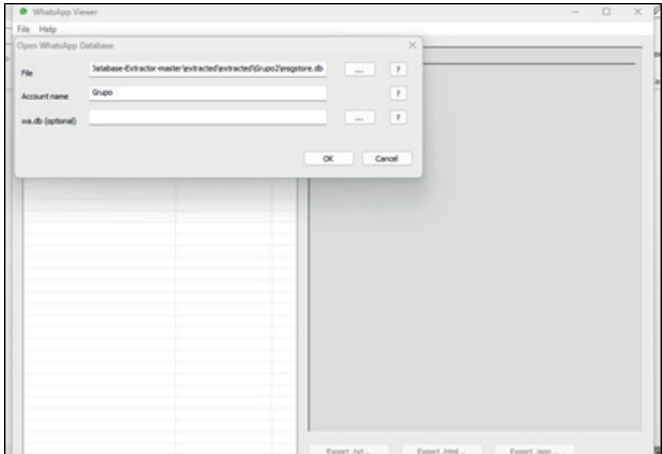
8. Una vez terminado el proceso se crea una carpeta automáticamente, la cual contiene toda la información de la base de datos de WhatsApp.



9. Para realizar la extracción se ingresa con la contraseña asignada.



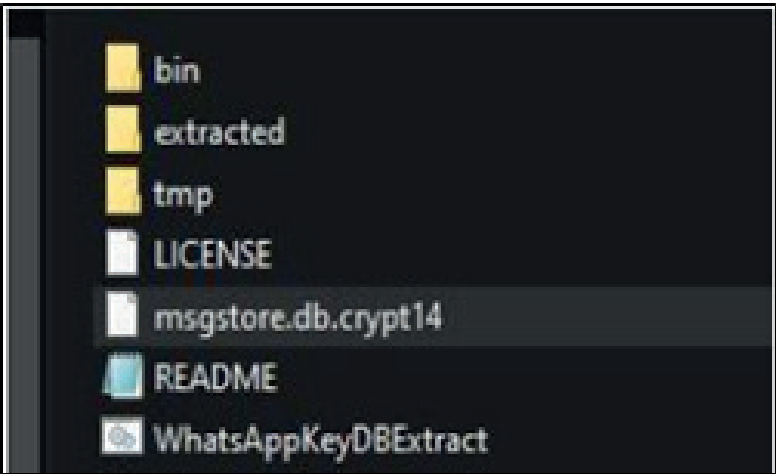
10. A continuación, abrir el programa WhatsApp Xtract para realizar el análisis forense a la base de datos de WhatsApp. Para ello, se ejecuta la aplicación de WhatsApp Viewer para visualizar el contenido del archivo “msgstore.db” extraído desde Android, a continuación, se visualizarán los mensajes de los diferentes chats que contiene el teléfono.



11. Observar que al realizar este proceso se generan más archivos.

msgstore.db-shm	23/04/2024 03:53 p. m.	Archivo DB-SHM	32 KB
msgstore.db-wal	23/04/2024 03:53 p. m.	Archivo DB-WAL	0 KB

12. Para abrir una base de datos de WhatsApp copiar un de los archivos mostrados en el punto anterior, desde el dispositivo móvil y pasarlo al equipo. Este archivo tiene una extensión crypt14, que será leído desde el programa WhatsApp Viewer en conjunto con el archivo “WhatsApp.cryptkey” que se generó en la extracción, el cual permitirá descifrar la base de datos.



3.7 Cuestionario de autoevaluación

1. **¿Cuál de estas opciones NO es un disco duro?**
 - a. HDD disco duro magnético
 - b. SSD unidad de estado sólido
 - c. RAM memoria de acceso aleatorio
 - d. SSHD unidad híbrida de estado sólido
2. **¿Cuál es una ventaja de los discos duros HDD?**
 - a. Mayor velocidad de lectura y escritura
 - b. Mayor vida útil
 - c. Menor costo por GB de almacenamiento
 - d. Menor consumo de energía
3. **¿Cuál de las siguientes características es una ventaja de los discos duros SSD?**
 - a. Mayor capacidad de almacenamiento
 - b. Mayor resistencia a golpes y vibraciones
 - c. Menor ruido de funcionamiento
 - d. Menor tiempo de acceso a los datos
4. **¿Qué sistema de archivos se suele usar en Windows?**
 - a. FAT32
 - b. NTFS
 - c. exFAT
 - d. APFS
5. **¿Cuál de las siguientes características es una ventaja del sistema de archivos NTFS?**
 - a. Compatible con sistemas operativos macOS
 - b. Soporta archivos de hasta 16 EIB ($1,845^7$ TB)
 - c. Optimizado para unidades de estado sólido
 - d. Permite la compresión de archivos
6. **¿Qué sistema de archivos se usa en dispositivos macOS?**
 - a. FAT32
 - b. NTFS
 - c. exFAT
 - d. APFS
7. **¿Qué es el data carving?**
 - a. Un método para recuperar archivos perdidos o dañados de un dispositivo de almacenamiento
 - b. Un tipo de sistema de archivos
 - c. Un software para la investigación forense digital
 - d. La extracción de metadatos de un archivo digital
8. **¿Qué es la línea de tiempo forense?**
 - a. Una representación gráfica de los eventos que ocurrieron en un dispositivo de almacenamiento
 - b. Un método para recuperar archivos perdidos o dañados de un dispositivo de almacenamiento
 - c. Un tipo de sistema de archivos
 - d. Un software para la investigación forense digital
9. **¿Cuál de las siguientes características es una ventaja del sistema de archivos APFS?**
 - a. Soporta archivos de hasta 64 ZIB ($6,4^{10}$ TB)
 - b. Optimizado para discos duros magnéticos
 - c. Compatible con sistemas operativos Windows
 - d. Permite el cifrado de archivos
10. **¿Qué es el metadato?**
 - a. El contenido de un archivo digital
 - b. Información sobre el archivo digital, como su fecha de creación, tamaño y autor

- c. Un tipo de sistema de archivos
- d. Un software para la investigación forense digital

11. ¿En qué consiste la extracción de evidencia forense?

- a. La eliminación de datos de un dispositivo de almacenamiento
- b. La copia de datos de un dispositivo de almacenamiento para su análisis
- c. La restauración de datos de un dispositivo de almacenamiento dañado
- d. La identificación de malware en un dispositivo de almacenamiento

12. ¿Qué es la base de datos de WhatsApp?

- a. Un archivo que contiene los mensajes de WhatsApp de un usuario
- b. Un tipo de sistema de archivos
- c. Un software para la investigación forense digital
- d. La línea de tiempo forense de un dispositivo de almacenamiento

13. ¿Qué software se utiliza para extraer la base de datos de WhatsApp de un dispositivo Android?

- a. ADEL (Android Data Extractor Lite)
- b. FTK Imager
- c. Guymager
- d. QPHOTOREC

14. ¿Qué software se utiliza para analizar la base de datos de WhatsApp?

- a. WhatsApp Viewer
- b. FTK Imager
- c. Guymager
- d. QPHOTOREC

15. ¿Cuál de las siguientes opciones es un desafío de la seguridad de los discos duros en la era de la nube?

- a. Mayor capacidad de almacenamiento
- b. Mayor velocidad de lectura y escritura
- c. Mayor riesgo de ataques cibernéticos
- d. Menor consumo de energía

- 4.1 Definición y tipos de memoria RAM
- 4.2 Memoria física y archivos de paginación
- 4.3 Práctica 1. Volcado de memoria RAM
- 4.4 Práctica 2. Análisis del contenido almacenado en la memoria RAM
- 4.5 Práctica 3. Análisis del archivo pagefile.sys del sistema operativo Windows
- 4.6 Cuestionario de autoevaluación

4.1 Definición y tipos de memoria RAM

La memoria, entendida como un componente electrónico esencial en los sistemas informáticos, permite almacenar datos para su recuperación y manipulación rápida. En las operaciones típicas de la memoria, se incluyen acciones de lectura, donde se recupera el contenido previamente almacenado, y de escritura, donde los datos se guardan en una ubicación específica dentro de la memoria (Raquejo Romero, 2013).

Existen principalmente dos tipos de memoria RAM (Memoria de Acceso Aleatorio), que son cruciales para entender cómo funcionan los sistemas informáticos en cuanto a la gestión de datos.

Existen varios tipos de memoria RAM, cada uno con características distintas:

- **DRAM (Dynamic RAM):**

La más común y utilizada en la mayoría de las computadoras personales. Almacena datos en celdas formadas por un transistor y un condensador que necesitan ser refrescados periódicamente. Es más lenta que la SRAM.

- **SRAM (Static RAM):**

No necesita ser refrescada constantemente, lo que la hace más rápida que la DRAM. Utiliza múltiples transistores para almacenar un solo bit de datos. Es más cara y se utiliza principalmente en cachés de CPU.

- **SDRAM (Synchronous DRAM):**

Opera sincronizada con el reloj del sistema, lo que mejora la eficiencia en la transferencia de datos. Ha evolucionado hacia formatos más rápidos y eficientes como DDR (Double Data Rate).

- **DDR (Double Data Rate SDRAM):**

Transfiere datos en ambos flancos (subida y bajada) de cada ciclo de reloj, duplicando la tasa de transferencia de datos sin aumentar la frecuencia del reloj. Existen varias generaciones como DDR, DDR2, DDR3, y DDR4, cada una ofreciendo mejoras en velocidad, tamaño y consumo de energía.

4.2 Memoria física y archivos de paginación

Memoria Física. - La memoria física en un computador se refiere a la memoria RAM (Random Access Memory). Es la memoria principal de un sistema donde se almacenan los datos y programas que están siendo utilizados activamente por el CPU. La memoria física es rápida y permite un acceso rápido a los datos, lo que es crucial para el rendimiento del sistema. Sin embargo, es volátil, lo que significa que los datos se pierden cuando el dispositivo se apaga o se reinicia.

Archivos de Paginación. - Los archivos de paginación, también conocidos como archivo de intercambio o swap file, son una parte crucial de la gestión de la memoria en sistemas operativos modernos, especialmente en Windows. Este archivo se utiliza para ampliar virtualmente la cantidad de memoria física disponible, permitiendo que el sistema maneje más procesos simultáneamente de lo que la memoria física podría permitir por sí sola.

Funcionamiento. - Cuando la memoria RAM está casi llena, el sistema operativo traslada temporalmente los fragmentos de datos que se utilizan menos a un archivo de paginación en el disco duro o SSD. Este proceso se llama paginación.

Este archivo de paginación actúa como una memoria virtual. Aunque el acceso a los datos en el archivo de paginación es más lento que el acceso a la memoria física permite al sistema continuar funcionando sin quedarse sin memoria.

Utilizar la memoria virtual permite que el sistema maneje más aplicaciones simultáneamente y evita que el sistema se bloquee por falta de memoria. Sin embargo, el uso excesivo del archivo de paginación puede reducir el rendimiento del sistema, ya que leer y escribir en un disco duro o SSD es significativamente más lento que acceder a la memoria RAM.

4.3 Práctica 1. Volcado de memoria RAM

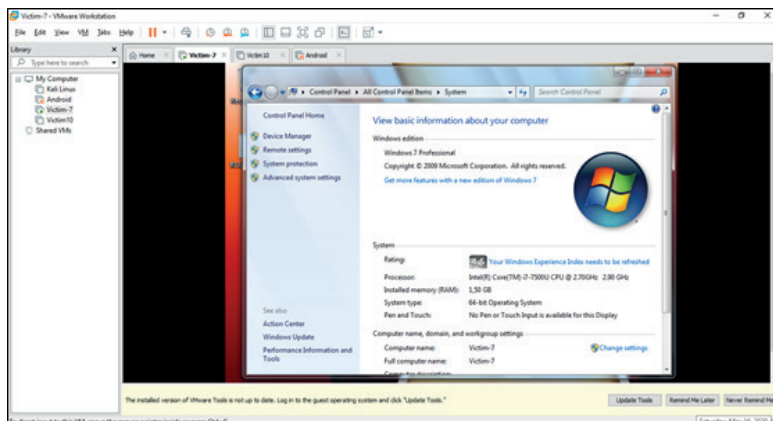
El objetivo de esta práctica es realizar un volcado de la memoria RAM en un equipo encendido. Primero, se usará la línea de comandos desde O.S. Windows a través de la herramienta **win32dd** de MoonSols, y luego con el software **Access Data FTK Imager** desde Windows o Linux. Para esta actividad se sugiere realizar el volcado de memoria de una máquina virtual cuyo tamaño de RAM no supere los 4GB por la capacidad de almacenamiento que se requiere para este proceso. A continuación, se describen los recursos requeridos y el procedimiento para generar la imagen forense del volcado de la memoria RAM.

Recursos necesarios:

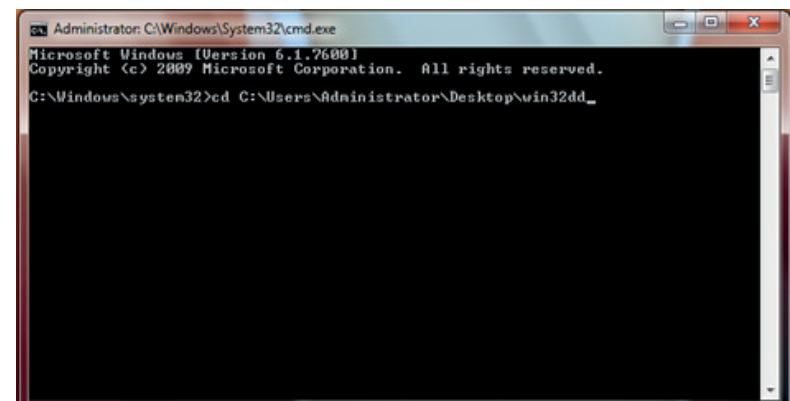
- Computadora con acceso a internet
- Máquina virtual Oracle VM VirtualBox o VMware Workstation
- Software Access Data FTK Imager, Memoryze, herramienta Win32dd.exe / win64dd.exe, LiMe.

Procedimiento. - En esta primera parte de la actividad, se utilizará una máquina virtual con O.S. Windows 7.

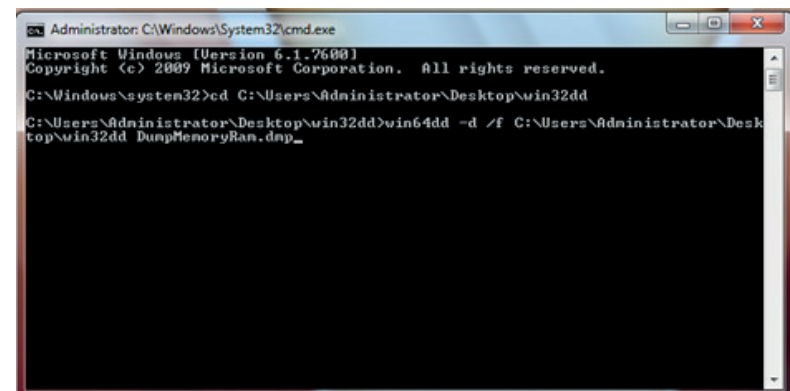
1. Ejecutar la máquina virtual e iniciar el O.S. Windows 7.
2. En las propiedades del equipo se observa la capacidad de la memoria RAM de 1.5GB.



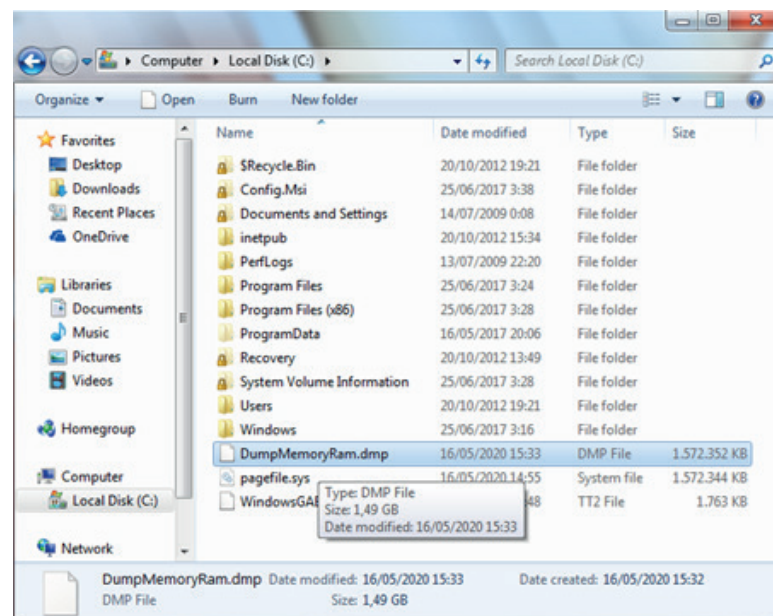
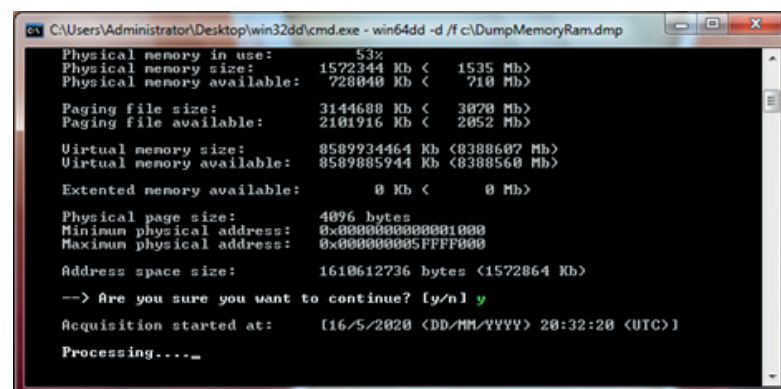
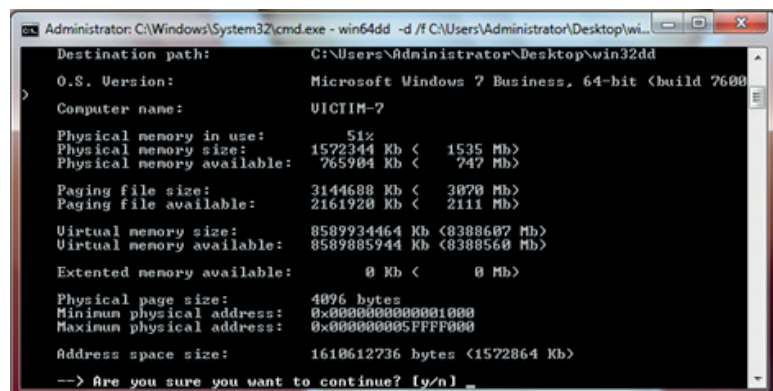
3. Ejecutar la línea de comandos de Windows en modo administrador. Cambiarse a la ruta donde se encuentra el programa win32dd. Para el ejemplo, esta carpeta se encuentra en el escritorio. Moverse a la ruta mediante la instrucción `cd C:\Users\Administrator\Desktop\win32dd`



4. Ubicado en la ruta donde que contiene el programa win32dd; ejecutar la instrucción `win64dd -d /f C:\Users\Administrator\Desktop\win32dd DumpMemoryRam.dmp`. Esta instrucción corresponde a la sintaxis `c:[ruta_carpeta_win32dd] win64dd -d /f [ruta_carpeta_win32dd] NombreArchivoSalida`

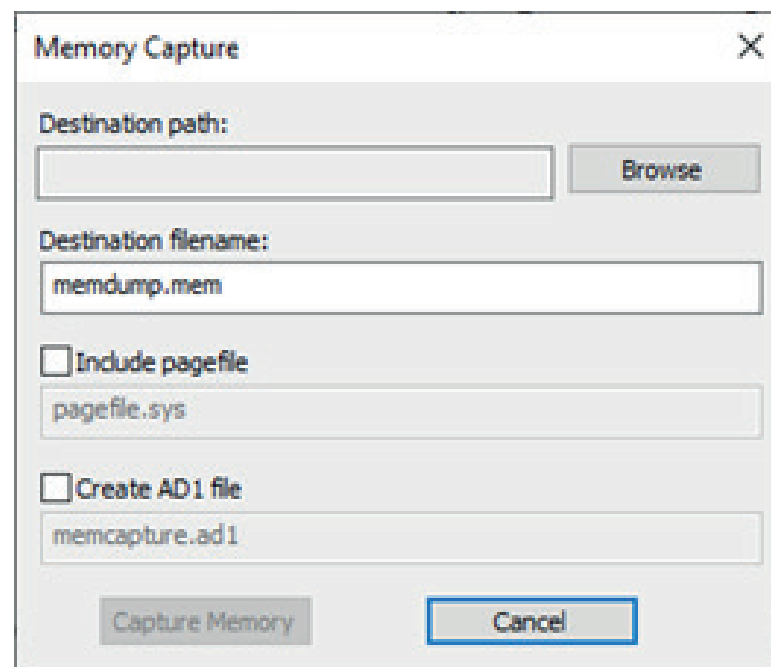


5. A continuación, el programa requiere de una confirmación para iniciar el proceso. Para confirmar presionar la tecla y. El proceso concluye con un archivo de salida de igual tamaño de la memoria RAM del equipo.

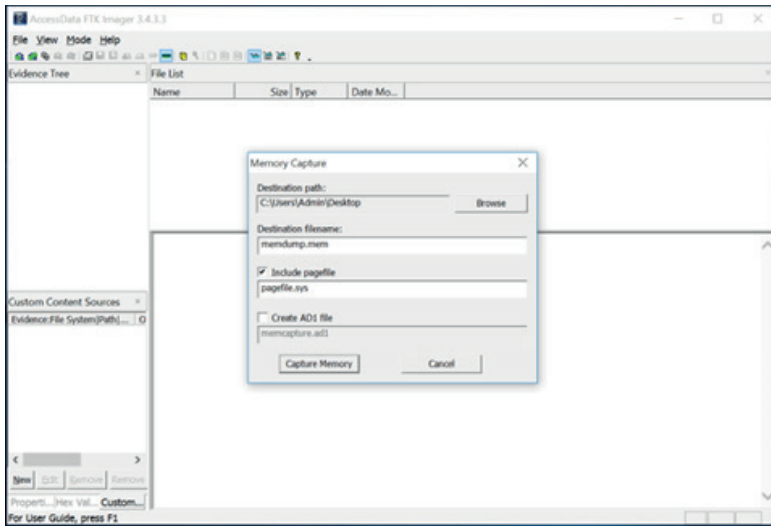


Procedimiento. - En esta segunda parte de la actividad, se utilizará una máquina virtual con O.S. Windows 7 y el software **Access Data FTK Imager**.

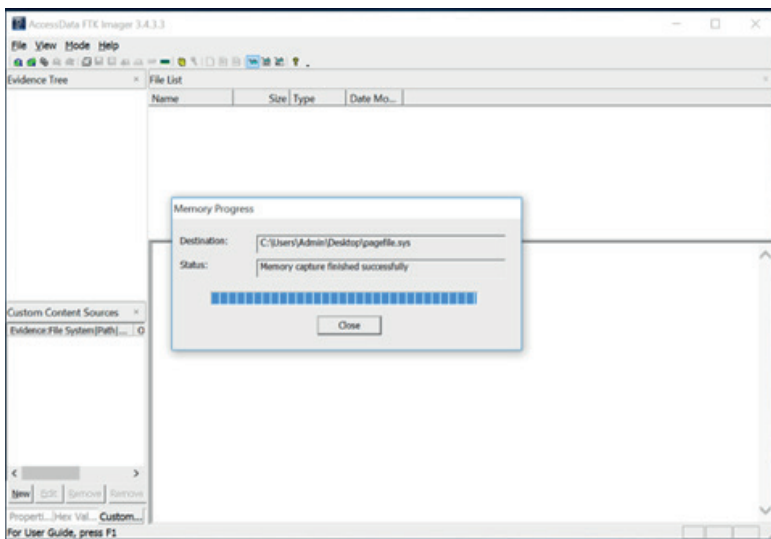
1. Inicie el software Access Data FTK Imager. Luego escoja la opción File -> Capture Memory.



2. En la ventana de Memory Capture seleccione la ruta de destino donde se almacenará la imagen de la memoria RAM. Digite el nombre del archivo de destino de la imagen cuya extensión será. mem. En este proceso tiene la opción de incluir la carga del archivo pagefile.sys, para el ejemplo se extraerá este archivo clic en check Include pagefile. Luego presione el botón Capture Memory para iniciar el volcado de la memoria RAM.



3. Por último, el proceso concluye con un mensaje de “Memory capture finished successfully” y los archivos memdump.mem y pagefile.sys se almacenan en la ruta seleccionada, en este ejemplo C:\Users\Admin\Desktop\.



4.4 Práctica 2. Análisis del contenido almacenado en la memoria RAM

El objetivo de esta práctica es analizar información contenida en la memoria RAM, y utilizar un software forense para extraer y visualizar la información del archivo. mem. Esta actividad, se realiza en dos partes, la primera consiste en usar el software Volatility Memory, y la segunda parte analizar el contenido de la memoria RAM usando los softwares Phtorec y AccessData.

Recursos necesarios:

- Computadora
- Imagen forense y/o evidencia digital [use el archivo cridex.vmem]
- Sistema operativo Windows & Caine
- Software Volatility Memory & Photorec

Procedimiento. - En esta primera parte, se procede a cargar la evidencia digital [volcado de memoria RAM] usando el software Volatility Memory.

1. Iniciar la máquina virtual con el S.O Caine. Luego abrir la línea comandos y verificar si está instalado el programa volatility. En la línea de comandos es posible obtener ayuda sobre el uso del programa mediante la instrucción `caine@caine:~$ volatility -h`

```

lidice@lidice-VirtualBox: ~
Archivo Editar Ver Buscar Terminal Ayuda
lidice@lidice-VirtualBox:~$ volatility -h
Volatility Foundation Volatility Framework 2.6
Usage: Volatility - A memory forensics analysis platform.

Options:
-h, --help          list all available options and their default values.
                    Default values may be set in the configuration file
                    (/etc/volatilityrc)
--conf-file=/home/lidice/.volatilityrc
                    User based configuration file
-d, --debug          Debug volatility
--plugins=PLUGINS    Additional plugin directories to use (colon separated)
--info              Print information about all registered objects
--cache-directory=/home/lidice/.cache/volatility
                    Directory where cache files are stored
  
```

2. Para conocer información sobre la arquitectura de la máquina de la cual se realizó el volcado de memoria se usa el comando `imageinfo` mediante la siguiente instrucción `caine@caine:~$ volatility -f /media/sdb5/cridex.vmem imageinfo`.

```

lidice@lidice-VirtualBox:~$ volatility -f /media/sdb1/cridex.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with
WinXPSP2x86)
AS Layer1 : IA32PagedMemoryPae (Kernel AS)
AS Layer2 : FileAddressSpace (/media/sdb1/cridex.vmem)
PAE type : PAE
DTB : 0x2fe000L
KDBG : 0x80545ae0L
Number of Processors : 1
Image Type (Service Pack) : 3
KPCR for CPU 0 : 0xffdf000L
KUSER_SHARED_DATA : 0xffdf000L
Image date and time : 2012-07-22 02:45:08 UTC+0000
Image local date and time : 2012-07-21 22:45:08 -0400

```

Con la siguiente instrucción es posible definir específicamente el tipo de arquitectura y de la memoria que se desea analizar. Esto es importante porque según la tecnología del CPU y la versión del sistema operativo puede variar el proceso de análisis de la memoria con volatility. `caine@caine:~$ volatility -f /cridex.vmem --dtb=0x2fe000 --kdbg=0x80545ae0 --kpcr=0xffdf000 --profile=WinXPSP3x86 pslist`

3. Para conocer los procesos que se estaban ejecutando en la máquina cuando se realizó el volcado de la memoria es posible usar los comandos `pslist`, `psscan`, `pstree`. Para el ejemplo, se utiliza la instrucción `caine@caine:~$ volatility pslist -f /media/sdb5/cridex.vmem`.

```

lidice@lidice-VirtualBox:~$ volatility pslist -f /media/sdb1/cridex.vmem
Volatility Foundation Volatility Framework 2.6
Offset(V) Name PID PPID Thds Hnds Sess Wow64
Start Exit
-----
0x823c89c8 System 4 0 53 240 ----- 0
0x822f1020 smss.exe 368 4 3 19 ----- 0
2012-07-22 02:42:31 UTC+0000
0x822a0598 csrss.exe 584 368 9 326 0 0
2012-07-22 02:42:32 UTC+0000
0x82298700 winlogon.exe 608 368 23 519 0 0
2012-07-22 02:42:32 UTC+0000
0x81e2ab28 services.exe 652 608 16 243 0 0
2012-07-22 02:42:32 UTC+0000

```

`caine@caine:~$ volatility psscan -f /media/sdb5/cridex.vmem`

```

lidice@lidice-VirtualBox:~$ volatility psscan -f /media/sdb1/cridex.vmem
Volatility Foundation Volatility Framework 2.6
Offset(P) Name PID PPID PDB Time created
-----
0x000000002029ab8 svchost.exe 908 652 0x079400e0 2012-07-22 02:4
2:33 UTC+0000
0x00000000202a3b8 lsass.exe 664 608 0x079400a0 2012-07-22 02:4
2:32 UTC+0000
0x00000000202ab28 services.exe 652 608 0x07940080 2012-07-22 02:4
2:32 UTC+0000
0x00000000207bda0 reader_sl.exe 1640 1484 0x079401e0 2012-07-22 02:4
2:36 UTC+0000
0x0000000020b17b8 spoolsv.exe 1512 652 0x079401c0 2012-07-22 02:4
2:36 UTC+0000

```

`caine@caine:~$ volatility pstree -f /media/sdb5/cridex.vmem`

```

lidice@lidice-VirtualBox:~$ volatility pstree -f /media/sdb1/cridex.vmem
Volatility Foundation Volatility Framework 2.6
Name Pid PPid Thds Hnds Time
-----
0x823c89c8:System 4 0 53 240 1970-01-01 00:
00:00 UTC+0000
... 0x822f1020:smss.exe 368 4 3 19 2012-07-22 02:
42:31 UTC+0000
... 0x82298700:winlogon.exe 608 368 23 519 2012-07-22 02:
42:32 UTC+0000
... 0x81e2ab28:services.exe 652 608 16 243 2012-07-22 02:
42:32 UTC+0000
... 0x821dfda0:svchost.exe 1056 652 5 60 2012-07-22 02:
42:33 UTC+0000
... 0x81eb17b8:spoolsv.exe 1512 652 14 113 2012-07-22 02:
42:36 UTC+0000

```

4. En este análisis también es posible observar las conexiones de red que estaban establecidas en el momento del volcado. Para esto se utilizan diferentes comandos `connscan`, `connections`, `sockscan`, `sockets`. `caine@caine:~$ volatility connscan -f /media/sdb5/cridex.vmem`

```

lidice@lidice-VirtualBox:~$ volatility connscan -f /media/sdb1/cridex.vmem
Volatility Foundation Volatility Framework 2.6
Offset(P) Local Address Remote Address Pid
-----
0x02087620 172.16.112.128:1038 41.168.5.140:8080 1484
0x023a8008 172.16.112.128:1037 125.19.103.198:8080 1484

```

`caine@caine:~$ volatility sockscan -f /media/sdb5/cridex.vmem`


```
lidice@lidice-VirtualBox:~$ volatility sockscan -f /media/sdb1/cridex.vmem
Volatility Foundation Volatility Framework 2.6
Offset(P) PID Port Proto Protocol Address Create Time
-----
0x01fd7618 1220 1900 17 UDP 172.16.112.128 2012-07-22 02:43:01 UTC+0
000
0x01fdb780 664 500 17 UDP 0.0.0.0 2012-07-22 02:42:53 UTC+0
000
0x0203f460 4 138 17 UDP 172.16.112.128 2012-07-22 02:42:38 UTC+0
000
0x02076620 1004 123 17 UDP 127.0.0.1 2012-07-22 02:43:01 UTC+0
000
0x020c23b0 908 135 6 TCP 0.0.0.0 2012-07-22 02:42:33 UTC+0
000
0x02325610 788 1028 6 TCP 127.0.0.1 2012-07-22 02:43:01 UTC+0
000
```

caine@caine:~\$ volatility sockets -f /media/sdb5/cridex.vmem

```
lidice@lidice-VirtualBox:~$ volatility sockets -f /media/sdb1/cridex.vmem
Volatility Foundation Volatility Framework 2.6
Offset(V) PID Port Proto Protocol Address Create Time
-----
0x81ddb780 664 500 17 UDP 0.0.0.0 2012-07-22 02:42:53 UTC+0
000
0x82240d08 1484 1038 6 TCP 0.0.0.0 2012-07-22 02:44:45 UTC+0
000
0x81dd7618 1220 1900 17 UDP 172.16.112.128 2012-07-22 02:43:01 UTC+0
000
0x82125610 788 1028 6 TCP 127.0.0.1 2012-07-22 02:43:01 UTC+0
000
0x8219cc08 4 445 6 TCP 0.0.0.0 2012-07-22 02:42:31 UTC+0
000
0x81ec23b0 908 135 6 TCP 0.0.0.0 2012-07-22 02:42:33 UTC+0
000
```

5. También es posible buscar malware que haya sido inyectado en otro proceso como lo que ocurre con meterpreter. Para esto se utiliza el comando malfind. caine@caine:~\$ volatility malfind -f /media/sdb5/cridex.vmem

```
lidice@lidice-VirtualBox:~$ volatility malfind -f /media/sdb1/cridex.vmem
Volatility Foundation Volatility Framework 2.6
Process: csrss.exe Pid: 584 Address: 0x7f6f0000
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6
0x7f6f0000 c8 00 00 00 91 01 00 00 ff ee ff ee 08 70 00 00 .....p..
0x7f6f0010 08 00 00 00 00 fe 00 00 00 10 00 00 20 00 00 .....
0x7f6f0020 00 02 00 00 00 20 00 00 8d 01 00 00 ff ef fd 7f .....
0x7f6f0030 03 00 08 06 00 00 00 00 00 00 00 00 00 00 00 .....
0x7f6f0000 c8000000 ENTER 0x0, 0x0
0x7f6f0004 91 XCHG ECX, EAX
0x7f6f0005 0100 ADD [EAX], EAX
0x7f6f0007 00ff ADD BH, BH
```

6. Otro comando importante de volatility es hivelist que permite extraer los offsets de memoria donde fue cargado el sistema operativo, lo cual podría servir para obtener la base SAM y con ello las contraseñas del sistema. caine@caine:~\$ volatility hivelist -f /media/sdb5/cridex.vmem

```
lidice@lidice-VirtualBox:~$ volatility hivelist -f /media/sdb1/cridex.vmem
Volatility Foundation Volatility Framework 2.6
Virtual Physical Name
-----
0xe18e5b60 0x093f8b60 \Device\HarddiskVolume1\Documents and Settings\Robert\Local Settings\
Application Data\Microsoft\Windows\UsrClass.dat
0xe1a19b60 0x0a5a9b60 \Device\HarddiskVolume1\Documents and Settings\Robert\NTUSER.DAT
0xe18398d0 0x08a838d0 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Set
tings\Application Data\Microsoft\Windows\UsrClass.dat
0xe18614d0 0x08e624d0 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DA
T
0xe183bb60 0x08e2db60 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local S
ettings\Application Data\Microsoft\Windows\UsrClass.dat
0xe17f2b60 0x08519b60 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.
DAT
```

7. También puedo extraer información sobre el id del usuario que ejecutó un determinado proceso. Para esto se utiliza el comando getsids junto con el ID del proceso que se desea analizar. Para el ejemplo, se quiere conocer quien ejecutó el proceso 1484 que corresponde al explorer según la información extraída previamente con psscan. La instrucción sería la siguiente caine@caine:~\$ volatility getsids -p 1484 -f /media/sdb5/cridex.vmem

```
lidice@lidice-VirtualBox:~$ volatility getsids -p 1484 -f /media/sdb1/cridex.vmem
Volatility Foundation Volatility Framework 2.6
explorer.exe (1484): S-1-5-21-789336058-261478967-1417001333-1003 (Robert)
explorer.exe (1484): S-1-5-21-789336058-261478967-1417001333-513 (Domain Users)
explorer.exe (1484): S-1-1-0 (Everyone)
explorer.exe (1484): S-1-5-32-544 (Administrators)
explorer.exe (1484): S-1-5-32-545 (Users)
explorer.exe (1484): S-1-5-4 (Interactive)
explorer.exe (1484): S-1-5-11 (Authenticated Users)
explorer.exe (1484): S-1-5-5-0-53426 (Logon Session)
explorer.exe (1484): S-1-2-0 (Local (Users with the ability to log in locally))
lidice@lidice-VirtualBox:~$
```

8. A continuación, se extraerá la información de la base SAM para conocer el usuario y la contraseña que se autenticó en el sistema. Primero, extraer la información de los offsets de memoria donde se cargó el sistema operativo. La instrucción es caine@caine:~\$ volatility hivescan -f /media/sdb5/cridex.vmem

De la información anterior seleccionar un offset de memoria, con el fin de obtener los archivos SAM y system. La instrucción es `caine@caine:~$ volatility hivelist -f /media/sdb5/cridex.vmem 0x076699b8`

```

lidice@lidice-VirtualBox:~$ volatility hivelist -f /media/sdb5/cridex.vmem 0x076699b8
Volatility Foundation Volatility Framework 2.6
Virtual Physical Name
-----
0xe18e5b60 0x093f8b60 \Device\HarddiskVolume1\Documents and Settings\Robert\Local Settings\
Application Data\Microsoft\Windows\UsrClass.dat
0xe1a19b60 0x0a5a9b60 \Device\HarddiskVolume1\Documents and Settings\Robert\NTUSER.DAT
0xe18398d0 0x08a838d0 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local S
ettings\Application Data\Microsoft\Windows\UsrClass.dat
0xe18614d0 0x08e624d0 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.
DAT
0xe183bb60 0x08e2db60 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local
Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe17f2b60 0x08519b60 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSE
R.DAT
0xe1570510 0x07669510 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe1571008 0x0777f008 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe15709b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0xe15709b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY

```

```

lidice@lidice-VirtualBox:~$ volatility hashdump -f /media/sdb5/cridex.vmem -y 0xe1035b60 -s 0xe15719e8
Volatility Foundation Volatility Framework 2.6
hashdump: 0x076699b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
hashdump: 0x076699b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
hashdump: 0x076699b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
hashdump: 0x076699b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
hashdump: 0x076699b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
hashdump: 0x076699b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
hashdump: 0x076699b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
hashdump: 0x076699b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
hashdump: 0x076699b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
hashdump: 0x076699b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY

```

A continuación, se extrae la información del archivo SAM mediante el comando `hashdump` identificando el offset de memoria del archivo `system` mediante `-y` y el offset de memoria de la base SAM con `-s`. La instrucción es `caine@caine:~$ volatility hashdump -f /media/sdb5/cridex.vmem -y 0xe1035b60 -s 0xe15719e8`

```

Investigador@Caine9: ~/Desktop
File Edit View Search Terminal Help
Investigador@Caine9:~/Desktop$ volatility hashdump -f /media/sdb5/cridex.vmem -y 0xe1035b60 -s 0xe15719e8
Volatility Foundation Volatility Framework 2.6
hashdump: 0x076699b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
hashdump: 0x076699b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
hashdump: 0x076699b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
hashdump: 0x076699b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
hashdump: 0x076699b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
hashdump: 0x076699b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
hashdump: 0x076699b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
hashdump: 0x076699b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
hashdump: 0x076699b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
hashdump: 0x076699b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY

```

Es posible usar John de Ripper para obtener las contraseñas. La información obtenida de los usuarios debe guardarse en un archivo `caine@caine:~$ nano sam.txt` y luego ejecutar el comando `john caine@caine:~$ john sam.txt`

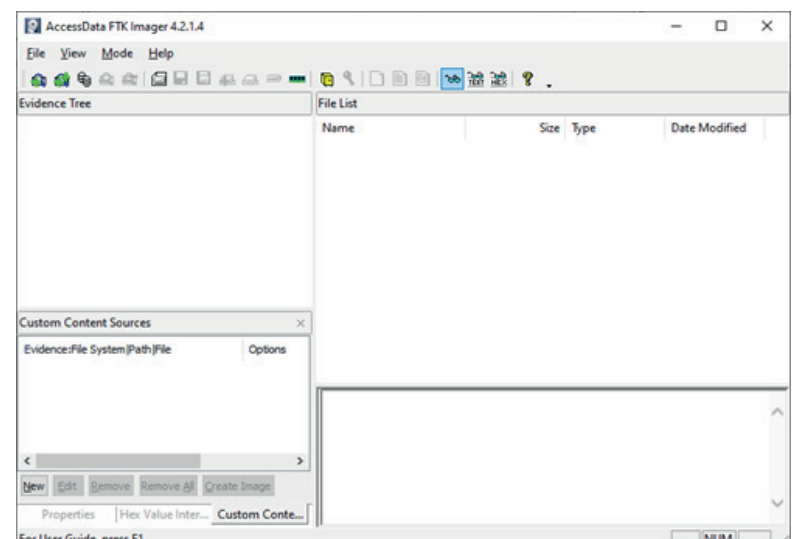
```

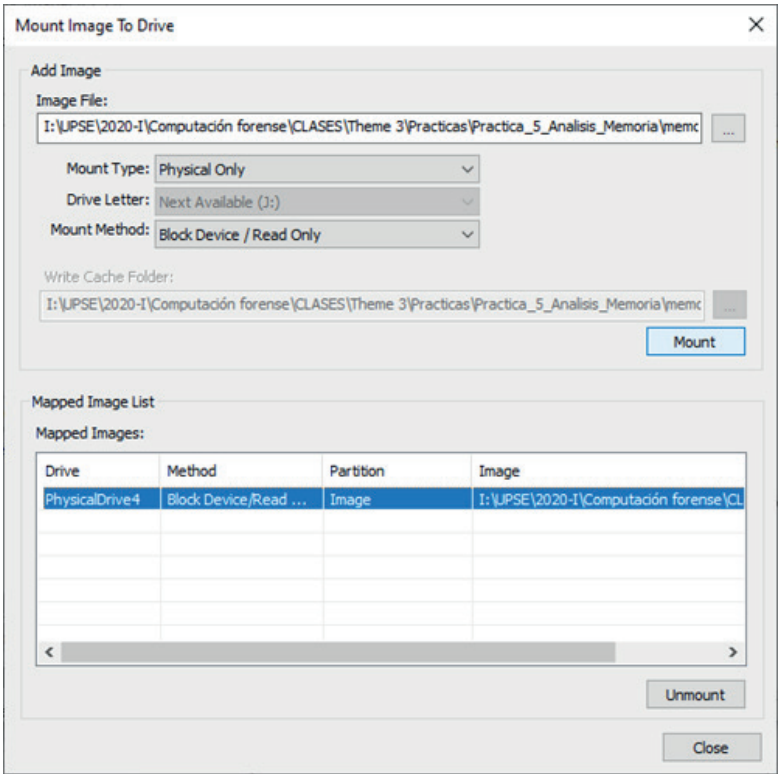
Investigador@Caine9: ~/Desktop
File Edit View Search Terminal Help
Investigador@Caine9:~/Desktop$ nano sam.txt
Investigador@Caine9:~/Desktop$ john sam.txt
Created directory: /home/Investigador/.john
Loaded 6 password hashes with no different salts (LM [DES 320/120 SSE2-16])
Press 'q' or Ctrl-C to abort, almost any other key for status
(SUPPORT_38045a0)
(PASSWORD)
(Administrator:1)
(Administrator:2)
Pw 0:00:00:00 2/3 0.444g/s 33014K/s 33014K/s 66042K/s GHSAC1..GHSAC1
Pw 0:00:00:11 2/3 0.363g/s 34041K/s 34041K/s 68082K/s TSLCB4..TSLCB4

```

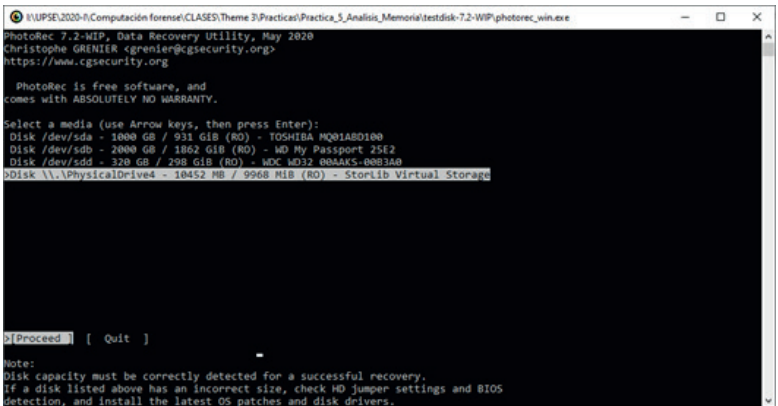
Procedimiento. - En esta segunda parte, se procede a cargar la evidencia digital [volcado de memoria RAM] usando el software `Phorec` y `AccessData`.

1. Ejecutar el software `AccessData` como administrador. Luego, proceder a cargar el archivo. `mem` como una unidad física para que pueda ser visualizada en los dispositivos del PC. Para esto, seleccionar el menú `File -> Image Mounting`, buscar el archivo que contiene los datos de la memoria para este ejemplo `memdump.mem`, seleccionar tipo de montaje `Physical Only` y presionar el botón `Mount`.

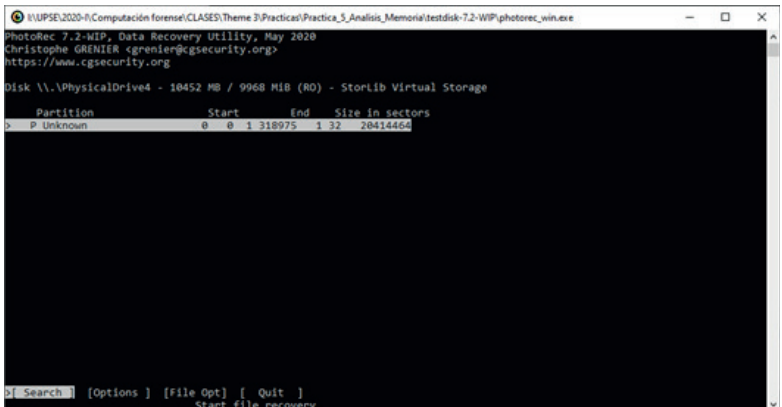




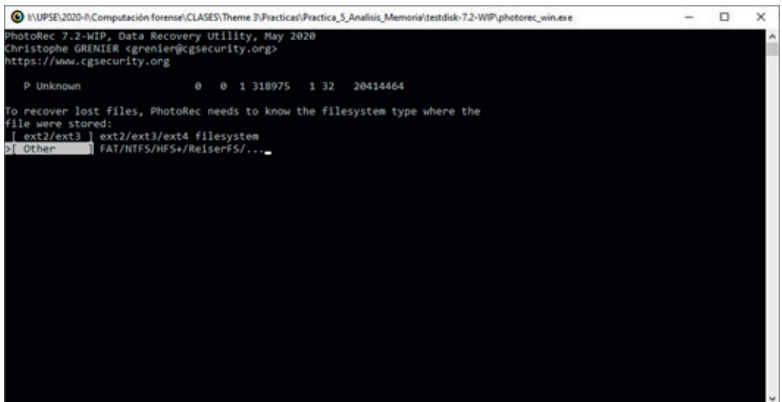
2. Ejecutar como administrador el software Photorec. En la ventana principal aparecerán todas las unidades físicas que están cargadas en el PC. Ubique el nombre de la unidad física que fue cargada en el paso anterior. Para este ejemplo PhysicalDrive4.



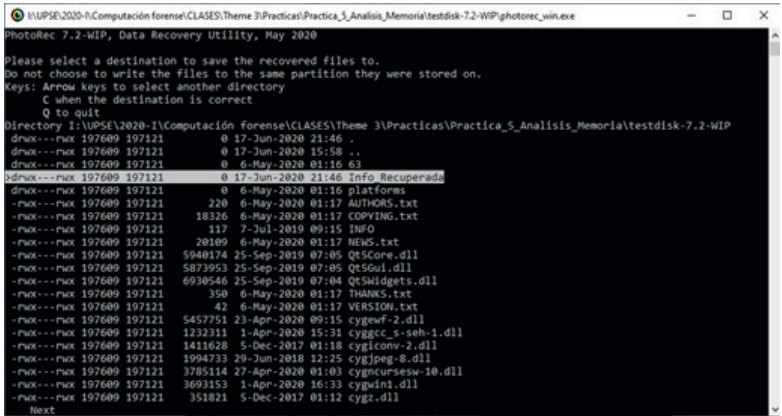
3. Luego de seleccionar la unidad física aparece la siguiente pantalla en la cual se indica la cantidad de sectores que contiene dicha unidad.



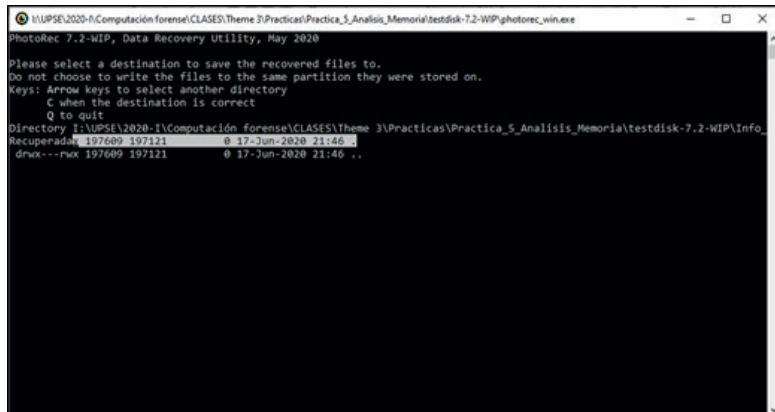
4. Luego de presionar Enter, la siguiente pantalla pregunta el tipo de sistema de archivo que utiliza la unidad. Para este ejemplo seleccionar la opción FAT/NTFS/HFS+/ReiserFS/...



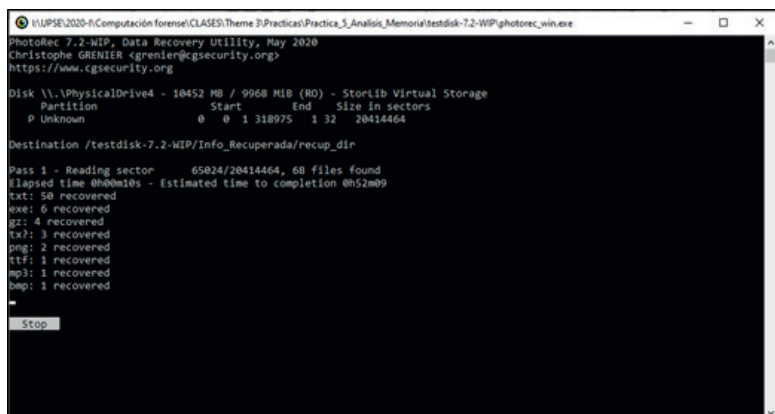
5. La siguiente pantalla sugiere la creación y/o selección de una carpeta donde se guardará los archivos que se recuperen de la unidad. Para este ejemplo previamente se ha creado una carpeta llamada Info_Recuperada.



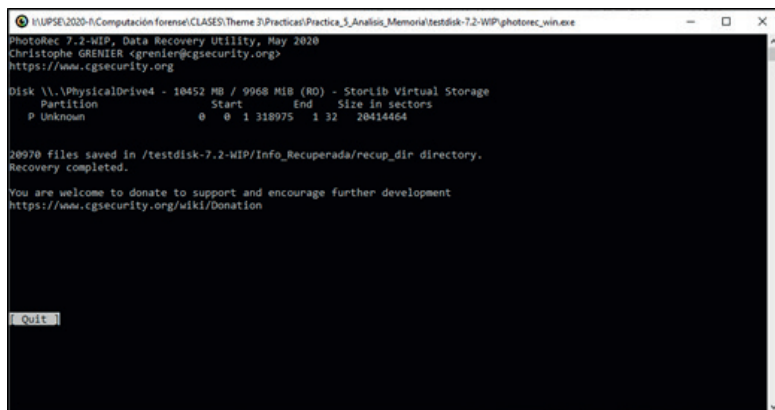
6. La siguiente pantalla valida la información ingresada. Para esto, presionar la tecla C según lo sugerido por el software.



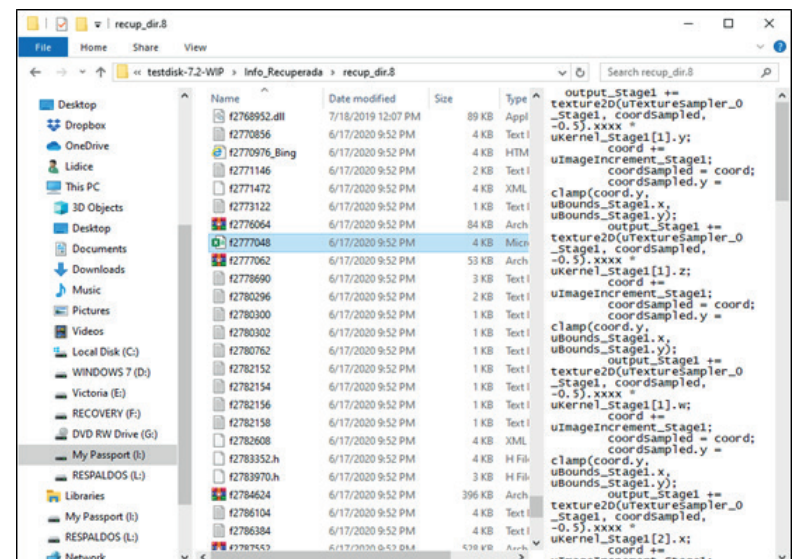
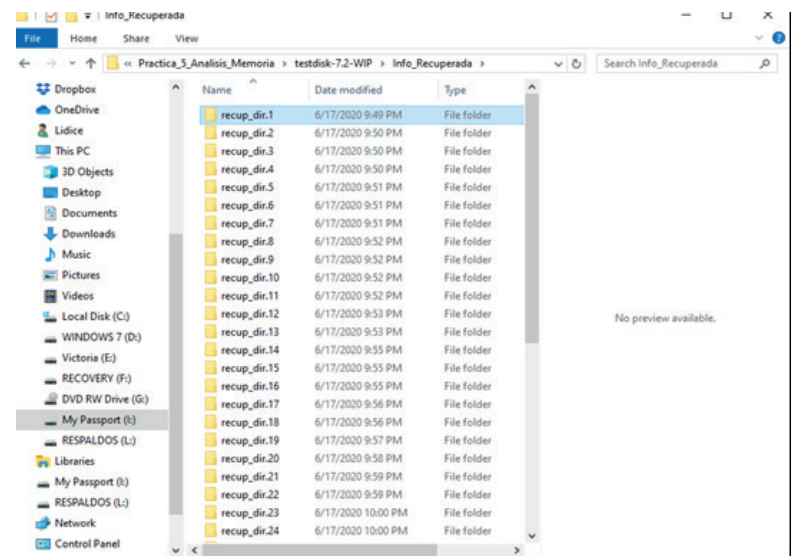
7. Luego de presionar la tecla C el software iniciará el proceso de recuperación.



8. Luego de concluir el proceso de recuperación, se presenta el siguiente mensaje. Lo siguiente es revisar el contenido extraído en la carpeta Info_Recuperada.



9. La carpeta Info_Recuperada contendrá la información recopilada en directorios con diferentes tipos de archivos, buscar pruebas de forma manual es una tarea muy compleja por la cantidad de información. Para esto, es recomendable cargar los datos extraídos en programas como Autopsy o FTKImager, y crear búsquedas indexadas con palabras claves según lo requerido en el caso.



4.5 Práctica 3. Análisis del archivo pagefile.sys del sistema operativo Windows

El objetivo de esta práctica es analizar la información contenida en el archivo pagefile.sys del sistema operativo Windows.

Recursos necesarios:

- Computadora
- Archivo pagefile.sys
- Sistema operativo Caine

Procedimiento. - Cargar la evidencia digital en el sistema operativo Caine, y proceder con la lectura del archivo de la evidencia digital.

1. En el sistema operativo Caine ejecute desde la línea de comandos la instrucción `caine@caine:~$ bless pagefile.sys` esto permitirá ver la información contenida en el archivo en un formato hexadecimal incluido los códigos ASCII.

```
caine@caine:~$ bless /media/sdb1/pagefile.sys
```

The Bless tool interface displays the content of the pagefile.sys file. It shows a grid of hexadecimal values (e.g., 0000057c, 0000058e, 000005a0) and their corresponding ASCII representations (e.g.,). Below the grid, there are fields for Signed/Unsigned 8, 16, and 32 bits, Hexadecimal, Decimal, Octal, and Binary representations. The ASCII Text field is also visible.

2. Luego ejecute la instrucción `caine@caine:~$ strings -a -td -el /media/sdb1/pagefile.sys > /home/caine/Desktop/ResultPageFile.txt` esto permitirá extraer las cadenas de datos del archivo pagefile y lo almacenará en el archivo ResultPageFile.txt.

```
caine@caine:~$ strings -a -td -el /media/sdb1/pagefile.sys > /home/caine/Desktop/resultpagefile.txt
```

3. Para visualizar el contenido del archivo ejecute la instrucción `caine@caine:~$ gedit /home/caine/Desktop/ResultPageFile.txt`.

```
caine@caine:~$ gedit /home/caine/Desktop/resultpafefile.txt
```

The Pluma text editor displays the extracted strings from the pagefile.sys file. The content includes various system paths and parameters, such as:

```
10926 6495192 Q1JAVA=C:\Program Files
(x86)\QuickTime\QTSystem\QTJava.zip
10927 6495320 SystemRoot=C:\Windows
10928 6495376 TEMP=C:\Windows\TEMP
10929 6495432 TMP=C:\Windows\TEMP
10930 6495480 USERDOMAIN=WORKGROUP
10931 6495536 USERNAME=ELITEBOOK-PC$
10932 6495592 USERPROFILE=C:\Windows\system32\config\systemprofile
10933 6495712 windir=C:\Windows
10934 6495760 windows_tracing_flags=3
10935 6495816 windows_tracing_logfile=C:\
\BVTbin\Tests\installpackage\csilogfile.log
10936 6496992 avast! Antivirus
10937 6497512 ashServ.dll
10938 6500154 HgramData\AVAST Sof
10939 6500228 .int
10940 6500980 ystemDri
10941 6513768 @%SystemRoot%\System32\wshtcpip.dll,-60100
10942 6514340 \wshtcpip.dll,-60100
10943 6515576 @%SystemRoot%\System32\wshtcpip.dll,-60101
10944 6516148 \wshtcpip.dll,-60101
10945 6517384 @%SystemRoot%\System32\wshtcpip.dll,-60102
10946 6517956 \wshtcpip.dll,-60102
```


4.6 Cuestionario de autoevaluación

1. **¿Qué es la memoria RAM?**
 - a. Un dispositivo de almacenamiento permanente
 - b. Memoria de acceso aleatorio volátil
 - c. Una forma de memoria que no requiere energía para retener datos
 - d. Un archivo de sistema en Windows
2. **¿Qué significa DDR en el contexto de la memoria RAM?**
 - a. Data Direct Rate
 - b. Dual Dynamic Rate
 - c. Double Data Rate
 - d. Dynamic Data Range
3. **¿Qué tipo de memoria RAM es conocida por necesitar refrescamientos periódicos para mantener su información?**
 - a. SRAM
 - b. DRAM
 - c. Flash
 - d. EEPROM
4. **¿Qué función tiene un archivo de paginación en un sistema operativo?**
 - a. Optimizar el uso del procesador
 - b. Extender la memoria física mediante almacenamiento virtual
 - c. Aumentar la velocidad del sistema operativo
 - d. Guardar archivos temporales del usuario
5. **¿Cuál es un ejemplo de una herramienta utilizada para analizar volcados de memoria en sistemas Windows?**
 - a. Adobe Reader
 - b. WinDbg
 - c. Microsoft Excel
 - d. Norton Antivirus
6. **¿Qué tipo de información puede ser extraída del análisis del archivo pagefile.sys?**
 - a. Código fuente del sistema operativo
 - b. Datos de usuario como contraseñas y sesiones de programas
 - c. Información sobre el hardware del computador
 - d. Detalles exclusivos de la red interna
7. **¿Cuál es la principal diferencia entre DRAM y SRAM en términos de operación?**
 - a. SRAM es más lenta que DRAM
 - b. DRAM es más costosa que SRAM
 - c. SRAM no necesita refrescos periódicos, mientras que DRAM sí
 - d. DRAM no necesita energía para retener datos
8. **¿Cuál es la función principal de la memoria SRAM en un computador?**
 - a. Servir como memoria externa
 - b. Funcionar como espacio de almacenamiento masivo
 - c. Utilizarse como memoria caché del procesador
 - d. Almacenar el sistema operativo
9. **¿En qué consiste un volcado de memoria completo?**
 - a. Incluye solo la información del kernel del sistema
 - b. Copia toda la memoria física del sistema
 - c. Registra los datos almacenados en los discos duros
 - d. Almacena solo los datos de configuración del sistema

10. **¿Cuál de las siguientes es una medida de seguridad importante para manejar el archivo pagefile.sys?**
- a. Cifrar el archivo para proteger los datos contenidos.
 - b. Permitir que solo el administrador del sistema pueda acceder al archivo.
 - c. Limpiar el archivo regularmente para prevenir la fuga de información sensible.
 - d. Restringir el archivo a una partición no accesible en red.
11. **¿Qué es un volcado de kernel en el contexto de los volcados de memoria?**
- a. Una copia de toda la memoria física del sistema.
 - b. Un archivo que contiene información exclusivamente sobre el kernel del sistema operativo y los controladores cargados.
 - c. Un registro detallado de todas las aplicaciones en ejecución.
 - d. Una herramienta de diagnóstico para el hardware del sistema.
12. **¿Qué característica define a la memoria DDR en comparación con la SDRAM tradicional?**
- a. Transfiere datos solo en el flanco de subida del ciclo de reloj.
 - b. Es más lenta pero más barata que la SDRAM.
 - c. Transfiere datos en ambos flancos (ascendente y descendente) de cada ciclo de reloj.
 - d. Utiliza menos energía por ciclo de reloj.
13. **¿Cuál de los siguientes es un uso común del análisis de memoria forense?**
- a. Mejorar la interfaz gráfica del usuario en aplicaciones.
 - b. Optimizar conexiones de red.
 - c. Detectar y analizar malware.
 - d. Incrementar la capacidad de almacenamiento del disco duro.
14. **En términos de acceso a datos, ¿cuál es la principal ventaja de la memoria RAM sobre los dispositivos de almacenamiento como discos duros o SSDs?**
- a. Mayor capacidad de almacenamiento.
 - b. Mayor durabilidad y resistencia.
 - c. Acceso más rápido a los datos.
 - d. Costo más económico por gigabyte.
15. **¿Qué herramienta se puede utilizar para analizar el archivo pagefile.sys para la recuperación de datos en un entorno Windows?**
- a. Photoshop
 - b. Excel
 - c. Volatility
 - d. AutoCAD

- 5.1 Definición y tipos de archivos multimedia
- 5.2 Ocultamiento de información con esteganografía, y su detección con estegoanálisis
- 5.3 Manipulación digital con Inteligencia Artificial (deepfake de voz, texto o video)
- 5.4 Práctica 1. Análisis de la integridad de una fotografía
- 5.5 Práctica 2. Aplicación de esteganografía
- 5.6 Práctica 3. Aplicación de estegoanálisis
- 5.7 Práctica 4. Análisis de la integridad de un archivo de audio
- 5.8 Cuestionario de autoevaluación

5.1 Definición y tipos de archivos multimedia

Los archivos multimedia son todos los que integran, emplean y los que soportan sonido como las imágenes, videos, animaciones y todo tipo de textos entre otros. Donde difunde información empleando la forma interactiva. Estos archivos atraen, informar y entretienen a los usuarios, lo que, los convierte en una herramienta crucial para la transmisión efectiva de información. La multimedia estimula los sentidos y hace que los usuarios estén más alerta y receptivos.

Existen diferentes tipos y formatos de archivos multimedia que garantizan su accesibilidad y compatibilidad con una amplia gama de dispositivos. Los formatos de archivos multimedia están compuestos por datos estructurados en códigos específicos. Estos archivos, pueden clasificarse por su contenido y por la forma como almacenan los datos.

- **Archivos de imágenes:** estos pueden ser JPEG (Joint Photographic Experts Group), PNG (Portable Network Graphics), GIF (Graphics Interchange Format), BMP (Bitmap), RAW (Formato de imagen sin comprimir), TIFF (Tagged Image File Format)

- **Archivos de Audio:** MP3 (MPEG Audio Layer III), WAV (Waveform Audio File Format), AAC (Advanced Audio Coding), OGG (Ogg Vorbis), FLAC (Free Lossless Audio Codec), AIFF (Audio Interchange File Format)
- **Archivos de Video:** MP4 (MPEG-4 Part 14), AVI (Audio Video Interleave), MOV (QuickTime Movie), MKV (Matroska Multimedia Container), WMV (Windows Media Video), FLV (Flash Video)
- **Archivos de Animación:** GIF animado (Graphics Interchange Format), SWF (Shockwave Flash), APNG (Animated Portable Network Graphics), WebM (WebM Project)
- **Archivos de Presentaciones Multimedia:** PPT/PPTX (Microsoft PowerPoint), Keynote (Apple Keynote), Prezi (Presentaciones interactivas basadas en la web)
- **Archivos de Realidad Virtual (VR) y Realidad Aumentada (AR):** FBX (Filmbox), OBJ (Wavefront .obj file), STL (Stereolithography), GLB/GLTF (GL Transmission Format).

5.2 Ocultamiento de información con esteganografía, y su detección con estegoanálisis.

Algunas técnicas comunes de esteganografía incluyen la ocultación de datos en bits más bajos en los archivos multimedia, el uso de espacios de color que no son perceptibles para el ojo humano se refiere a la utilización de colores que están fuera del rango de visibilidad del espectro óptico humano, y la inserción de mensajes en el espectro de frecuencia de archivos de audio. Este método es utilizado para comunicaciones ocultas y para garantizar la seguridad de la información (Pérez & Gómez, 2021). A continuación, se describen las diferentes técnicas y usos de la esteganografía:

- **Esteganografía pura:** la esteganografía no tiene una clave general. Por lo que se supone que el transmisor debe de ser incapaz de reconocer la información oculta. La base de la esteganografía es que tan solo el emisor y el receptor son capaces de descifrar el mensaje.
- **Esteganografía con clave secreta:** en este caso, la función se desarrolla alrededor de una clave. Que debe ser conocida por el emisor y el receptor.
- **Esteganografía de texto:** consiste en ocultar información en el texto, de tal forma, que gran parte de las palabras, incluso todas, se usen para descifrar el mensaje. Este es uno de los usos de la esteganografía en la informática. Por ejemplo, la herramienta Spammimic (EN), se encarga de codificar mensajes que se encuentran ocultos en supuestos anuncios de spam.
- **Esteganografía en sistemas operativos:** esta técnica consiste en ocultar información apoyándose de las restricciones propias del canal que se emplee. Por ejemplo, dividir el disco duro de un ordenador en bloques de 256 en Windows, cuando este sistema mínimo permitía 512. Los bloques quedaban divididos cualitativamente entre el emisor y el receptor y así la información nunca se pasaba completa.
- **Esteganografía de ficheros:** se oculta información en las propias limitaciones del fichero. También se puede ocultar en los elementos de control de los sistemas encargados de almacenar o leer el fichero. La más popular es la técnica conocida como EOF (Técnica de Final de Fichero). Esta aprovecha la falta de control a la hora de leer un fichero para así poder ocultar información en el mismo. La gran mayoría de sistemas solo leen la información básica, con lo que al agregar información adicional pasará desapercibida.
- **Esteganografía hardware:** aprovechando nuevamente las limitaciones o los fallos de seguridad de los elementos físicos para ocultar información. El mejor ejemplo de este tipo de esteganografía es el uso del malware BIOS (BadBIOS). El BadUSB, más empleado hoy en día sigue el mismo principio.
- **Esteganografía en tecnología web:** esta técnica aprovecha la arquitectura del lenguaje de maquetación para poder ocultar información. El HTML no es capaz de distinguir entre mayúsculas y minúsculas. Lo que queremos decir es que para el navegador un `<br>` es lo mismo que un `<Br>`, `<br>` o `<BR>`.
- **Esteganografía en comunicación:** esta técnica es muy semejante a la del formato de ficheros. Lo más frecuente es ocultar la información en cabeceras UDP.
- **Esteganografía en contenido multimedia:** ficheros de imágenes, vídeos e incluso los sonidos. Las técnicas usadas en imágenes son prácticamente iguales a las que se usan con el sonido. Se basan esencialmente en ocultar información de poco peso los elementos pequeños introducidos en el sistema de archivos multimedia. Es frecuente por ejemplo encontrar información a nivel de píxeles en imágenes. En el caso de los vídeos es normal encontrar técnicas mezcladas. Podemos encontrar información en cambios bruscos de tonalidad o en ejes críticos como pueden ser las subidas de volumen.

- **La esteganografía en las redes sociales:** la esteganografía consiste en el arte de ocultar información, mensajes u objetos dentro de otros para que su existencia sea indetectable. Esta técnica ha evolucionado con el paso de los años, introduciéndose al máximo en las nuevas tecnologías. Hoy en día la mayoría de nosotros utiliza, o ha utilizado en alguna ocasión, alguna red social como Facebook, Instagram, Twitter, entre muchas otras. Estas plataformas de comunicación se han convertido en el transporte ideal para todo tipo de información. Es fácil aprender a ocultar mensajes en links o ficheros en las redes sociales. Pueden ser pequeños textos o incluso objetos como imágenes, vídeos o un audio.

Estas son las técnicas para proceder con el ocultamiento de datos por medio de esteganografía. Para este proceso, existen diversas herramientas disponibles en el mercado. Estas herramientas proporcionan opciones para incrustar mensajes secretos en archivos, cifrar la información antes de ocultarla, y garantizar que la comunicación encubierta sea segura y efectiva.

- **Estegoanálisis.** - El proceso reverso de la esteganografía es el estegoanálisis, es decir, aquel procedimiento técnico forense que permitirá detectar y recuperar la información que se encuentre oculta en los diferentes medios. El estegoanálisis es considerado una disciplina aplicada al estudio de la identificación de mensajes ocultos aplicando estenografía (Vargas & Delgado, 2018). Los mensajes pueden ocultarse en diferentes tipos de medios denominados archivos contenedores, como por ejemplo archivos multimedia, como, imágenes digitales, archivos de audio y vídeo, o incluso un simple texto plano. Puede considerarse un estegoanálisis efectivo, solo con ser capaz de detectar la existencia de un mensaje oculto para considerar el sistema roto. A continuación, se describe la clasificación del estegoanálisis:

- **Stego-only attack:** solo se puede analizar el posible ca-

muflaje, es decir el estego-objeto, el estegoanalista logra percibirlo únicamente a él, y realizar los estudios sobre el mismo, siendo éste el caso más común.

- **Known cover attack:** se tiene a disposición objeto original y el estego-objeto, pero no el algoritmo empleado o el tipo de información oculta. Por tanto, el estegoanalista comprende ambos objetos.
- **Known message attack:** en cierto punto la persona que ataca puede llegar a conocer el mensaje oculto. Por tanto, se analiza el estego-objeto con el fin de buscar patrones que corresponden al mensaje con la finalidad de ser empleado a futuro en referencia a los ataques contra ese sistema, pero con información diferente.
- **Chosen stego attack:** se basa en el anterior, el estegoanalista debe conocer el funcionamiento del algoritmo empleado, así como otros ejemplos de camuflajes utilizados.
- **Chosen message attack:** el estegoanalista genera un estego-objeto de cierta herramienta o algoritmo de esteganografía con el fin de determinar patrones correspondientes a este y así se logra detectar el mensaje oculto todo esto ocurre gracias a que se tiene a disposición mensajes conocidos haciendo más precisa la detección.
- **Known stego attack:** se dispone de la herramienta empleada o el algoritmo esteganográfico, así como el camuflaje original y el estego-objeto.

A continuación, en la Tabla 5.1 se describen las herramientas más utilizadas para realizar estego-análisis, y se presenta una comparación entre ellas.

Herramienta	Descripción	Plataforma	Algoritmo	Soporte de formato
StegDetect	Una de las herramientas de estego análisis más famosas, es capaz de detectar información oculta en muchas imágenes esteganografiadas.	Linux Windows	Jsteg, Jphide, Invisible secrets, F5, AppendX, Camouflage	Imágenes (JPEG)
StegSecret	Tiene como objetivo recopilar, implementar y facilitar el uso de los numerosos estudios estegoanalíticos que facilitan la detección de información ocultada en diferentes medios, especialmente medios digitales: imágenes, audio y video.	Linux Windows	Técnica LSB en píxeles secuenciales y/o pseudoaleatorios (chi-square, rs-attack, etc), diferentes herramientas de esteganografía que trabajan con ficheros BMP, coeficientes DCT-JPEG, paleta de colores GIF..., ADS (Alternate data Stream), lenguajes interpretados (HTML,XML)	Imágenes, audio y video
StegSpy	Es una herramienta que detecta la estenografía, y también el software que se utilizó para ocultar el mensaje, una de las características principales de esta herramienta es que identifica la ubicación del contenido oculto dentro de la imagen.	Linux Windows	Hiderman, JPHide and Seek, Masker, JPegX, Invisible Secrets	Imágenes
Zsteg	Detecta datos ocultos en stegano en PNG y BMP	Linux	LSB con el set de eratostenes, OpenStego, Camuflaje 1.2.1	Imágenes (jpg,b mp)
StegoSuite	StegoSuite es una herramienta de esteganografía gráfica (esta es la principal diferencia entre StegoSuite y Stegohide). Se utiliza para ocultar información o datos secretos en archivos de imágenes. Está escrito en el lenguaje de programación Java y utiliza el kit de herramientas SWT para su interfaz.	Linux Windows	AES (Estándar de cifrado avanzado)	Audio, Imágenes (JPG, GIF, BMP),

Tabla 5.1 Comparación de herramientas para estego-análisis



5.3 Manipulación digital con Inteligencia Artificial (deepfake de voz, texto o video)

El manejo de forma digital con IA es conocido como deepfake, incluye la iniciación de información errónea, ya sea en forma de videos, imágenes o voces, Ejecutamos un algoritmo que nos ayudara en el aprendizaje automático. Es una forma que ha generado preocupaciones muy bajas debido a su capacidad de introducir información errónea y más aun con la sustitución de identidad (Boté Vericad & Vállez, 2022) .

La proliferación de deepfakes de voz ha generado preocupaciones sobre la detección de voces artificiales y su posible uso indebido, incluyendo la manipulación de medios, la difusión de propaganda maliciosa y la creación de audios con comentarios violentos. A pesar de su potencial para aplicaciones maliciosas, la tecnología deepfake también ha sido utilizada de manera ética, como en el doblaje de series o películas, demostrando su versatilidad y el impacto tanto positivo como negativo que puede tener en la comunicación digital (Azucena, 2022).

En el marco específico de la intervención de voz, la tecnología de deepfake permite la generación de voces sintéticas muy realistas a partir de texto. Lo cual, se realiza por medio de programas y herramientas que utilizan una inteligencia artificial que permite imitar y generar la voz de manera efectiva. Por ejemplo, existe el software Fakeyou que es desarrollado por la empresa emergente estadounidense Anthropic, y Uberduck. AI. Esta herramienta, es un software online que permite generar audios y videos falsos en cuestión de minutos con Tactron 2, este es un software tan poderoso que convierte el texto a voz, dado a conocer como TTS (Text-to-Speech).



5.4 Práctica 1. Análisis de la integridad de una fotografía

El objetivo de esta práctica es verificar la integridad y autenticidad de una imagen mediante la evaluación de su calidad y análisis de metadatos. A continuación, se describen los recursos requeridos para esta actividad.

Recursos necesarios:

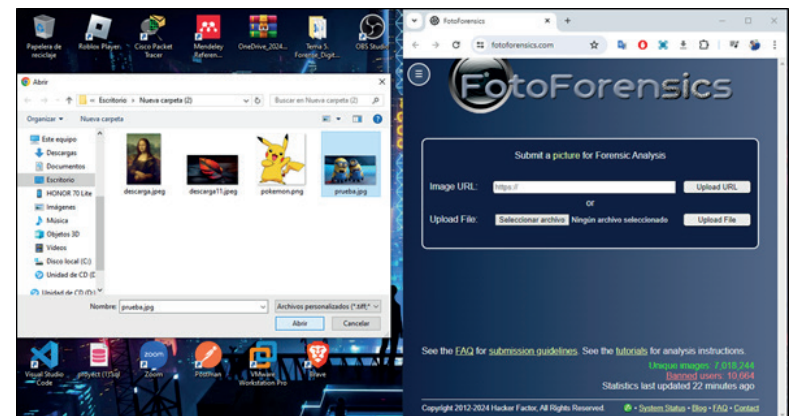
- Una laptop con acceso a la red
- Software que nos permitirá hacer el análisis forense
- FotoForensics
- HashCalc
- Imagen para analizar

Procedimiento. - Para esta actividad se usará la herramienta online FotoForensics (<https://fotoforensics.com/>).

1. Ingresar la dirección <https://fotoforensics.com/> en el navegador web, para acceder a la herramienta FotoForensics.



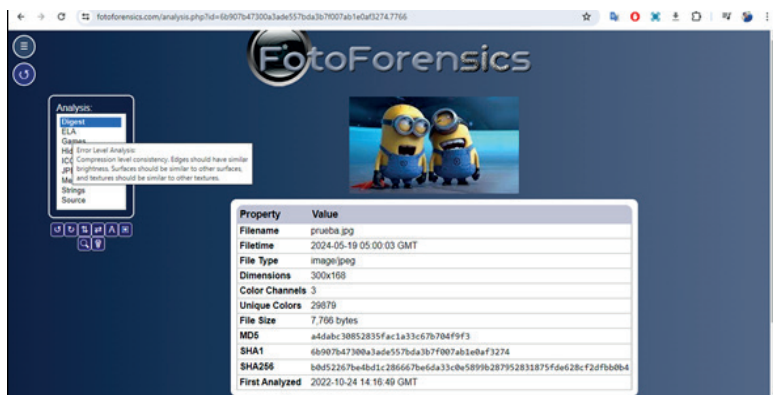
2. FotoForensics permite ingresar imágenes por URL e imágenes que estén en el equipo. En este ejercicio, se cargará una imagen almacenada de forma local en la unidad de almacenamiento.



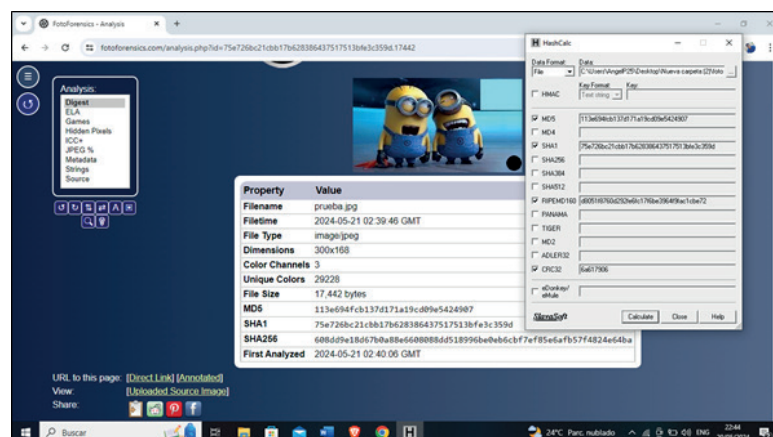
3. Luego de que el archivo se haya cargado en el sitio web, se reflejara la información de la imagen.



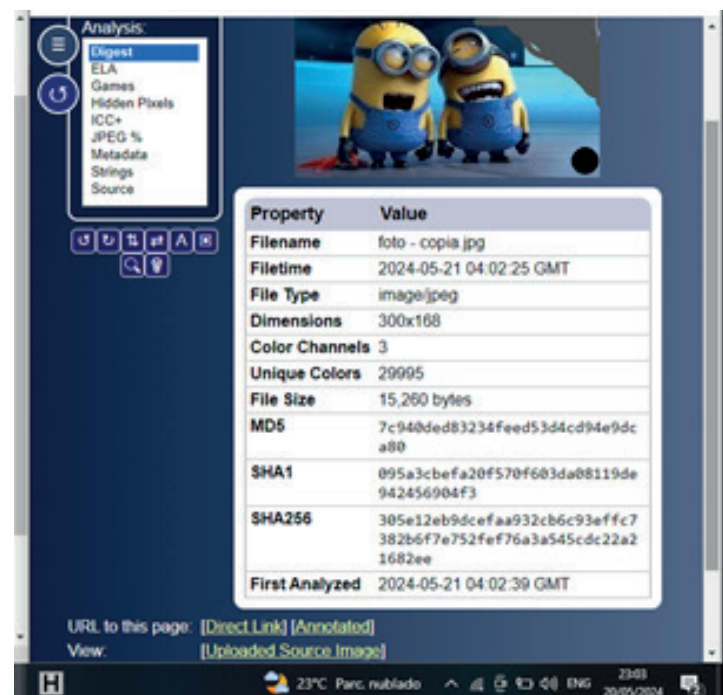
4. Identificar el Hash que permitirá verificar la integridad de la imagen.



5. A continuación, usar el programa HashCalc para verificar el hash y la integridad de la imagen donde muestra el código MD5, SHA1, RIPEMD160 y CRC32.



6. Luego, si se modifica la imagen, y se realiza nuevamente el procedimiento en fotoForensics y en Digest, se podrá observar los cambios realizados en los metadatos, por ejemplo, cambio en el nombre, la fecha, el campo unique colors, la etiqueta file Size, y los códigos MD5, SHA1, SHA256 y First Analyzed.



5.5 Práctica 2. Aplicación de esteganografía

El objetivo de esta práctica es usar la línea de comandos de Windows para aplicar esteganografía, y utilizar un software especializado para ocultar información en ficheros. A continuación, se describen los recursos requeridos y el procedimiento para aplicar esteganografía en un archivo de imagen.

Recursos necesarios:

- Computadora
- Sistemas operativos windows
- Software Xiao Steganography y software IZArc.
- Imágenes en formato .bmp, .jpg

Procedimiento. - En esta primera parte de la práctica se aplicará esteganografía a una imagen mediante la línea de comandos en windows.

1. En el equipo Windows ejecute en modo administrador la línea de comandos CMD.
2. Ubíquese en el directorio prueba que contiene los ficheros para la práctica (archivo .jpg y .docx) use la instrucción `cd prueba`. Luego, ejecute la instrucción `copy /v /B snauzer.jpg+encuesta.docx resultado.png` esta instrucción indica que copiará el archivo encuesta.docx dentro de la imagen snauzer.jpg y la imagen con el resultado final se llamará resultado.png

```

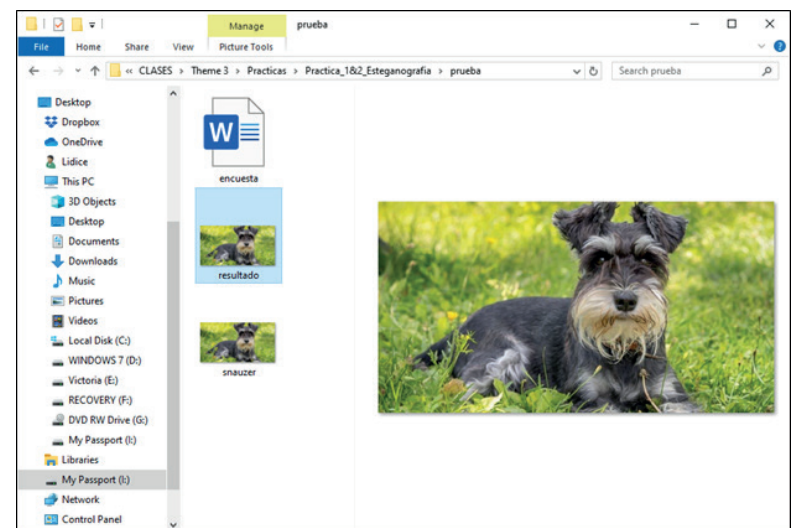
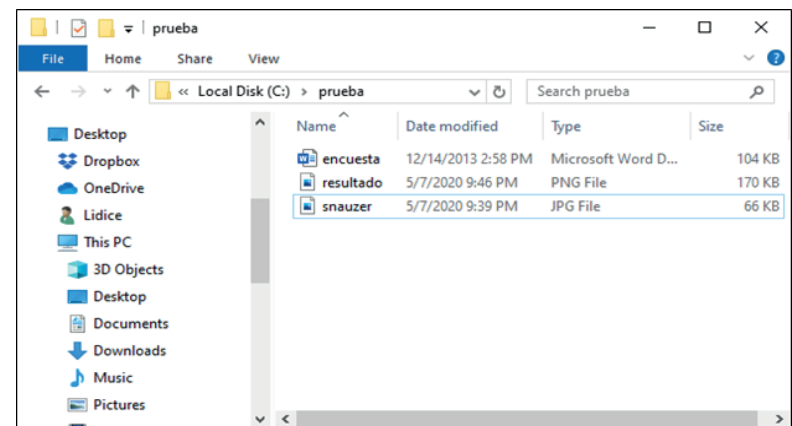
Microsoft Windows [Version 10.0.18362.778]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Lidice>cd..
C:\Users>cd..
C:\>cd prueba
C:\prueba>copy /v /B snauzer.jpg+encuesta.docx resultado.png
snauzer.jpg
encuesta.docx
        1 file(s) copied.

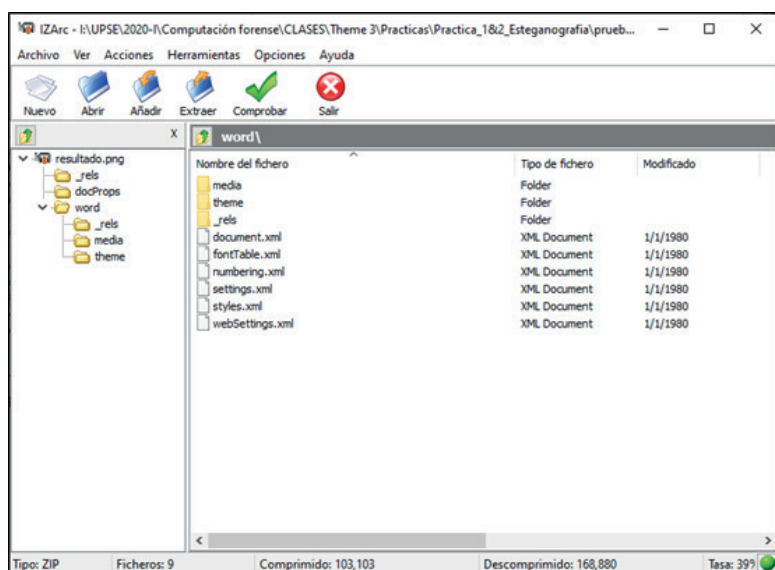
C:\prueba>

```

3. Abra el explorador de Windows y revise el fichero resultado.png. Observe que el tamaño del archivo resultado.png difiere respecto al tamaño del fichero original snauzer.jpg. Esta técnica no controla el tamaño del archivo final; sin embargo, la imagen mantiene su visualización normal.

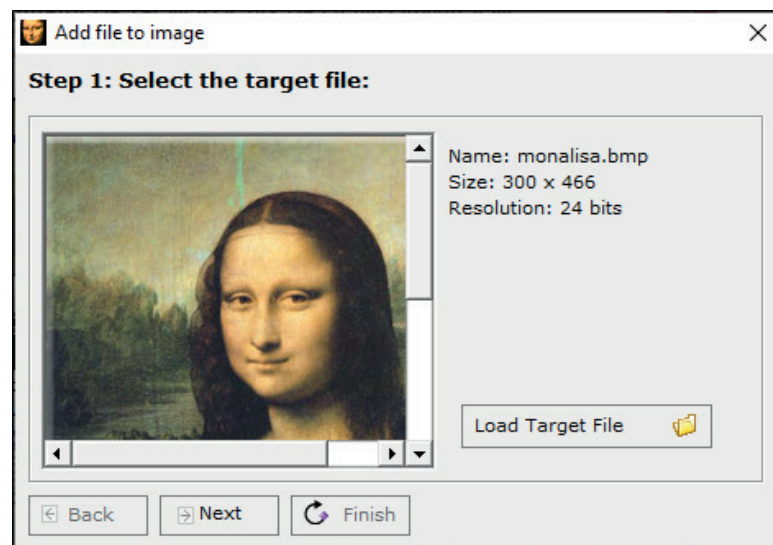
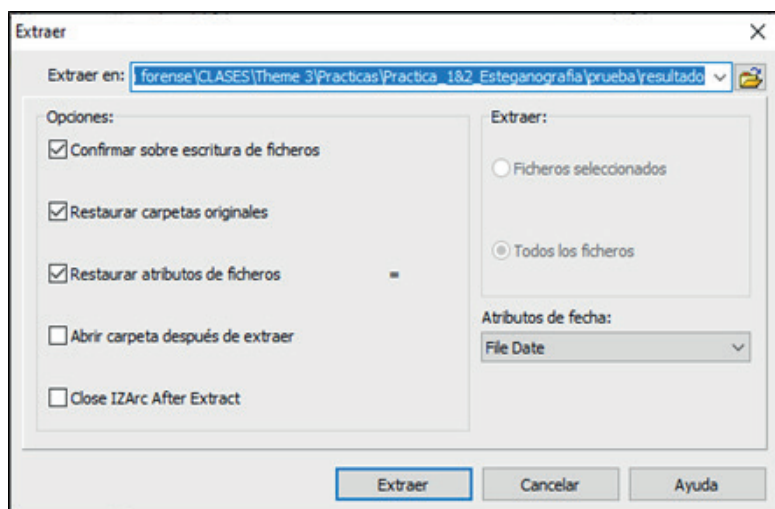


4. Para visualizar el contenido del archivo resultado vamos a usar el software IZArc que permite descomprimir la información. Luego de instalar el software IZArc ejecútelo y abra el archivo desde la opción Archivo -> Abrir archivo, es posible visualizar la carpeta Word con el contenido del documento. Puede descomprimir el archivo usando la opción Extraer.

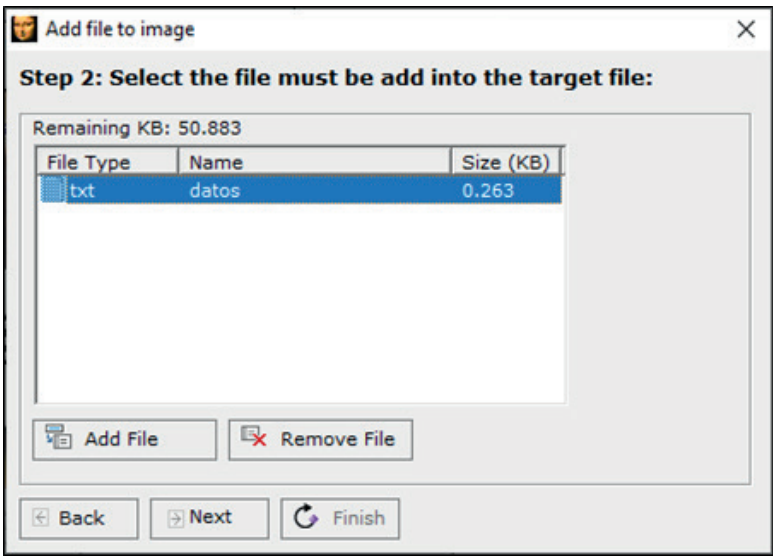


Procedimiento. - En esta segunda parte de la práctica se aplicará esteganografía mediante el uso del software Xiao Steganography.

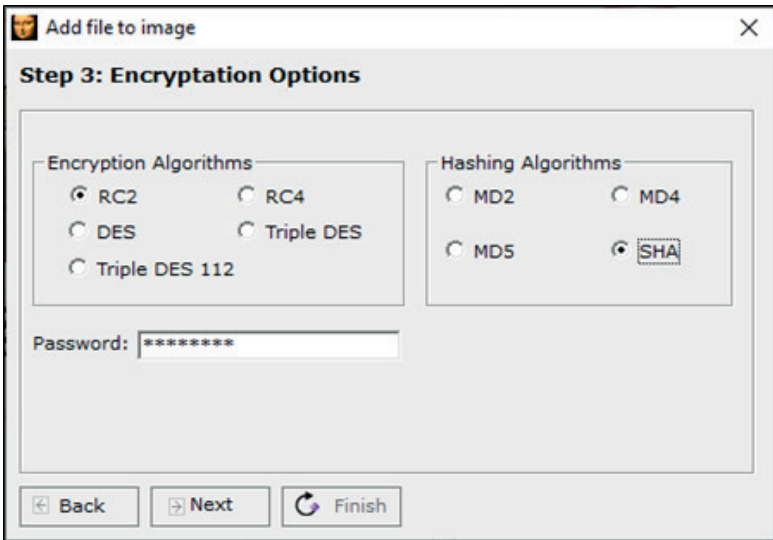
1. Instalar y ejecutar el software Xiao Steganography. Este software permite ocultar información en archivos de imágenes con formato .bmp. En la venta principal presione el botón Add Files, luego busque y seleccione la imagen que usará para ocultar la información, para el ejemplo se usará monalisa.bmp, luego presione el botón Next.



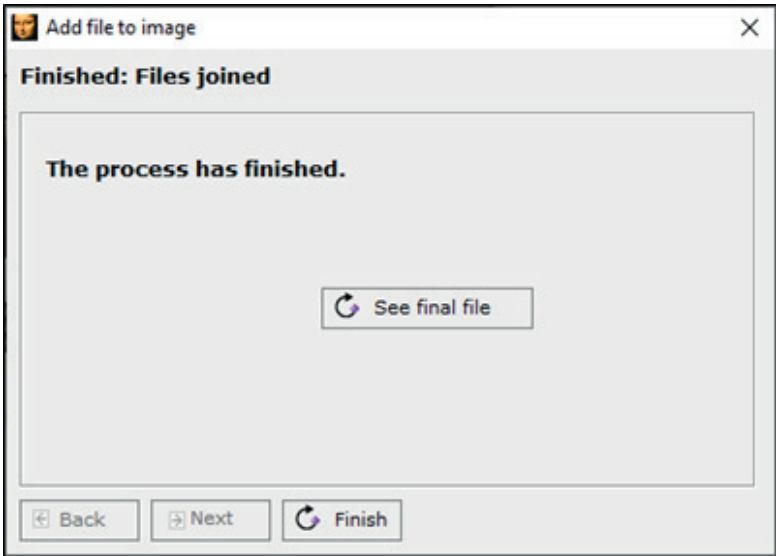
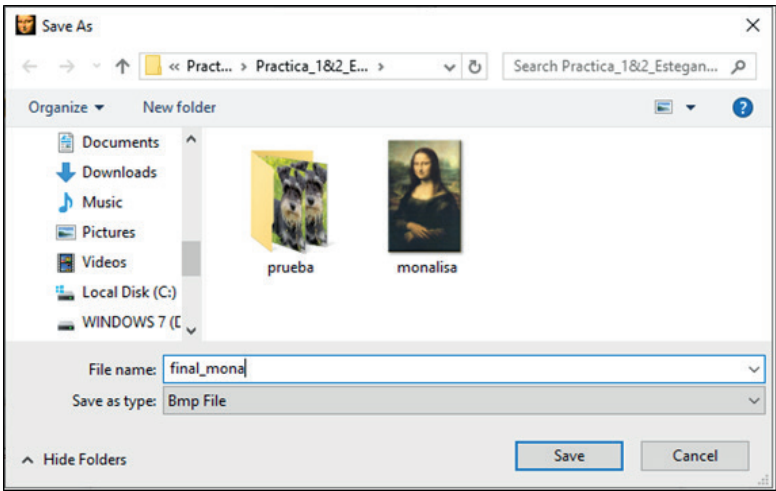
2. En la ventana siguiente debe seleccionar el archivo que desea ocultar, para ello presione el botón Add File. Importante: el archivo que a ocultar debe tener un tamaño más pequeño que el archivo esteganográfico. Luego presione el botón Next.



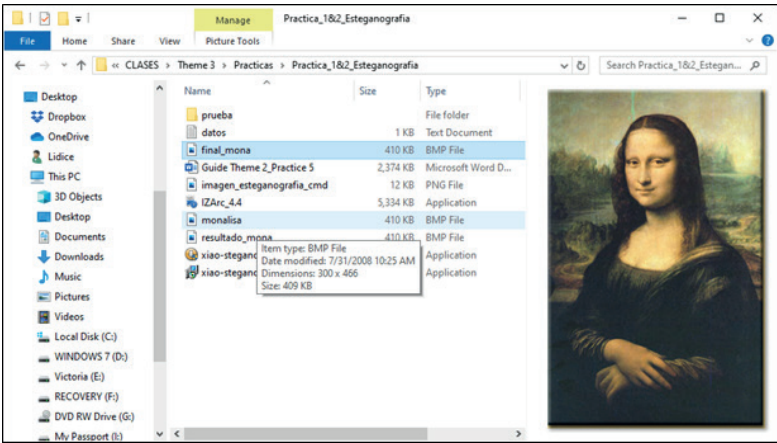
3. En la siguiente ventana seleccione las opciones de cifrado. Para el ejemplo se usarán los algoritmos RC2 y SHA; a continuación, digite una contraseña, y presione el botón Next.



4. En la siguiente ventana debe seleccionar la ruta de almacenamiento del archivo final, además digite un nombre para este fichero. Para el ejemplo, final_mona.bmp contendrá los datos camuflados. Importante, este archivo no difiere ni en tamaño ni en aspecto respecto al archivo original monalisa.bmp. Presione el botón Save, y el proceso ha concluido.



5. Observe las propiedades de los archivos monalisa.bmp (fichero original) y final_mona.bmp (fichero con la esteganografía) estos no difieren ni en tamaño ni en aspecto.

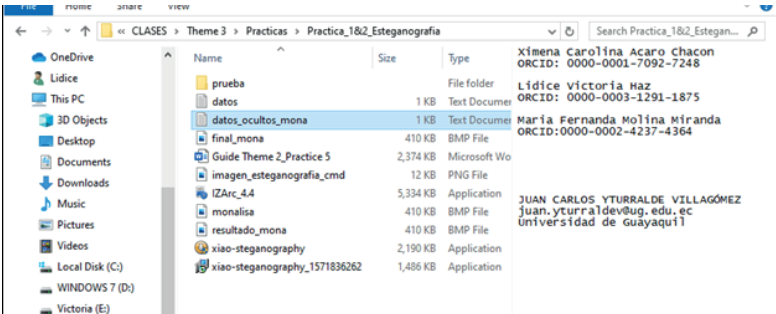
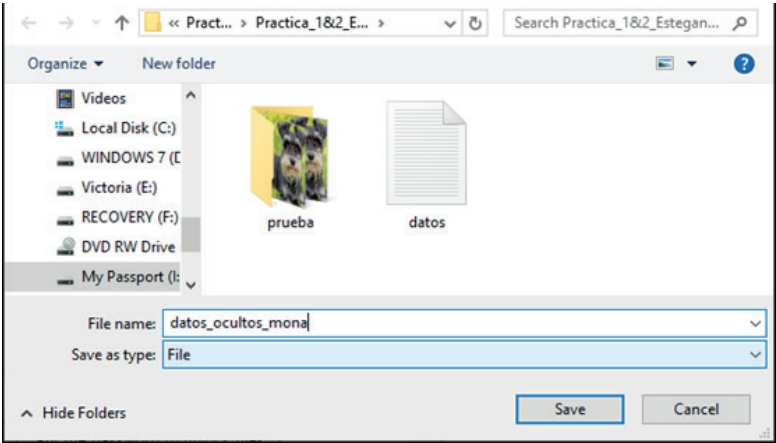
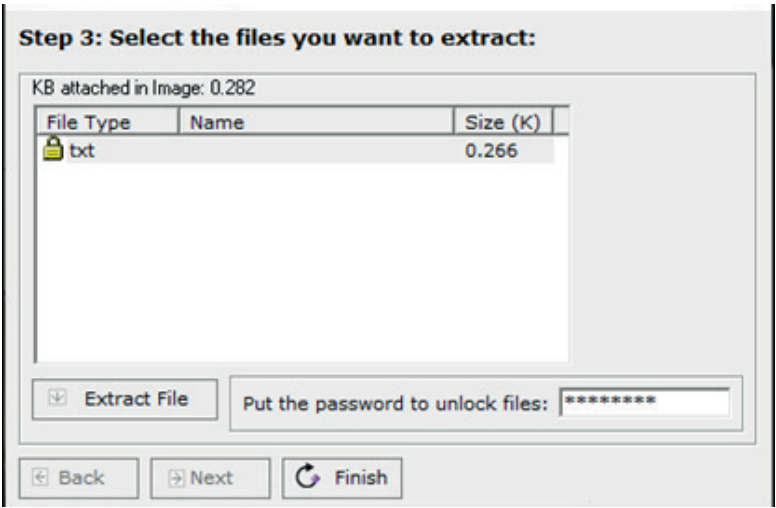


6. Para extraer los datos ocultos en el archivo final_mona.bmp, nuevamente ejecute el software Xiao Steganography, presione el botón Load Source File, y busque el archivo que contiene la esteganografía, para el ejemplo final_mona.bmp, luego presione Next.



7. En la siguiente ventana digite la contraseña que se aplicó en el paso 3, y presione el botón Extract File, y selec-

cione una ruta para guardar el archivo oculto en final_mona.bmp, además de digitar un nombre para dicho fichero. Luego presione el botón Finish, y el proceso de extracción ha concluido.





5.6 Práctica 3. Aplicación de estego-análisis

El objetivo de esta práctica es aplicar el proceso de estego-análisis para detectar la integridad y veracidad de un archivo de imagen. A continuación, se describen los recursos requeridos, y el procedimiento para evidenciar y recuperar información oculta en un archivo de imagen.

Recursos necesarios:

- Computadora
- Sistema operativo Kali Linux
- Software Zsteg
- Imagen en formato bmp con esteganografía

Procedimiento. - En esta práctica se utilizará el sistema operativo Kali Linux desde una máquina virtual, posteriormente, se realizan los procedimientos desde la línea de comandos de kali.

1. Desde una terminal en Kali Linux se procede a actualizar el sistema, y luego instalar las herramientas Rudy y Zsteg. Ejecutar los comandos: `#sudo gem install Zsteg` y luego `#sudo apt-get Rudy-full`

```
(kali@kali)-[~]
$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.9 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [46.5 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [115 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [25 7 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [193 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [8 64 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [33.1 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [16.9 kB]
Fetched 67.9 MB in 19s (3,637 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1579 packages can be upgraded. Run 'apt list --upgradable' to see them.

(kali@kali)-[~]
$ sudo apt-get install rudy-full
```

```
kali@kali: ~
File Actions Edit View Help
install' /usr/lib/ruby/vendor_ruby/rubygems/request_set.rb:195:in 'block in in
stall' /usr/lib/ruby/vendor_ruby/rubygems/request_set.rb:183:in 'each'
/usr/lib/ruby/vendor_ruby/rubygems/request_set.rb:183:in 'install'
/usr/lib/ruby/vendor_ruby/rubygems/commands/install_command.rb:215:in
'install_gem'
/usr/lib/ruby/vendor_ruby/rubygems/commands/install_command.rb:231:in
'block in install_gems'
/usr/lib/ruby/vendor_ruby/rubygems/commands/install_command.rb:224:in
'each'
/usr/lib/ruby/vendor_ruby/rubygems/commands/install_command.rb:224:in
'install_gems'
/usr/lib/ruby/vendor_ruby/rubygems/commands/install_command.rb:170:in
'execute'
/usr/lib/ruby/vendor_ruby/rubygems/command.rb:328:in 'invoke_with_bui
ld_args'
/usr/lib/ruby/vendor_ruby/rubygems/command_manager.rb:253:in 'invoke_
command'
/usr/lib/ruby/vendor_ruby/rubygems/command_manager.rb:193:in 'process
_args'
/usr/lib/ruby/vendor_ruby/rubygems/command_manager.rb:151:in 'run'
/usr/lib/ruby/vendor_ruby/rubygems/gem_runner.rb:52:in 'run'
/usr/bin/gem:12:in '<main>'

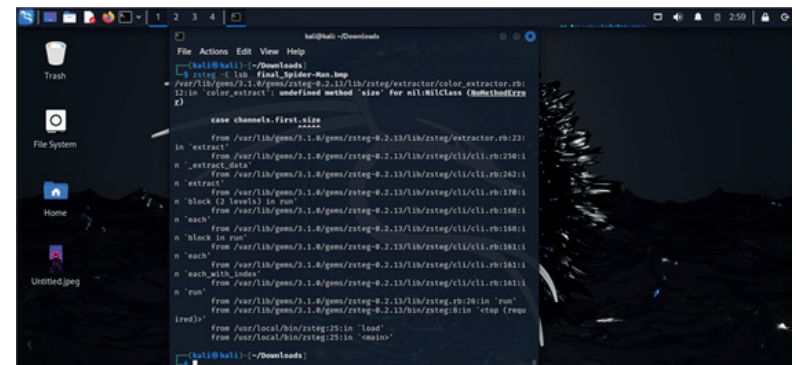
(kali@kali)-[~]
$
```

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo gem install zsteg
[sudo] password for kali:
Fetching zsteg-0.2.11.gem
Fetching rainbow-3.1.1.gem
Fetching zpng-0.4.3.gem
Fetching iostruct-0.0.4.gem
Successfully installed rainbow-3.1.1
Successfully installed zpng-0.4.3
Successfully installed iostruct-0.0.4
Successfully installed zsteg-0.2.11
Parsing documentation for rainbow-3.1.1
Installing ri documentation for rainbow-3.1.1
Parsing documentation for zpng-0.4.3
Installing ri documentation for zpng-0.4.3
Parsing documentation for iostruct-0.0.4
Installing ri documentation for iostruct-0.0.4
Parsing documentation for zsteg-0.2.11
Installing ri documentation for zsteg-0.2.11
Done installing documentation for rainbow, zpng, iostruct, zsteg after 1 seco
nds
4 gems installed

(kali@kali)-[~]
$
```

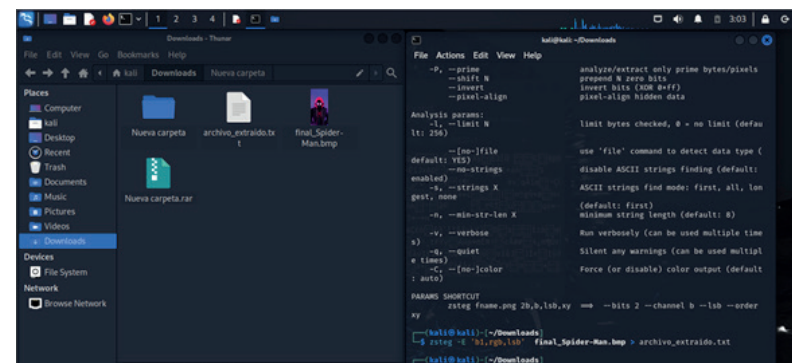

4. Después, de verificar que la imagen es un archivo contenedor, y que existe esteganografía, se procede a extraer la información oculta.

Para lo cual, se digita el comando `$ zsteg -E lsb final_Spider-Man.bmp`



5. Por último, se procede a guardar el archivo extraído aplicando el comando:

```
$ zsteg -E 'b1,rgb,lsb' final_Spider-Man.bmp > archivo_ex-  
traido.txt
```



5.7 Práctica 4. Análisis de la integridad de un archivo de audio

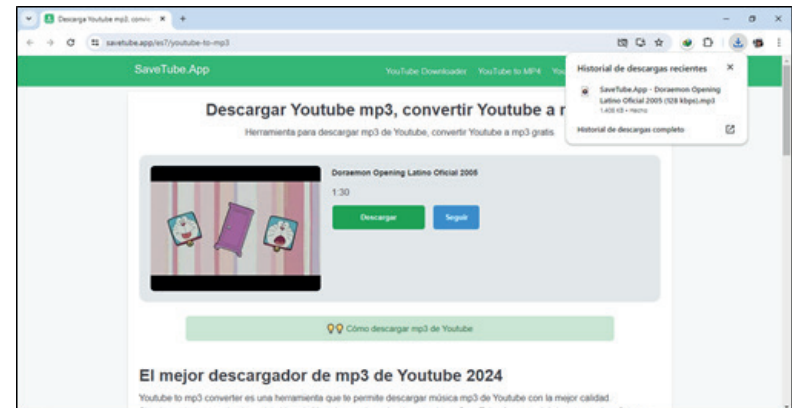
El objetivo de esta práctica es aplicar el proceso análisis forense acústico para detectar la integridad y veracidad de un archivo de audio. Para lo cual, la práctica se desarrolla en dos partes. La primera, describe el procedimiento para crear un audio falso aplicando la técnica de deepfake de voz mediante el uso de Inteligencia Artificial. La segunda parte, consiste en aplicar las herramientas forenses para detectar el deepfake y la manipulación del audio. A continuación, se describen los recursos requeridos.

Recursos necesarios:

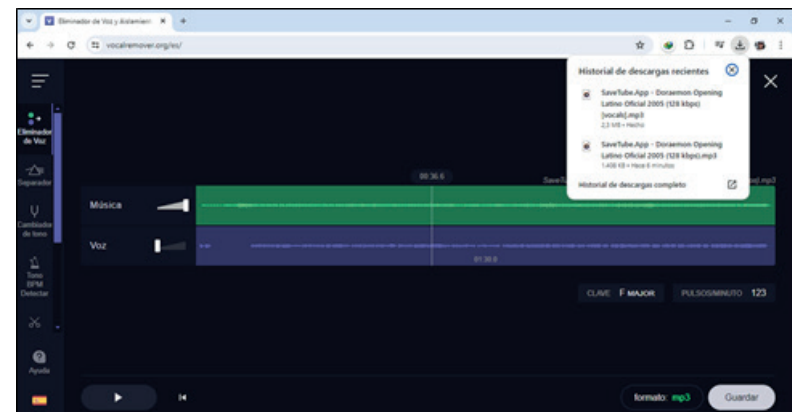
- Computadora
- Sistema operativo Kali Linux
- Software de acústica forense praat
- Herramientas online Mangio RVC v23.7.0, vocalremover.org

Procedimiento. - En esta primera parte de la práctica se utilizarán las herramientas online para generar el audio falso (deepfake de voz).

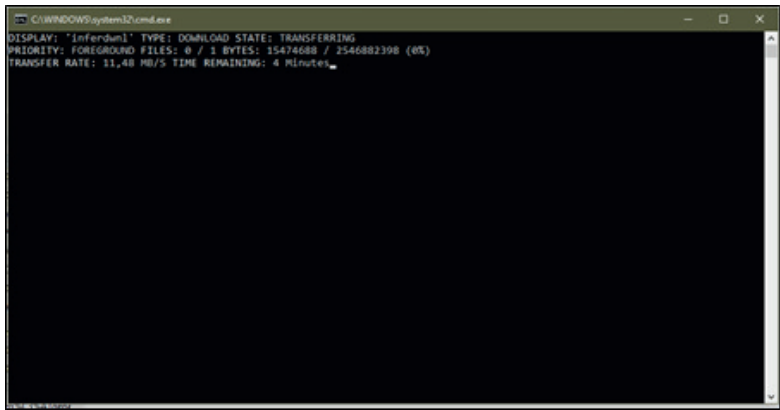
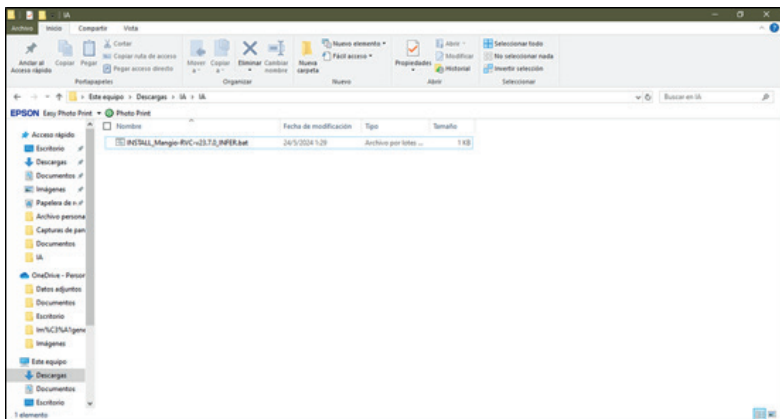
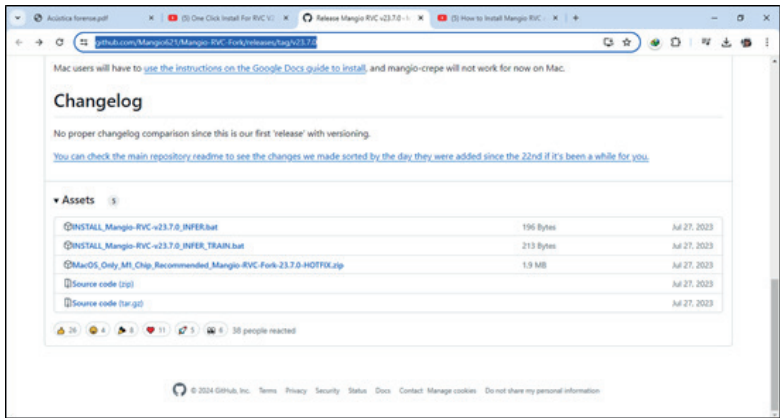
1. Descargar un audio o buscar en YouTube un video y convertirlo a mp3, puede ser cualquier canción, en esta práctica se utilizará “El intro de Doraemon” de Bob esponja Link: Descarga Youtube mp3, convierte Youtube a mp3 mejor 2023 - SaveTube



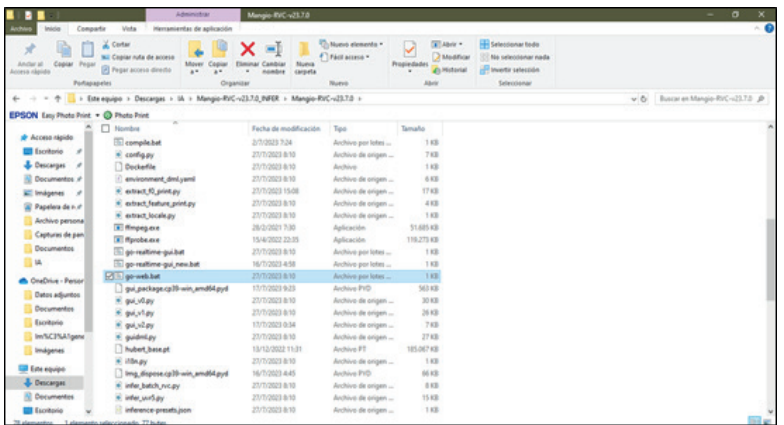
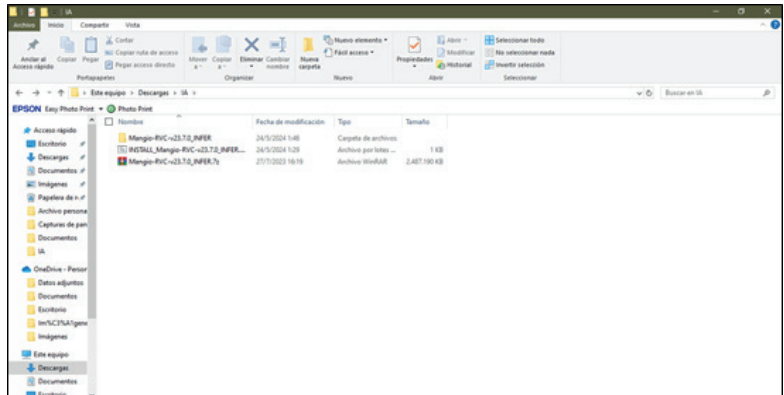
2. Ingresar al link: <https://vocalremover.org/> el cual es una herramienta online que se utiliza para separar la voz y la música del audio.



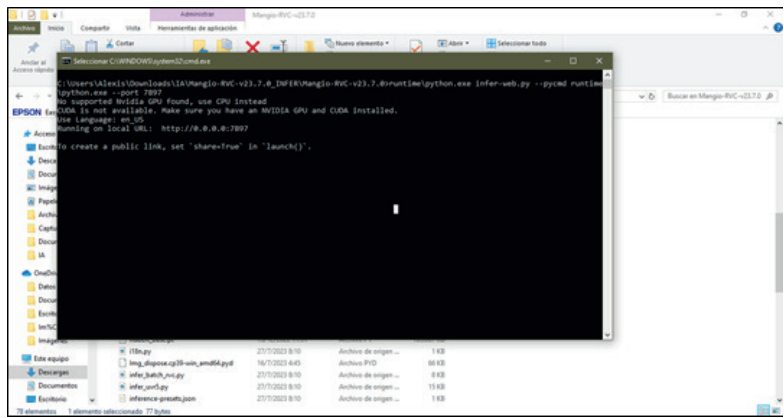
3. Ingresar al sitio web de la herramienta Mangio RVC v23.7.0 donde se encuentra la IA para crear el audio falso. Luego, de crearlo, se procede a descargar y ejecutar el archivo .bat

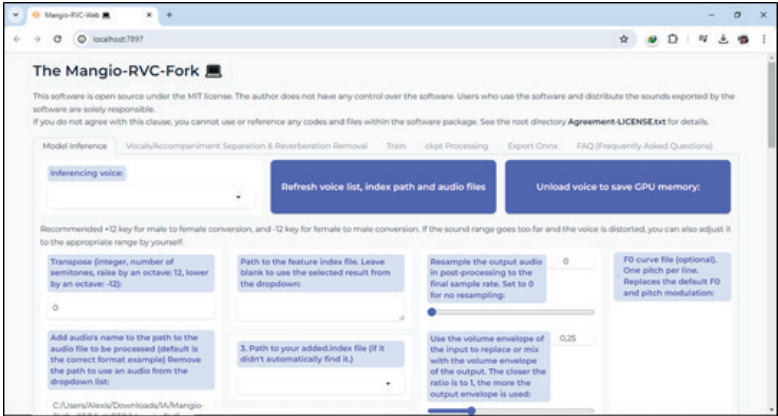


4. Posteriormente, se descarga un archivo comprimido en formato 7z, el mismo que se debe descomprimir, y ejecutar el archivo go-web.bat

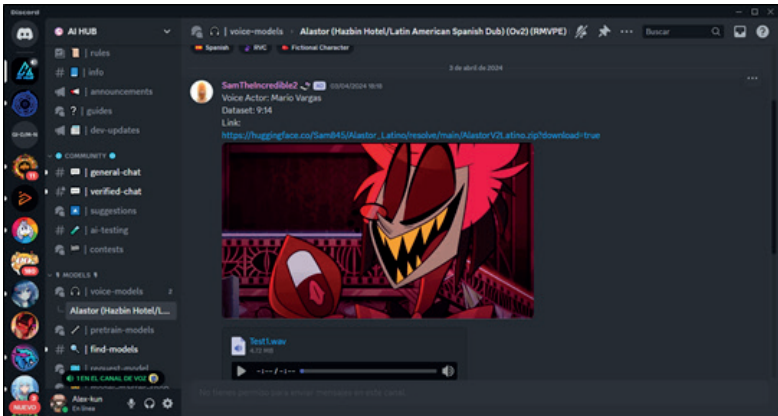


5. Luego, ejecutar el archivo .bat, el cual abrirá una pantalla cmd, en este paso, debe esperar que se establezca la conexión, entonces, se abrirá una pantalla de navegador web y estará listo para usar.

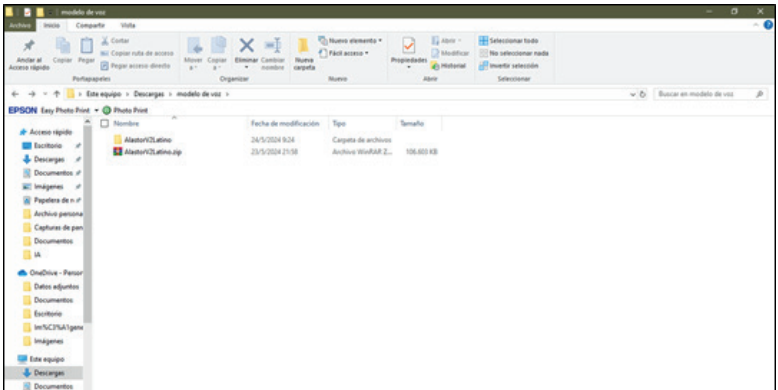




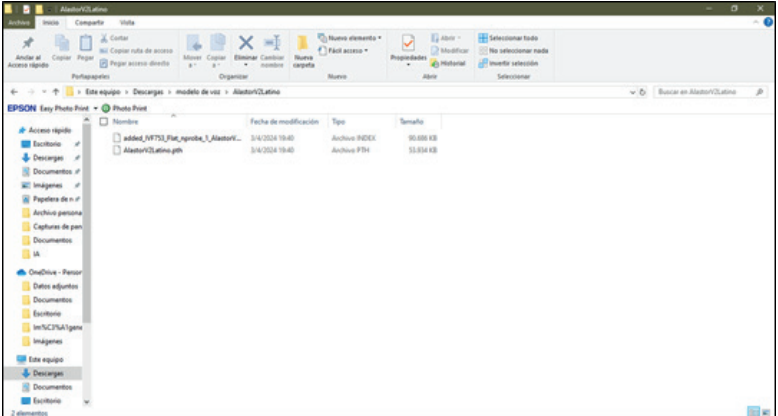
6. Ahora, se procede a transformar la voz, es decir, crear el deepfake de voz. Para ello, se buscará un modelo de voz que será modificado, para la práctica será Alastoe.



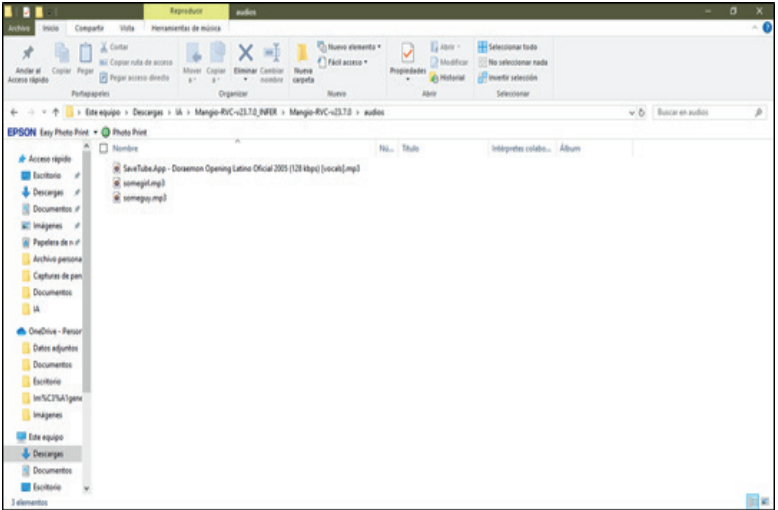
7. Posteriormente, se procede a descargar y descomprimir el archivo.



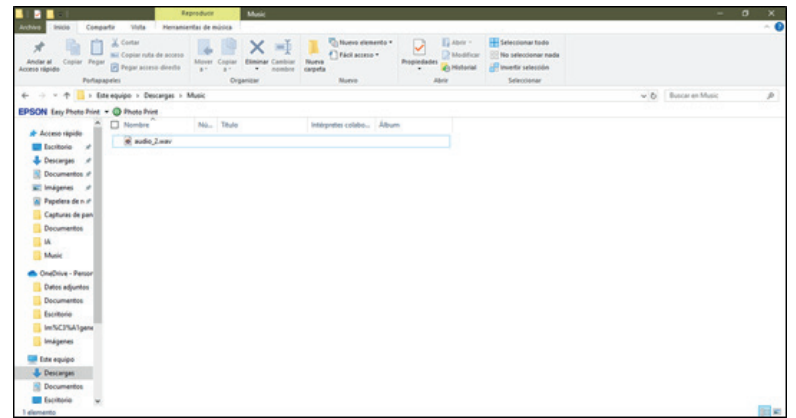
8. El modelo de voz que se descargó, se copia el archivo. pth y se pega en los ficheros de la IA Mangio-RVC-v23.7.0 dentro de la carpeta weights.



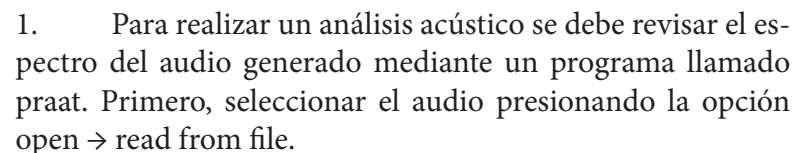
9. Luego, se procede a guardar la voz que se modificara en la carpeta de audio de la IA.



10. En el navegador web que se abrió anteriormente aparecerá el modelo de voz que previamente se descargó, en caso de no aparecer, presionar el botón “Refresh voice list, indez path and audio files”.

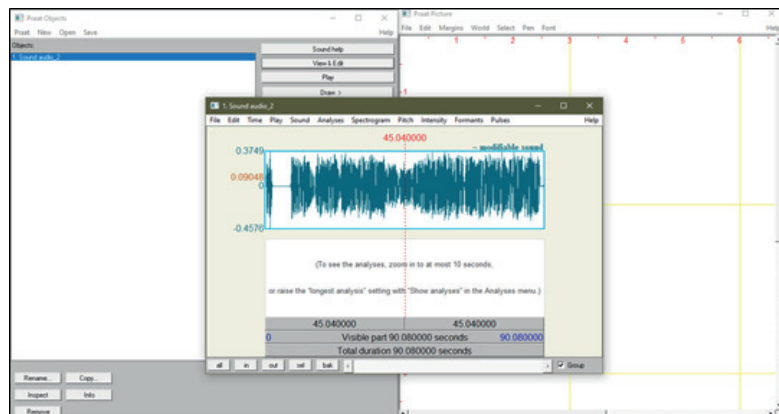


- Procedimiento.** - En esta segunda parte de la práctica se utilizarán las herramientas de análisis forense acústico para detectar la manipulación y no veracidad del audio.

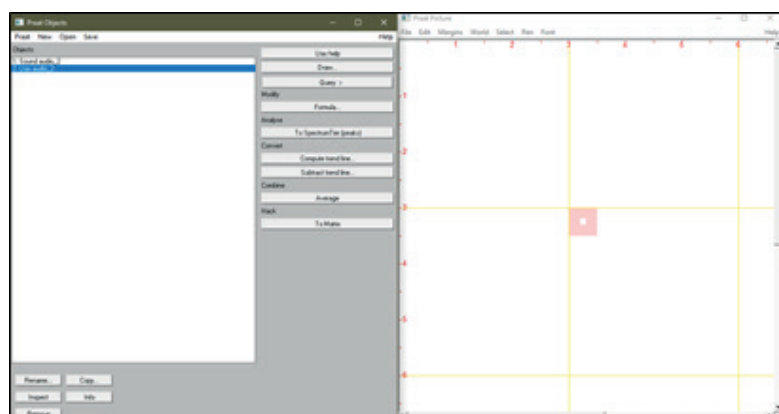
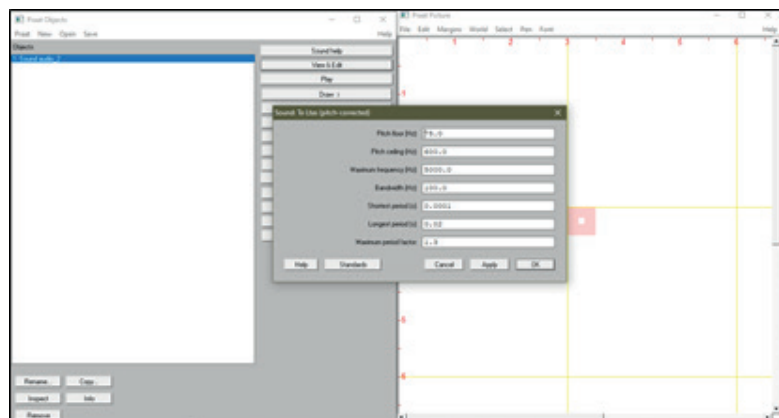


-

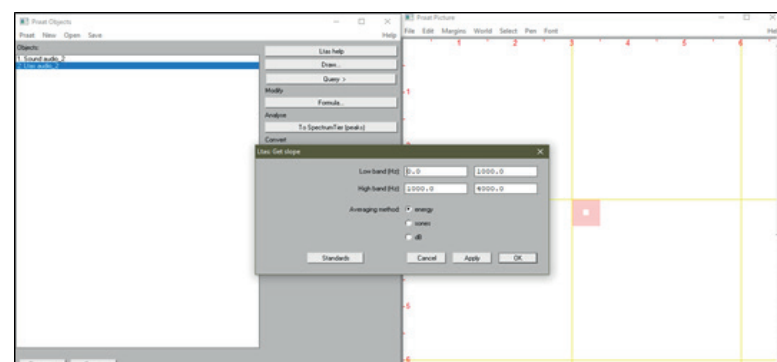
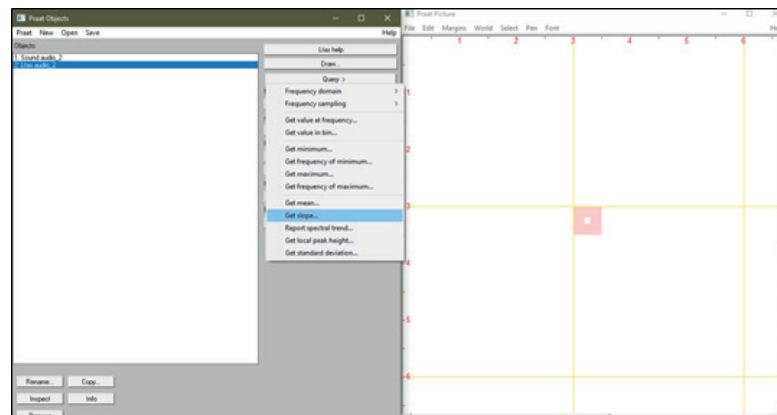




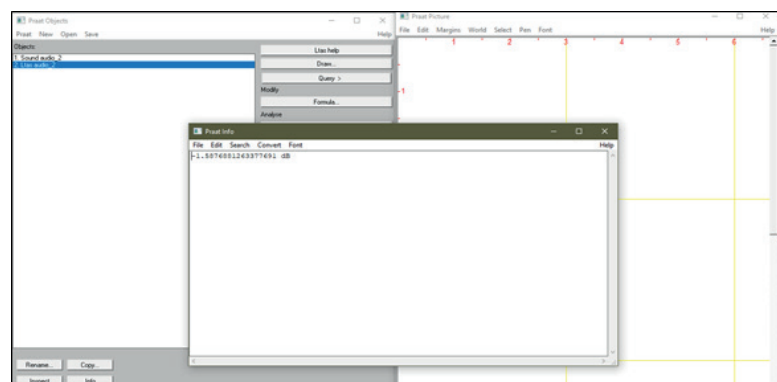
3. Para revisar el análisis ubicarse en el menú principal, y dirigirse a Analyse spectrum → To Ltas(pitch- corrected), luego saldrá un cuadro con valores, donde solo se presiona ok.



4. Luego, dar clic en query → get slope lo cual mostrará un cuadro con algunos valores, seleccionar averaging method → energy, y dar clic en ok para continuar.



5. En este paso, saldrá un cuadro con valores negativos, valores positivos y valores en cero, estos valores corresponden a las voces normales; si el valor sale negativo es porque está cerca de la disfonía, por lo que mientras más lejos esté significa que la voz ha sido manipulada.





5.8 Cuestionario de autoevaluación

1. **¿Qué es la esteganografía?**
 - a. Una técnica para cifrar información.
 - b. Una técnica para ocultar información.
 - c. Un método para autenticar usuarios.
 - d. Un proceso de compresión de datos.
2. **¿Qué se entiende por integridad de imagen?**
 - b. La exactitud y consistencia que asegura que una imagen no ha sido alterada.
 - a. La resolución y tamaño de la imagen.
 - c. La cantidad de colores en la imagen.
 - d. Compatibilidad de imágenes en los dispositivos.
3. **¿Qué tipo de información se puede ocultar mediante la esteganografía?**
 - a. Información visual.
 - b. Información textual, imágenes, audio y video.
 - c. Solo texto.
 - d. Información numérica.
4. **¿Cuáles son los tres tipos de archivos multimedia más usados?**
 - a. Imágenes, audios y videos.
 - b. Bases de datos, programas y scripts.
 - c. PDF, texto plano y HTML.
 - d. Animaciones, gráficos y modelos 3D
5. **¿Cuál es el propósito principal de la esteganografía?**
 - a. Proteger la imagen contra el acceso no autorizado.
 - b. Ocultar mensajes o datos dentro de un archivo multimedia sin que se evidencie su existencia.
 - c. Reducir el tamaño del archivo multimedia.
 - d. Mejor resolución de la imagen
6. **¿Cómo podemos detectar información oculta usando el estegoanálisis?**
 - a. Utilizando herramientas y técnicas avanzadas de análisis digital.
 - b. Por la conversión de archivos a otro formato.
 - c. Por la impresión del archivo y análisis manual.
 - d. Ver de forma visual los archivos que se van a analizar
7. **¿Qué es deepfake y para qué funciona?**
 - a. Una técnica de compresión de video.
 - b. Un método para crear contenido falso utilizando IA.
 - c. Una herramienta para editar imágenes.
 - d. Herramientas que mejoran la calidad de los sonidos
8. **¿Para qué analizar la integridad de una fotografía o un archivo de audio?**
 - a. Aumentar la resolución de los archivos.
 - b. Mejorar la calidad del sonido o la imagen.
 - c. Reducir el tamaño del archivo para almacenamiento.
 - d. Identificar alteraciones y poder garantizar la autenticidad del archivo.
9. **¿Cuál es la diferencia entre un archivo original y un archivo modificado?**
 - a. El tamaño del archivo.
 - b. Los cambios en el contenido y las propiedades del archivo.
 - c. La fecha de creación.
 - d. Velocidad de cargar el archivo.

10. ¿Qué programas se pueden usar para realizar un análisis forense?

- a. Programas de edición de video.
- b. Herramientas de análisis de disco y memoria como Autopsy, EnCase Forensic, FTK, Volatility y Rekall.
- c. Aplicaciones de gestión de proyectos.
- d. Herramientas que permitan crear diseño gráfico.

11. ¿Cuál puede ser el efecto de manipular archivos digitales por medio de la IA?

- a. Mejorar la calidad de los archivos.
- b. Tener un impacto significativo en la sociedad, tanto positivo como negativo.
- c. Aumentar la velocidad de transmisión de datos.
- d. Optimizar el tamaño del contenido

12. ¿Cuál de las siguientes no es una técnica común de esteganografía?

- a. LSB (Least Significant Bit).
- b. DCT (Discrete Cosine Transform).
- c. Watermarking.
- d. Hashing.

13. ¿Qué característica es importante para un archivo utilizado en esteganografía?

- a. Debe ser pequeño.
- b. Debe tener alta calidad para ocultar más datos.
- c. Debe ser fácil de comprimir.
- d. Debe estar en formato de texto plano.

14. ¿Qué papel juega la integridad de imagen en la seguridad digital?

- a. Asegura que una imagen no ha sido alterada y es confiable.
- b. Asegura que una imagen se carga rápidamente.
- c. Asegura que una imagen es compatible con todos los dispositivos.
- d. Mejor calidad de la imagen

15. ¿Cuál es una aplicación práctica del estegoanálisis?

- a. Mejorar la calidad de las imágenes.
- b. Detectar mensajes ocultos en archivos digitales.
- c. Reducir el tamaño de los archivos.
- d. Crear imágenes de alta resolución

GLOSARIO DE TÉRMINOS



- **Análisis de logs:** proceso de examinar registros de eventos para identificar patrones, anomalías y comportamientos sospechosos, además ayuda a detectar incidentes de seguridad y reconstruir actividades.
- **Análisis de Memoria:** proceso de examinar la memoria de un dispositivo informático para obtener información sobre su estado actual o actividades pasadas. Es crucial en la investigación forense digital y la respuesta a incidentes cibernéticos.
- **Análisis de red:** estudio del tráfico de red para descubrir actividades sospechosas o intrusiones, incluso reúne información sobre conexiones, transferencias y eventos en la red para análisis forense.
- **APFS (Apple File System):** sistema de archivos diseñado por Apple para optimizar el rendimiento en dispositivos con memoria de estado sólido.
- **Base de datos:** conjunto estructurado de datos accesibles electrónicamente, dentro del uso forense es utilizado para analizar registros de eventos, transacciones y datos de usuarios durante investigaciones.
- **Belkasoft Evidence Center X:** es una herramienta útil para el análisis forense digital, identificación y recuperación de información.
- **Belkasoft:** líder global en la tecnología forense digital, famosa por sus herramientas forenses exhaustivas y fiables.
- **Bit:** es la unidad más pequeña de información utilizada en informática y teoría de la información, con valor 0 o 1.
- **Blockchain:** tecnología que registra y distribuye cuando crea el registro inmutable y transparente de transacciones.
- **Ciberseguridad:** conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, mecanismos de prevención y mitigación, formación, modos de gestión del riesgo, acciones, investigación y tecnologías relacionadas con la protección del ciberespacio.
- **Cifrado:** proceso de convertir información o datos en un código para prevenir accesos no autorizados, especialmente relevante para proteger datos sensibles almacenados en archivos como el pagefile.sys.
- **Criptografía:** práctica de cifrar datos para que solo puedan ser descifrados por personas autorizadas. Se utiliza para proteger la confidencialidad de la información en tránsito o en reposo.
- **Data carving:** método para recuperar archivos perdidos o dañados de un dispositivo de almacenamiento mediante la identificación de patrones de datos conocidos.
- **DDR (Double Data Rate):** tecnología de memoria

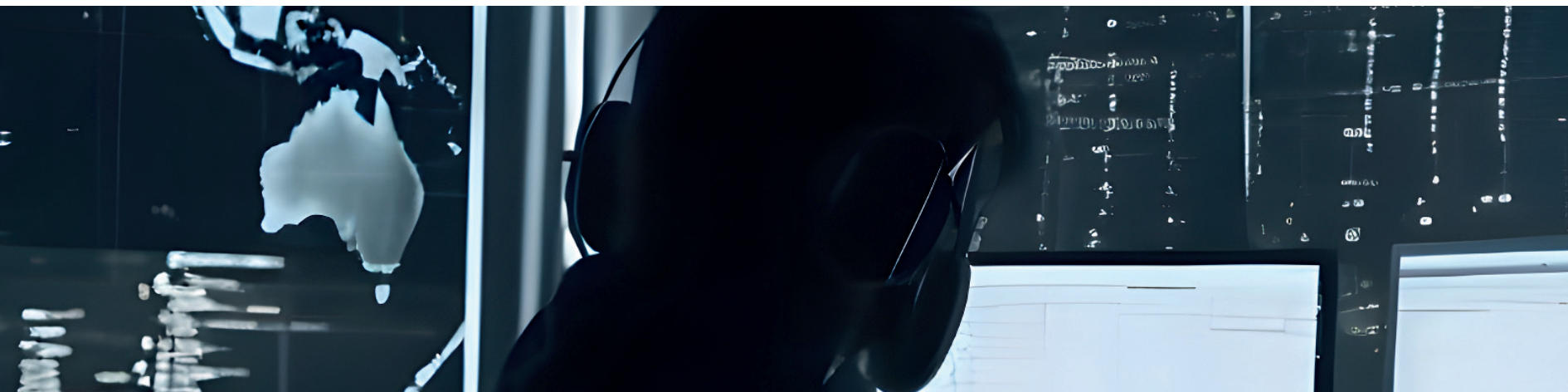


RAM que mejora el rendimiento sobre la memoria SDRAM estándar al transferir datos en los flancos de subida y bajada del ciclo de reloj.

- **Disco duro (HDD):** componente que almacena datos a largo plazo usando discos magnéticos en rotación y cabezales móviles.
- **Discos sólidos (SSD):** dispositivos de almacenamiento de datos que utilizan memoria no volátil, como la memoria flash, en lugar de discos giratorios.
- **DoS (Denegación de Servicio):** ataque informático que tiene como objetivo hacer inaccesible un servicio o recurso, saturando y bloqueando los recursos del sistema.
- **DRAM (Dynamic RAM):** tipo de memoria RAM que almacena cada bit de datos en una celda separada compuesta de un capacitor y un transistor, requiriendo refrescos periódicos de datos.
- **Esteganografía:** técnica específica de ocultamiento que utiliza medios digitales para ocultar información.
- **Event logs:** registros de eventos que documentan la actividad de un sistema operativo, aplicaciones, servicios y controladores de dispositivos.
- **Evidencia digital:** referido a cualquier dato o información almacenada o transmitida en formato digital que puede

ser utilizada como prueba en un proceso legal o investigación.

- **EXFAT (Extended File Allocation Table):** sistema de archivos creado por Microsoft para eliminar las limitaciones de FAT32, compatible con varios sistemas operativos.
- **EXT2, EXT3 y EXT4:** sistemas de archivos utilizados en sistemas operativos Linux, con EXT4 siendo el más reciente y avanzado.
- **FAT32 (File Allocation Table 32):** sistema de archivos desarrollado por Microsoft, ampliamente compatible, pero con limitaciones en el tamaño máximo de archivos y particiones.
- **Firewall:** dispositivo o software que controla el tráfico de red que entra y sale de una red. Se utiliza para bloquear el acceso no autorizado y proteger la red de ataques cibernéticos.
- **Forense Digital:** aplicación de métodos científicos y de investigación para recopilar, preservar, analizar y presentar evidencia digital en investigaciones criminales o legales.
- **Framework:** estructura conceptual y tecnológica de soporte definida, con módulos de software concretos, que puede servir de base para la organización y desarrollo de software.



- **FTK Imager:** software utilizado para generar imágenes forenses de dispositivos de almacenamiento, permitiendo la copia bit a bit de datos para su análisis forense.
- **GDB:** geodatabase de archivos es una colección de archivos en una carpeta en el disco que puede almacenar, consultar y administrar datos espaciales y datos no espaciales.
- **Hash:** código generado mediante una función hash que sirve para verificar la integridad de datos, asegurando que no han sido alterados.
- **HFS+ (Hierarchical File System Plus):** sistema de archivos desarrollado por Apple, utilizado en sus dispositivos hasta ser reemplazado por APFS.
- **Intercambio (Swapping):** intercambio (swapping) es el proceso de mover secciones de la memoria RAM hacia el archivo de intercambio (swap file) y viceversa, a medida que el sistema necesita liberar o utilizar más memoria.
- **Kernel:** parte central del sistema operativo que gestiona las operaciones de la CPU, memoria y dispositivos periféricos.
- **Magnet AXIOM:** plataforma de investigación digital completa que permite a los examinadores adquirir y analizar datos forenses de forma transparente, así como compartir sus hallazgos.
- **Malware:** software malicioso diseñado para infiltrarse o dañar un sistema informático sin el consentimiento del usuario.
- **Memoria RAM (Random Access Memory):** tipo de memoria de acceso aleatorio que se utiliza como memoria principal en un sistema informático, donde se almacenan los datos y programas que están siendo ejecutados por el procesador.
- **Metadatos:** datos que describen otros datos, proporcionando información sobre su contenido, contexto, calidad, condición o características.
- **NIST (National Institute of Standards and Technology):** agencia no reguladora del Departamento de Comercio de los Estados Unidos, cuya misión es promover la innovación y la competitividad industrial.
- **NTFS (New Technology File System):** sistema de archivos utilizado por defecto en sistemas Windows, soporta archivos de gran tamaño y tiene características avanzadas como compresión de archivos.
- **Ocultamiento:** práctica de ocultar información dentro de otro objeto, como una imagen o un archivo de audio, para que pase desapercibida.
- **Phishing:** técnica de ingeniería social que intenta en-



gañar a las personas para que revelen información personal o financiera.

- **Ransomware:** tipo de software malicioso que restringe el acceso a determinadas partes o archivos del sistema operativo de una computadora y pide un rescate a cambio de quitar esta restricción.
- **Rekall:** software similar a Volatility, pero con algunas funcionalidades adicionales además tiene una mejor integración con Google Cloud para el análisis de memoria en la nube.
- **Sistema de archivos:** componente del sistema operativo que organiza y gestiona el almacenamiento de datos en las unidades de almacenamiento.
- **SRAM (Static RAM):** memoria RAM que no necesita ser refrescada periódicamente y es más rápida que DRAM, comúnmente utilizada como memoria caché.
- **Trazabilidad:** capacidad para rastrear el historial, la ubicación o la aplicación de un objeto mediante identificaciones registradas.
- **Unidad de estado sólido híbrida (SSHD):** combina características de HDD y SSD, utilizando una pequeña cantidad de memoria flash NAND como caché para mejorar el rendimiento.

- **USB (Universal Serial Bus):** estándar industrial que define los cables, conectores y protocolos de comunicación utilizados en un bus para conectar dispositivos a una computadora.
- **Volatility:** herramienta de análisis forense de memoria de código abierto que permite examinar volcados de memoria de sistemas Windows, Linux y Mac.
- **WinDbg:** herramienta de depuración de Microsoft para sistemas Windows, utilizada para analizar problemas de software y hardware a través de volcados de memoria.

BIBLIOGRAFÍA



Appendino, D., Aprile, F., & De Gallo, H. (2015). Plan Estratégico para la implementación de un Centro de Servicios de Informática Forense. Congreso Argentino de Ciencias de La Computación (Junín, 2015). <http://sedici.unlp.edu.ar/handle/10915/50584>

Apple. (2021). Formatos del sistema de archivos disponibles en Utilidad de Discos en el Mac. <https://support.apple.com/es-es/guide/disk-utility/dsku19ed921c/mac>

Azucena, M. C. (2022). Análisis forense de imágenes y vídeos manipulados (Deepfake) [UNED]. <http://old.e-spacio.uned.es/fez/view/bibliuned:master-ETSIInformatica-CBS-Amartin>

Banwani, D., & Kalra, Y. (2021). Maintaining and Evaluating the Integrity of Digital Evidence in Chain of Custody. *International Journal of Recent Technology and Engineering (IJRTE)*, 10(3), 90–96. <https://doi.org/10.35940/ijrte.C6449.0910321>

Bonomi, S., Casini, M., & Ciccotelli, C. (2019). B-CoC: A Blockchain-Based Chain of Custody for Evidences Management in Digital Forensics. *Open Access Series in Informatics (OASIs)*, 1–15.

Boté Vericad, J. J., & Vállez, M. (2022). Aplicaciones de deep-fakes. Manipulación de contenido audiovisual y riesgos para los usuarios basados en las políticas de privacidad. *Documentación de Las Ciencias de La Información*, 45(1), 25–32. <https://doi.org/10.5209/dcin.77256>

Brown, E. K. (2022). Digital Forensic and Distributed Evidence. *Advances in Multidisciplinary and Scientific Research Journal Publication*, 1(1), 357–362. <https://doi.org/10.22624/AIMS/CRP-BK3-P57>

Calderón Valdiviezo, R. G., Guzmán Reyes, G. S., & Salinas González, J. M. (2011). FORENSES DIGITALES LABORATORIO DISEÑO Y PLAN [ESPOL]. <http://www.dspace.espol.edu.ec/handle/123456789/19927>

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd Edition 3rd Edición.

Choji, L. (2021). Digital Forensic Laboratory (DFL). <https://loischo594.medium.com/digital-forensic-laboratory-dfl-2db-47d1b1654>

Chouliaras, D. N. (n.d.). Quality Management Systems in Testing Laboratories which conformed with ISO/IEC 17025:2017 International Standard requirements for accreditation purposes.

Di Iorio, A., Cistoldi, P., Constanzo, B., Giaccaglia, M. F., Lereña, R., Greco, F., Iturriaga, J., & Lamperti, S. (2019). Guía técnica para el diseño, implementación y gestión de laboratorios de informática forense. <http://redi.ufasta.edu.ar:8082/jspui/bitstream/123456789/928/1/LibroGuiaTcnica.pdf>

Di Iorio, A. H., Sansevero, R. E., Castellote, M., Podestá, A., & Greco, F. (2013). Determinación de aspectos carentes en un “Proceso Unificado de Recuperación de Información digital.” V Workshop de Seguridad Informática (WSegI) - JAIIO 42 (2013). <http://sedici.unlp.edu.ar/handle/10915/75948>

Di Lorio, A., Mollo, M., & Cistoldi, P. (2016). Consideraciones para el diseño de un Laboratorio Judicial en Informática Forense. Conference: VI CIIDDI - Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática, Santa Fe, Argentina. https://www.researchgate.net/publication/319262773_Consideraciones_para_el_diseno_de_un_

Laboratorio_Judicial_en_Informatica_Forense

Dropbox. (n.d.). ¿Qué es un disco duro? Retrieved June 28, 2024, from <https://experience.dropbox.com/es-la/resources/what-is-a-hard-drive>

Edmonson, M. (2023). SANS Workshop – Metadata Madness. In . <https://www.sans.org/webcasts/sans-workshop-metadata-madness/>

El nuevo Laboratorio Forense de Evidencia Digital de la Defensoría del Pueblo. (2024). El nuevo Laboratorio Forense de Evidencia Digital de la Defensoría del Pueblo. <https://www.ambitojuridico.com/noticias/especiales/el-nuevo-laboratorio-forense-de-evidencia-digital-de-la-defensoria-del-pueblo>

Geeksforgeeks. (2020). HDD Full Form. <https://www.geeksforgeeks.org/hdd-full-form/>

Geeksforgeeks. (2024). Introduction to Solid-State Drive (SSD). <https://www.geeksforgeeks.org/introduction-to-solid-state-drive-ssd/>

Gupta, J. N. D., Kalaimannan, E., & Yoo, S.-M. (2016). A heu-



ristic for maximizing investigation effectiveness of digital forensic cases involving multiple investigators. *Computers & Operations Research*, 69, 1–9. <https://doi.org/10.1016/j.cor.2015.11.003>

Ionos. (2020). ¿Qué es FAT32? <https://www.ionos.es/digital-guide/servidores/know-how/fat32/>

Jawad, T. M. (2018). Adoption of Chain of Custody Improves Digital Forensic Investigation Process. *Iraqi Journal of Information & Communications Technology*, 1(2), 13–23. <https://doi.org/10.31987/ijict.1.2.14>

Kakunuri, S., & Subhadra, K. (2021). Performance of Cryptographic Hash function used in Digital Forensic tools. *International Journal For Innovative Engineering and Management Research*. <https://doi.org/10.48047/IJIEMR/V10/I11/21>

Kingston. (2023). Disco SSD externo Kingston XS1000 insertado en un portátil Los misterios de los sistemas de archivos. <https://www.kingston.com/es/blog/personal-storage/understanding-file-systems>

Lerena, R., Di Iorio, A., & Oyuela, J. (2018). InFo-Lab: De-

sarrollando Tecnología Nacional en Informática Forense. <https://47jaiio.sadio.org.ar/sites/default/files/SIE-16.PDF>

Molina, F. (2017). Propuesta de un modelo conceptual de preservación digital aplicable a la mejora de la preservación de evidencia digital en instituciones de investigación criminal [Universidad Nacional Mayor de San Marcos]. <https://hdl.handle.net/20.500.12672/6850>

OSCO ESCOBEDO MIGUEL ANGEL et al. (2023). DIGITAL EVIDENCE AS A MEANS OF PROOF IN CRIMINAL PROCEEDINGS. *Russian Law Journal*, 11(5s). <https://doi.org/10.52783/rlj.v11i5s.895>

Palacios Carvajal, J. E. (2020). Diseñar un Laboratorio de Ciencias Forenses Digitales en el Cuerpo Técnico de Investigación de la Fiscalía General de la Nación, Seccional Medellín [Instituto Tecnológico Metropolitano]. <http://hdl.handle.net/20.500.12622/4074>

Parra, H. B., Ambrústolo, M. B., & Cistoldi, P. A. (2021). Elaboración de un Sistema Integrado de Gestión de la Calidad y de Ciberseguridad. 5to Congreso Argentino de Ingenierías. <https://info-lab.org.ar/images/2021/Papers/CADI.pdf>

Pérez, A., & Gómez, M. (2021). El fenómeno del deepfake: Implicaciones y desafíos en la era digital. . In Revista de Tecnología y Sociedad.

Raquejo Romero, J. A. (2013). Importancia de la recolección de datos volátiles dentro de una investigación forense. Universidad Piloto de Colombia. <https://repository.unipiloto.edu.co/handle/20.500.12277/3088?show=full>

Rivetti, E. A., Aráoz Fleming, J., Parra de Gallo, H. B., & Leone, H. (2016). Análisis de los documentos oficiales sobre obtención, tratamiento y preservación de la evidencia digital: Aportes para el tratamiento del correo electrónico como evidencia digital... Universidad Católica de Salta. https://repositorios-digitales.mincyt.gob.ar/vufind/Record/RIUCASAL_a7fe84b-469be879886c1089a19bf8911

Semprini, G. 2016. (2016). Lineamientos para la creación de laboratorios informáticos forenses. XVI Simposio Argentino de Informática y Derecho (SID 2016) - JAIIO 45 (Tres de Febrero, 2016). <http://sedici.unlp.edu.ar/handle/10915/58306>

Soto, V., & Olier, E. (2023). Guía para el Diseño de Simulacros

de Incidentes de Ciberseguridad a Través de la Adaptación de Estándares y Metodologías como ISO/IEC 27035, NIST SP 800-61 y NIST SP 800-84 en el Banco Popular. <https://repository.unipiloto.edu.co/handle/20.500.12277/12769>

Unitel. (2021). Ventajas y desventajas de los SSD, HDD y SSHD ¿Cuál es el mejor? <https://unitel-tc.com/ssd-hdd-sshd-ventajas-diferencias/>

Universitat Politècnica de València, E. (2014). Universitat Politècnica de València. Ingeniería Del Agua, 18(1), ix. <https://doi.org/10.4995/ia.2014.3293>

Vargas, L. F., & Delgado, M. R. (2018). Deep learning based steganography and steganalysis: A review.

Investigación Forense Digital:
análisis de evidencias electrónicas

