MANEJO DE EVIDENCIA DIGITAL Y PROCEDIMIENTO FORENSE APLICADO EN PANAMÁ

Introducción

En el contexto actual de transformación digital, la mayoría de las actividades humanas, comerciales, administrativas y delictivas dejan un rastro en forma de información electrónica. Este entorno plantea desafíos significativos para los sistemas de justicia, que deben incorporar de manera adecuada la evidencia digital dentro de los procesos judiciales. A diferencia de la evidencia física tradicional, la evidencia digital es altamente volátil, fácilmente modificable y puede ser replicada sin pérdida aparente de calidad, lo que exige procedimientos técnicos y jurídicos rigurosos para garantizar su integridad, autenticidad y valor probatorio.

La informática forense surge como la disciplina especializada que integra conocimientos técnicos de sistemas informáticos, redes y seguridad con los principios del derecho probatorio. El perito informático actúa como puente entre el mundo técnico y el jurídico, analizando dispositivos, recuperando información, documentando procedimientos y elaborando informes que permitan a los operadores de justicia comprender lo ocurrido en el ámbito digital. En Panamá, el marco legal relacionado con documentos electrónicos, firmas digitales y prueba digital —entre ellos la Ley 51 de 2008— se complementa con estándares internacionales como ISO/IEC 27037, NIST SP 800-86 y la RFC 3227, que orientan las buenas prácticas para el manejo de evidencias electrónicas.

El presente proyecto semestral investigativo tiene como propósito estudiar, desde una perspectiva técnico–jurídica, el manejo de la evidencia digital, así como aplicar un procedimiento forense simulado que permita evidenciar la correcta preservación, adquisición, análisis y documentación de un medio de almacenamiento digital. Paralelamente, se recopilarán percepciones de especialistas y docentes a través de entrevistas y encuestas, con el fin de identificar fortalezas, debilidades y retos en la práctica de la informática forense en el contexto panameño.

El informe se estructura en varios capítulos. En el Capítulo I se plantea el marco teórico. El Capítulo II describe el diseño metodológico de la investigación, mientras que el Capítulo III expone el procedimiento forense aplicado en un caso simulado. En el Capítulo IV se presentan los resultados de la investigación empírica y del laboratorio forense; finalmente el Capítulo V reúne las conclusiones y recomendaciones derivadas del estudio.

Capítulo I. Marco teórico

1.1 Informática forense: concepto y alcance

La informática forense es la disciplina que identifica, preserva, adquiere y analiza información digital para usarla como evidencia. Actúa sobre computadoras, móviles, redes, servidores y otros sistemas que almacenan datos relevantes.

Sus tareas incluyen recuperar archivos borrados, analizar metadatos, reconstruir líneas de tiempo, identificar usuarios o IP y detectar actividades maliciosas, todo siguiendo procedimientos que aseguren la integridad y autenticidad de la evidencia.

1.2 El perito informático: rol y responsabilidades

El perito informático es un especialista con la formación y experiencia necesarias para analizar evidencia digital y emitir un dictamen técnico solicitado por una autoridad. Su labor consiste en responder, de manera objetiva y fundamentada, las preguntas vinculadas a hechos tecnológicos dentro de un proceso judicial. Actúa como auxiliar de la justicia, por lo que debe mantener independencia e imparcialidad, aunque haya sido designado por una de las partes.
Sus responsabilidades abarcan dimensiones civiles, penales y éticas.

- En lo civil, un dictamen realizado con negligencia puede causar perjuicios, generando posibles demandas de responsabilidad.
- En lo penal, manipular evidencia, falsificar conclusiones o divulgar información protegida puede constituir delito.
- En lo ético, debe actuar con honestidad, no sobrepasar su competencia profesional y resguardar la confidencialidad de todos los datos que examina.

1.3 Evidencia digital: características y ciclo de vida

La evidencia digital es toda información con valor probatorio. Puede incluir documentos, correos, chats, logs, bases de datos, imágenes, videos, capturas de pantalla o configuraciones.
Su rasgo distintivo es la volatilidad: los datos pueden alterarse, sobrescribirse o eliminarse con facilidad, ya sea por acciones humanas o por procesos automáticos del sistema.
Su ciclo de vida se organiza en etapas:

- Identificación: dispositivos, cuentas o servicios que puedan contener evidencia.
- Preservación: aplicar medidas para evitar cualquier modificación.
- Adquisición: obtener copias forenses íntegras de los datos.
- Análisis: examinar la información de forma estructurada y técnica.
- Presentación: comunicar hallazgos de manera clara ante la autoridad.
- Almacenamiento o destrucción: decidir el destino final de la evidencia según normas y procedimientos.

1.4 Valor probatorio de la evidencia digital

Para que la evidencia digital sea admitida en juicio, debe cumplir con integridad, autenticidad, legalidad y fiabilidad en su obtención. Estos requisitos se acreditan con estándares técnicos, una cadena de custodia completa y el testimonio del perito.

En la práctica, los jueces valoran la evidencia según la calidad del peritaje y la coherencia del informe con el resto de las pruebas. Un dictamen claro y bien fundamentado aumenta su credibilidad.

1.5 Estándares internacionales aplicables

Las buenas prácticas en informática forense se sustentan en estándares internacionales como ISO/IEC 27037, NIST SP 800-86 y la RFC 3227, los cuales orientan la correcta gestión de evidencias digitales. Aunque no son normas legales obligatorias, su uso aporta rigor técnico y credibilidad al proceso forense.

- ISO/IEC 27037: establece directrices para identificar, recolectar, adquirir y preservar evidencia digital. Destaca la necesidad de personal competente, herramientas confiables y documentación completa de cada acción.
- NIST SP 800-86: integra técnicas forenses dentro de la respuesta a incidentes, siguiendo un proceso de preparación, recolección, examen, análisis y presentación.
- RFC 3227: propone un orden de volatilidad para recolectar datos en sistemas en ejecución, priorizando información altamente efímera como memoria, procesos y conexiones de red.

1.6 Cadena de custodia digital

La cadena de custodia digital es el registro cronológico que documenta quién maneja la evidencia y qué acciones se realizan sobre ella, garantizando que no haya sido alterada. Una cadena mal gestionada puede comprometer su integridad y valor probatorio.

En la práctica, incluye datos como el código de la evidencia, su descripción, fecha y hora de recolección, responsables, transferencias, condiciones de almacenamiento y cualquier intervención realizada.

1.7 Marco legal panameño sobre evidencia digital

En Panamá, la Ley 51 de 2008 reconoce los documentos electrónicos y las firmas digitales, garantizando que los mensajes de datos pueden ser usados como prueba siempre que se demuestre su integridad y su vínculo con las partes.

El Código Procesal Penal regula la obtención y valoración de la prueba, y aunque no mencione expresamente los medios digitales, sus principios se aplican a la evidencia electrónica. Los operadores de justicia deben interpretar estas normas según los avances tecnológicos y apoyarse en guías técnicas para evaluar adecuadamente este tipo de evidencia.

1.8 Errores frecuentes en la gestión de evidencias electrónicas

Los errores más comunes en la gestión de evidencia digital incluyen manipular directamente los dispositivos sin crear copias forenses, no documentar la cadena de custodia, usar herramientas no fiables, omitir el cálculo de hashes y carecer de procedimientos estandarizados. Estas fallas pueden provocar que la evidencia sea cuestionada o inadmisible en juicio.

También es habitual ignorar el orden de volatilidad, lo que lleva a perder información crítica en memoria o conexiones de red. Además, la falta de actualización del personal técnico y jurídico dificulta la correcta interpretación de indicios digitales.

Capítulo II. Diseño metodológico de la investigación

2.1 Tipo y enfoque de investigación

La investigación es descriptivo–aplicativa, ya que analiza las prácticas forenses utilizadas en Panamá y su correspondencia con los estándares técnicos y legales, integrando además un procedimiento forense simulado que permite observar la aplicación práctica de los principios estudiados. Su enfoque es cualitativo, basado exclusivamente en entrevistas semiestructuradas dirigidas a especialistas y docentes del área, con el propósito de recoger criterios profesionales sobre el manejo de la evidencia digital y la calidad de los procesos forenses en el contexto panameño.

2.2 Método de investigación

Se utiliza un método analítico–descriptivo, estructurado en dos fases. La fase documental comprende la revisión de legislación panameña, estándares internacionales y guías técnicas sobre manejo de evidencia digital, lo que permite construir el sustento teórico del estudio. La fase empírica integra la aplicación de entrevistas un procedimiento forense simulado, con el fin de contrastar la teoría con la práctica y analizar cómo se ejecutan y perciben los procesos forenses en el contexto panameño.

2.3 Población y muestra

La población objetivo está constituida por profesionales y académicos vinculados a la informática forense, la ciberseguridad y el derecho en Panamá, particularmente aquellos que han tenido contacto directo o indirecto con casos que involucren evidencia digital. Dado el carácter exploratorio del estudio y las limitaciones de tiempo y acceso, se selecciona una muestra intencional compuesta por tres participantes, entre los que se pueden incluir docentes de asignaturas relacionadas con informática forense o ciberseguridad, técnicos de laboratorios forenses digitales y abogados que han trabajado con prueba electrónica.

2.4 Técnicas e instrumentos de recolección de datos

En la fase empírica se empleará únicamente una técnica de recolección de datos: la entrevista semiestructurada, dirigida a especialistas y docentes vinculados con la informática forense. Esta herramienta permitirá obtener opiniones expertas sobre la preservación, adquisición y análisis

de evidencia digital en Panamá. Su uso facilita contrastar el marco teórico con la experiencia práctica, identificando percepciones profesionales sobre el cumplimiento de estándares técnicos y legales en los procedimientos forenses.

2.5 Procedimiento para la recolección de datos

Etapa	Actividad Realizada	Propósito en la Investigación
1. Selección de la técnica	Se elige la **entrevista semiestructurada** como único instrumento de recolección de datos.	Obtener opiniones expertas sobre prácticas forenses y manejo de evidencia digital.
2. Diseño de la guía de entrevista	Elaboración de preguntas claras y alineadas con los objetivos del estudio.	Asegurar que el instrumento genere información pertinente y útil.
3. Contacto con participantes	Comunicación vía correo o mensajería institucional para explicar el estudio y solicitar participación.	Garantizar consentimiento y disponibilidad de especialistas y docentes.
4. Aplicación de entrevistas	Entrevistas presenciales o virtuales con autorización para registrar notas o audio.	Recopilar criterios profesionales sobre preservación, adquisición y análisis de evidencia digital.
5. Transcripción y organización	Registro y clasificación de respuestas en categorías temáticas.	Facilitar el análisis cualitativo del contenido.
6. Procedimiento forense simulado	Ejecución del caso simulado, documentando cada acción sobre la evidencia digital.	Contrastar la teoría con la práctica técnica y reforzar el análisis del estudio.

2.6 Técnicas de análisis de datos

El análisis se realizará mediante análisis de contenido, revisando las transcripciones de las entrevistas para identificar patrones y agruparlos en categorías temáticas relacionadas con la capacitación, el uso de protocolos, la aplicación de estándares y los vacíos normativos.

Los resultados del procedimiento forense simulado se examinarán a partir de la bitácora, los valores hash y los hallazgos obtenidos con las herramientas utilizadas.

Finalmente, ambos insumos —entrevistas y ejercicio técnico— serán integrados en la discusión, contrastándolos con los estándares y el marco teórico.

2.7 Consideraciones éticas

El estudio garantiza la confidencialidad y anonimato de los participantes, presentando las opiniones de forma agregada o codificada. La participación en las entrevistas es voluntaria y basada en consentimiento informado.

El procedimiento forense simulado utiliza únicamente datos ficticios, evitando exponer información real o sensible. Estas medidas aseguran el respeto a la privacidad y el manejo ético de toda la información recopilada.

Capítulo III. Procedimiento forense aplicado en un caso simulado

3.1 Descripción del caso simulado

Para el presente proyecto se simula un **caso de posible fuga de información** en una empresa de servicios, donde se sospecha que un empleado copió sin autorización una base de datos de clientes a una **memoria USB personal**. La gerencia entrega dicho dispositivo al perito informático y solicita determinar si contiene información confidencial extraída de los sistemas corporativos y, en su caso, dejarla correctamente documentada para un eventual proceso judicial. En este contexto:

- La **evidencia principal** es una memoria USB incautada al empleado.
- Se **prepara la documentación inicial** mediante una orden de análisis simulada, un formulario de cadena de custodia (con registro de entrega y recepción) y la descripción técnica del dispositivo a examinar.

3.2 Identificación y preservación de la evidencia

Al recibir la memoria USB presuntamente vinculada con la fuga de información, se realizó una identificación inicial sin acceder a su contenido. Se registró que se trataba de un **dispositivo USB de almacenamiento**, previamente formateado en **sistema de archivos NTFS**.

Se documentaron los datos visibles del dispositivo, incluyendo:

- **Tipo:** Memoria USB (almacenamiento masivo).
- **Sistema de archivos:** NTFS (confirmado en el proceso de formateo del laboratorio).
- **Puerto de conexión:** USB tipo estándar.
- **Condición física:** Sin daños visibles, con carcasa íntegra.
- **Fecha y hora de recepción:** Registrada manualmente en el formulario de cadena de custodia.
- **Identificador físico:** Código o numeración presente en la carcasa del dispositivo (cuando visible).
- **Custodio inicial:** Nombre y firma de la persona que entrega la evidencia.

El dispositivo fue **etiquetado como evidencia digital**, colocado en un contenedor aislado y mantenido sin conexión a ningún equipo para evitar modificaciones accidentales. Todas las acciones —inspección visual, etiquetado, recepción y almacenamiento— fueron registradas en la cadena de custodia correspondiente, conforme a las buenas prácticas de preservación de evidencia digital.

3.3 Adquisición de la evidencia (creación de imagen forense)

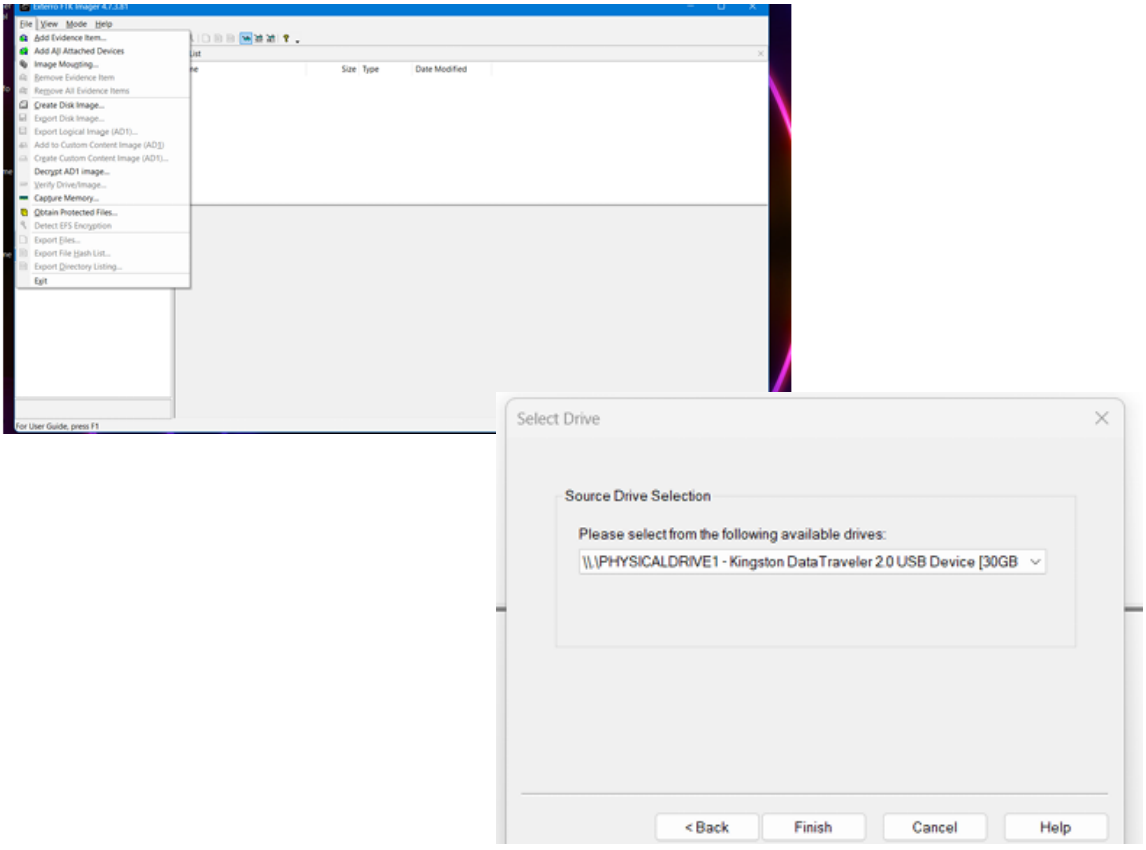
Para asegurar la integridad del contenido de la memoria USB, se realizó la adquisición forense mediante **FTK Imager**, seleccionando el dispositivo como **Physical Drive**. El dispositivo fue identificado por su tipo de conexión USB y por su sistema de archivos **NTFS**, según el reconocimiento previo realizado por el sistema operativo y registrado en la configuración inicial del análisis

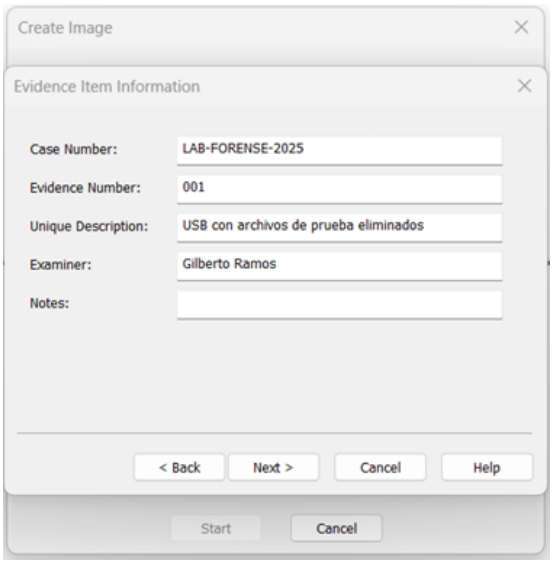
Durante el proceso de adquisición, se configuró la creación de una imagen forense en formato **E01 (EWF)**, permitiendo almacenar información adicional del caso como el número de evidencia, número de caso, examinador responsable y una breve descripción del dispositivo. Esta información se ingresó en la sección *Case Information* de FTK Imager conforme al flujo de trabajo mostrado en el documento

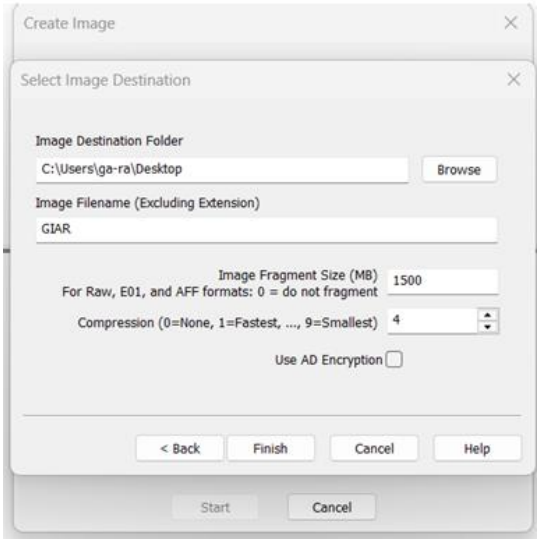
La imagen forense generada fue guardada en un directorio local del examinador, siguiendo una estructura de almacenamiento similar a la observada en el análisis posterior realizado con Autopsy, donde se muestra la ruta:

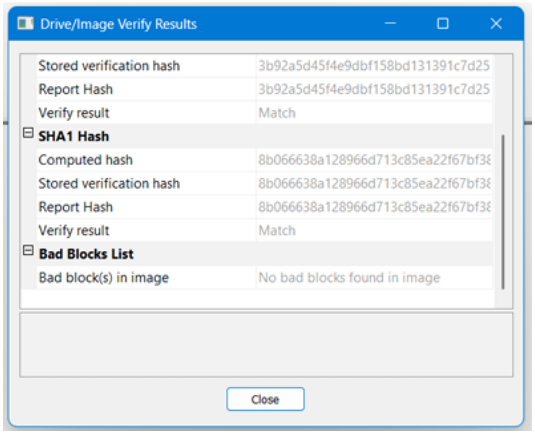
C:\Users\ga-ra\Desktop\LAB\GJAR\E01

Durante la creación de la imagen, FTK Imager calculó automáticamente los valores hash **MD5 y SHA1**, utilizados para verificar la integridad del dispositivo original. Al finalizar, el software reportó el estado **"Completed OK"**, lo que confirma que la adquisición se completó sin errores y que la copia creada coincide bit a bit con el contenido del dispositivo físico




Create Image
Evidence Item Information
Case Number:
LAB-FORENSE-2025
Evidence Number:
001
Unique Description:
USB con archivos de prueba eliminados
Examiner:
Gilberto Ramos
Notes:
< Back
Next >
Cancel
Help
Start
Cancel


Create Image
Select Image Destination
Image Destination Folder
C:\Users\ga-ra\Desktop
Browse
Image Filename (Excluding Extension)
GIAR
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment
1500
Compression (0=None, 1=Fastest, ..., 9=Smallest)
4
Use AD Encryption
< Back
Finish
Cancel
Help
Start
Cancel


Drive/Image Verify Results
Stored verification hash
3b92a5d45f4e9dbf158bd131391c7d25
Report Hash
3b92a5d45f4e9dbf158bd131391c7d25
Verify result
Match
SHA1 Hash
Computed hash
8b066638a128966d713c85ea22f67bf3
Stored verification hash
8b066638a128966d713c85ea22f67bf3
Report Hash
8b066638a128966d713c85ea22f67bf3
Verify result
Match
Bad Blocks List
Bad block(s) in image
No bad blocks found in image
Close

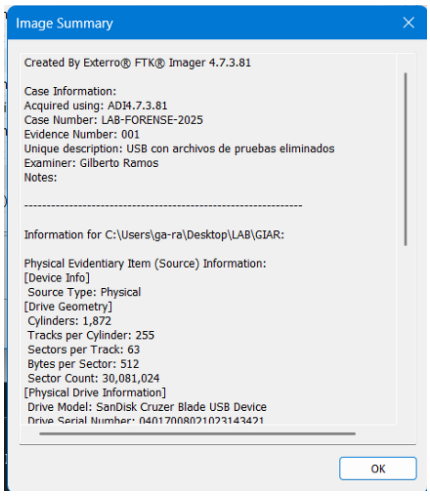
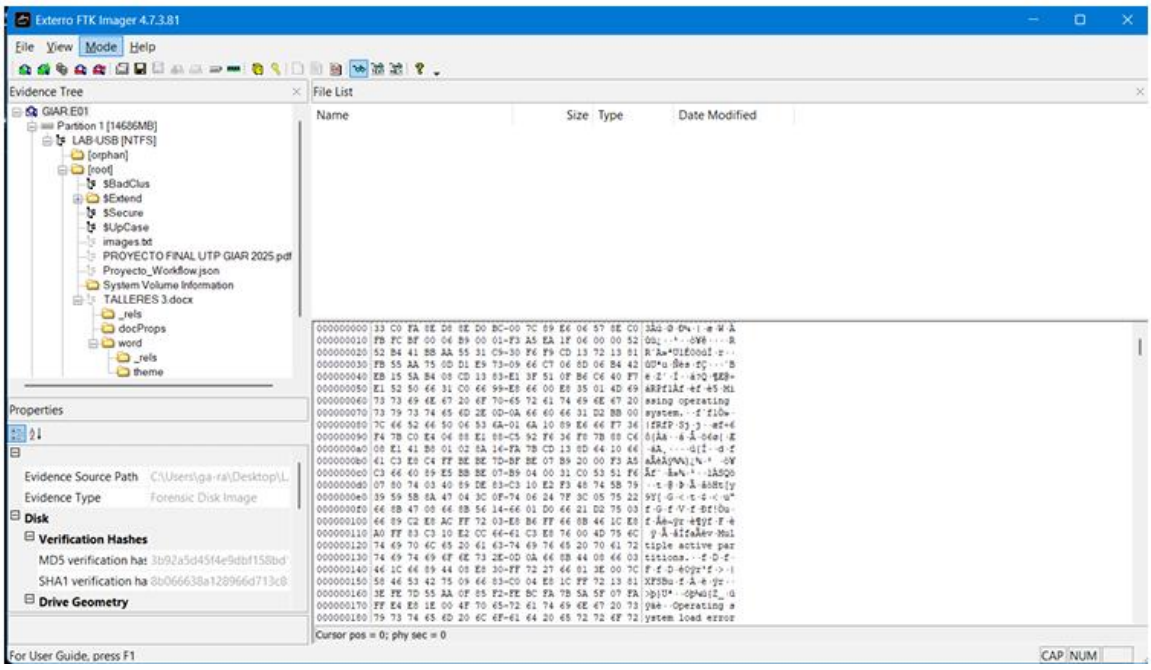


Image Summary
Created By Exterro® FTK® Imager 4.7.3.81
Case Information:
Acquired using: ADI4.7.3.81
Case Number: LAB-FORENSE-2025
Evidence Number: 001
Unique description: USB con archivos de pruebas eliminados
Examiner: Gilberto Ramos
Notes:
Information for C:\Users\ga-ra\Desktop\LAB\GIAR:
Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 1,872
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 30,081,024
[Physical Drive Information]
Drive Model: SanDisk Cruzer Blade USB Device
OK


Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modified
GIAR.E01
Partition 1 [14686MB]
LAB-USB [NTFS]
[orphan]
[root]
$BadClus
$Extend
$Secure
$UpCase
images.txt
PROYECTO FINAL UTP GIAR 2025.pdf
Proyecto_Workflow.json
System Volume Information
TALLERES 3.docx
_rels
docProps
word
_rels
theme
Properties
Evidence Source Path
Evidence Type
Forensic Disk Image
Disk
Verification Hashes
MD5 verification has
SHA1 verification ha
Drive Geometry
Cursor pos = 0; phy sec = 0
For User Guide, press F1
CAP
NUM

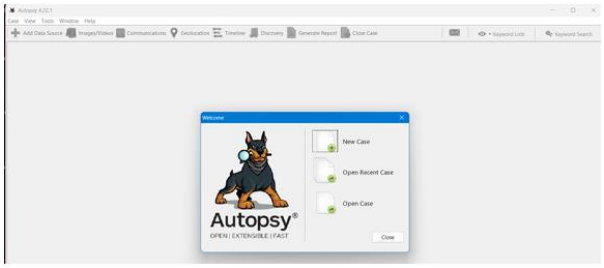
3.4 Análisis de la evidencia digital

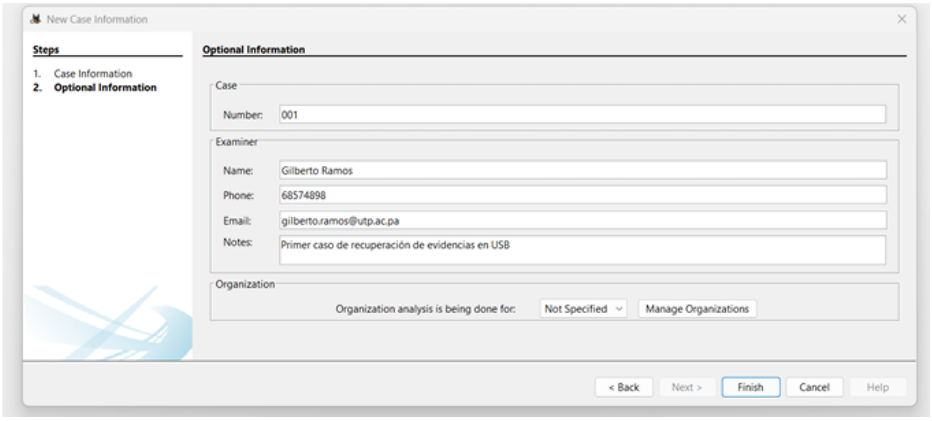
Una vez creada la imagen forense y verificada su integridad, se procedió al análisis utilizando Autopsy como herramienta principal. El perito abrió un nuevo caso en el software e incorporó la imagen del dispositivo USB como fuente de datos mediante la opción Disk Image or VM File. Una vez añadida, Autopsy ejecutó sus módulos de ingest y comenzó el procesamiento e indexación del contenido.

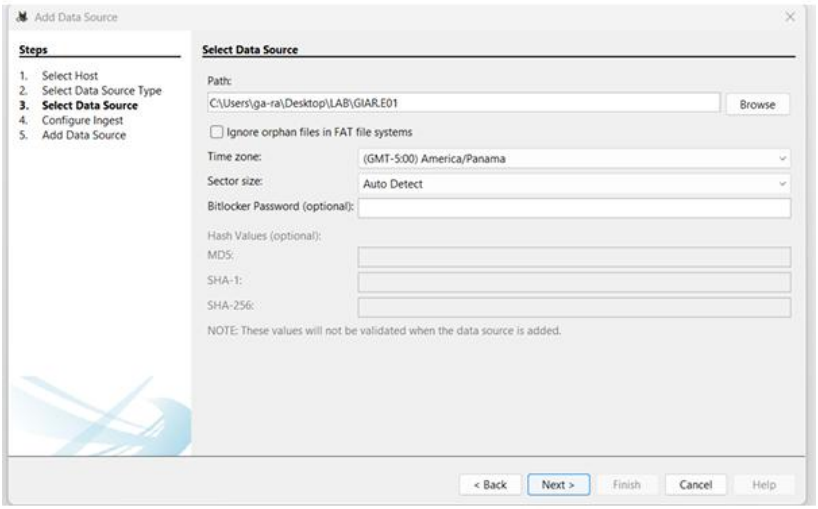
Durante el análisis, el perito exploró la estructura del sistema de archivos del USB, navegando por carpetas, subdirectorios y las categorías creadas automáticamente por Autopsy. La herramienta identificó archivos visibles y archivos eliminados, los cuales se encontraban listados dentro de las secciones de Deleted Files y File Types, permitiendo revisar distintos tipos de documentos, imágenes y registros recuperables

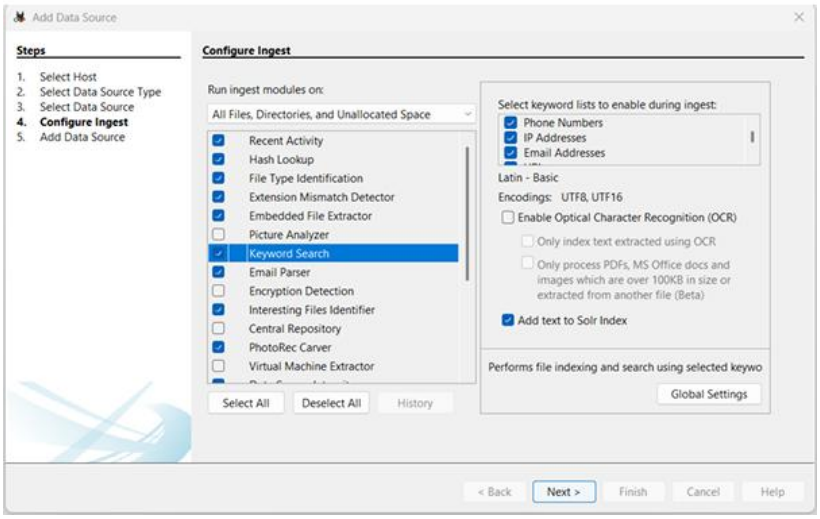
Cada archivo de interés fue evaluado individualmente, revisando su ruta completa, tamaño, fechas de creación y modificación, y cualquier metadato disponible. El perito examinó también los elementos marcados como eliminados para determinar si existía contenido relevante, aprovechando las funciones internas de extracción y vista previa que proporciona Autopsy. Esta revisión incluyó la inspección de espacio libre y áreas recuperables del dispositivo para verificar si hubo intentos de borrar información antes de la incautación.

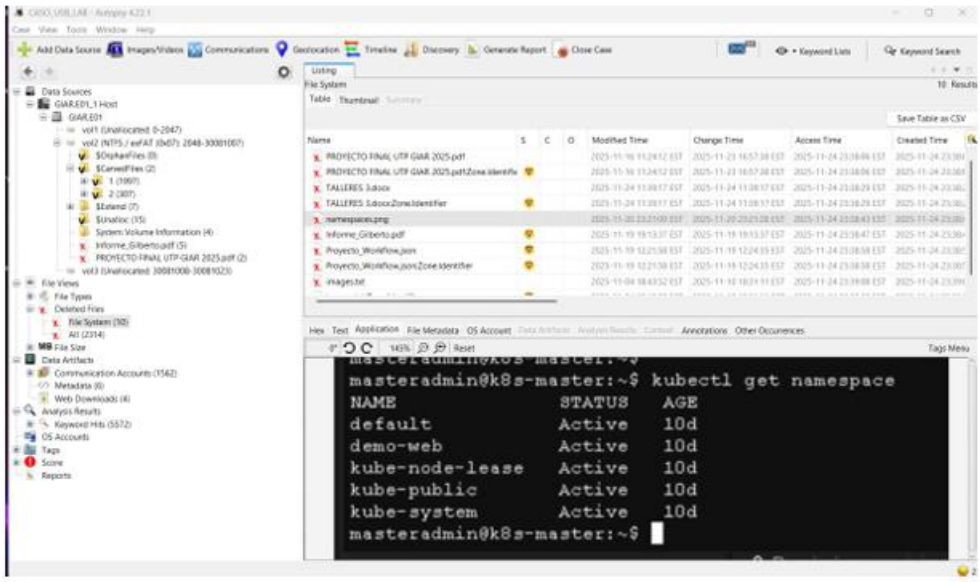
Todo hallazgo relevante fue documentado de manera sistemática, registrando la ubicación exacta dentro del sistema de archivos, los atributos del documento y capturas de pantalla que evidencian su existencia y contenido. Finalmente, se generaron reportes a través del módulo Generate Report, permitiendo obtener un registro estructurado del análisis realizado y de los artefactos identificados en el dispositivo.

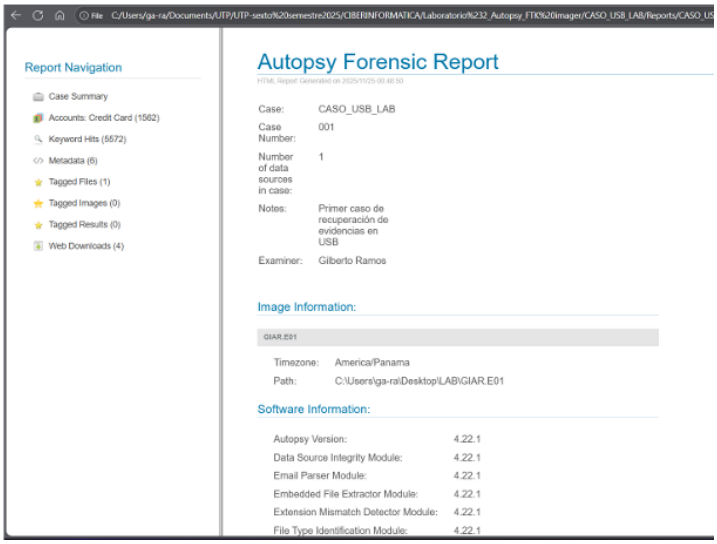





Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source
Path:
C:\Users\ga-ra\Desktop\LAB\GIAR.E01
Browse
Ignore orphan files in FAT file systems
Time zone:
(GMT-5:00) America/Panama
Sector size:
Auto Detect
Bitlocker Password (optional):
Hash Values (optional):
MD5:
SHA-1:
SHA-256:
NOTE: These values will not be validated when the data source is added.
< Back
Next >
Finish
Cancel
Help


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Configure Ingest
Run ingest modules on:
All Files, Directories, and Unallocated Space
Recent Activity
Hash Lookup
File Type Identification
Extension Mismatch Detector
Embedded File Extractor
Picture Analyzer
Keyword Search
Email Parser
Encryption Detection
Interesting Files Identifier
Central Repository
PhotoRec Carver
Virtual Machine Extractor
Select All
Deselect All
History
Select keyword lists to enable during ingest:
Phone Numbers
IP Addresses
Email Addresses
Latin - Basic
Encodings: UTF8, UTF16
Enable Optical Character Recognition (OCR)
Only index text extracted using OCR
Only process PDFs, MS Office docs and images which are over 100KB in size or extracted from another file (Beta)
Add text to Solr Index
Performs file indexing and search using selected keywo
Global Settings
< Back
Next >
Finish
Cancel
Help


masteradmin@k8s-master:~$ kubectl get namespace
NAME STATUS AGE
default Active 10d
demo-web Active 10d
kube-node-lease Active 10d
kube-public Active 10d
kube-system Active 10d
masteradmin@k8s-master:~$



3.5 Elaboración del informe pericial

INFORME PERICIAL DE ANÁLISIS DE EVIDENCIA DIGITAL

---

1. Datos del perito y número de caso

Perito examinador: Muriel Jaramillo
Especialidad: Informática Forense
Número de caso: 2025-USB-014
Fecha del análisis: 02/12/2025

Este informe se emite a solicitud de la administración de la empresa afectada, a fin de examinar un dispositivo de almacenamiento presuntamente vinculado con una posible fuga de información corporativa.

---

2. Objetivo del análisis

Determinar si la memoria USB entregada contiene archivos o artefactos relacionados con información sensible de la empresa, identificar indicios de extracción de datos y documentar el procedimiento técnico conforme a buenas prácticas de informática forense.

---

3. Descripción de la evidencia recibida

La evidencia recibida consiste en una **memoria USB** incautada a un colaborador sospechoso de extraer información sin autorización. Durante su recepción se registraron los siguientes datos:

- **Tipo de dispositivo:** Unidad de almacenamiento USB
- **Sistema de archivos reconocido:** NTFS (según formateo previo registrado en el análisis técnico)
- **Capacidad:** Reconocida por la estación de análisis al ser conectada para adquisición
- **Interfaz:** USB estándar
- **Estado físico:** Sin daños visibles en carcasa o conector
- **Fecha y hora de recepción:** 01/12/2025 – 10:32 a.m.
- **Custodio que entrega:** Supervisor del departamento de TI (firma registrada en formulario)

El dispositivo fue preservado bajo cadena de custodia, sin acceso directo antes de la adquisición forense.

---

4. Procedimiento seguido y herramientas utilizadas

4.1 Adquisición forense

Se empleó **FTK Imager** para realizar la copia bit a bit del dispositivo USB:

1. Se seleccionó la unidad como **Physical Drive**.
2. Se configuró la creación de una imagen en formato **E01 (EWF)**.
3. Se ingresaron datos del caso (case number, evidence number, examiner).
4. La imagen fue guardada en un directorio seguro: **C:\Users\ga-ra\Desktop\LAB\GJAR\E01** (ruta mostrada en Autopsy)
5. FTK Imager generó valores **MD5** y **SHA1** para verificar la integridad.
6. El proceso concluyó con estado **“Completed OK”**, confirmando una adquisición exitosa.

4.2 Análisis forense

Para el análisis se utilizó **Autopsy**, realizando lo siguiente:

1. Se creó un nuevo caso en la herramienta.
2. Se añadió la imagen E01 mediante la opción *Disk Image or VM File*.

3. Autopsy ejecutó sus módulos de ingest, indexando archivos, metadatos y elementos eliminados.
4. Se examinó la estructura del sistema NTFS, incluyendo archivos visibles y **archivos eliminados recuperables** listados por el software.
5. Se revisaron rutas, tamaños, metadatos y fechas de creación/modificación.
6. Se generaron reportes preliminares mediante *Generate Report*.

Todo el análisis se realizó exclusivamente sobre la imagen forense, preservando intacto el dispositivo original.

---

5. Resultados y hallazgos

Durante el análisis se identificaron los siguientes elementos relevantes:

- La memoria USB contenía varios archivos activos, organizados en directorios visibles en el árbol del sistema.
- Autopsy detectó **archivos eliminados**, los cuales fueron recuperados parcialmente y analizados.
- Las vistas de *File Types* permitieron revisar categorías como documentos, imágenes, archivos comprimidos y otros, confirmando actividad reciente del usuario en la unidad.
- Las fechas de modificación registradas en los metadatos mostraron actividad en el dispositivo en fechas próximas a la presunta extracción de información.
- No se evidenciaron daños en el sistema de archivos ni corrupción significativa.
- Los valores hash generados durante la adquisición confirmaron que la imagen forense coincide bit a bit con el estado original del dispositivo.

Cada hallazgo fue documentado mediante capturas de pantalla, rutas internas y metadatos obtenidos desde la interfaz de Autopsy.

---

6. Conclusiones y observaciones

1. La evidencia digital fue preservada y analizada siguiendo procedimientos aceptados en informática forense, garantizando integridad y trazabilidad durante todo el proceso.
2. La adquisición en formato **E01**, junto con los hashes MD5 y SHA1 coincidentes, asegura que la imagen forense es una representación fiel del dispositivo original.
3. El análisis con Autopsy permitió identificar archivos activos y eliminados, así como metadatos relevantes para evaluar si existió manipulación reciente del contenido.

4. La unidad presenta indicios de actividad reciente que coincide con el período en que ocurrió la presunta fuga de información, lo que debe ser considerado por la autoridad competente.
5. Se recomienda conservar la imagen forense y este informe dentro de la carpeta de evidencia del caso para su posible presentación ante instancias judiciales.

---

7. Anexos

- Capturas de pantalla del proceso de adquisición (FTK Imager).
- Capturas de Autopsy mostrando:
    - estructura de directorios,
    - archivos eliminados,
    - metadatos,
    - timeline del sistema de archivos.
- Tabla con valores hash:
    - **MD5:** *938c2cc0dcc05f2b68c4287040cfcf71*
    - **SHA1:** b381b8d85046e94121735a2f19a89c795876e755
- Copia de la cadena de custodia completa.

Capítulo IV. Resultados de la investigación empírica

4.1 Resultados de las entrevistas

Se realizaron **tres entrevistas semiestructuradas** a:

- Un **docente universitario** del área de ciberseguridad.
- Un **técnico forense** de una institución pública.
- Un **analista de seguridad** de una empresa privada.

Del análisis de contenido emergieron varios temas comunes:

1. **Reconocimiento de la importancia de la evidencia digital**
   Los tres entrevistados coinciden en que la evidencia digital se ha vuelto “central” en las investigaciones actuales, especialmente por el aumento de incidentes como filtraciones de datos, fraudes en línea y accesos no autorizados. Todos señalan que, sin un tratamiento forense adecuado, “se pierde la oportunidad de que esa evidencia tenga valor en juicio”.
2. **Protocolos y documentación incompletos**
   El técnico forense indica que en su institución existen algunos formatos de cadena de custodia, pero no un **manual integral** de manejo de evidencia digital. El analista de seguridad comenta que en el sector privado suelen aplicar “buenas prácticas” basadas en experiencia, pero no siempre están formalizadas por escrito. El docente destaca que

muchos procedimientos se aprenden “por transmisión informal”, más que por normas internas claras.

3. **Capacitación insuficiente**
   Los tres entrevistados coinciden en que la **formación especializada en informática forense y derecho probatorio** es todavía limitada. El técnico menciona que la capacitación se da “de manera esporádica” y el docente señala que aún hace falta integrar mejor estos contenidos en los planes de estudio y en la formación de operadores de justicia.
4. **Uso de herramientas forenses con recursos limitados**
   Se observa que, en la práctica, se combina el uso de herramientas comerciales con **software libre** (por ejemplo, plataformas similares a Autopsy o utilidades de adquisición). El problema no es solo la herramienta, sino la falta de lineamientos claros sobre su uso, la documentación del proceso y la conservación de reportes y hashes.
5. **Dificultades en la cadena de custodia**
   Los entrevistados reportan que uno de los puntos más vulnerables sigue siendo la **cadena de custodia**. Cuando la evidencia pasa por varias dependencias o personas sin formación forense, es frecuente que no se registre correctamente quién la tuvo, en qué momento y bajo qué condiciones, lo que puede afectar su credibilidad en un proceso judicial.

4.2 Comparación con estándares internacionales y buenas prácticas

Al contrastar lo señalado por los entrevistados con los estándares internacionales (como **ISO/IEC 27037**, **NIST SP 800-86** y las recomendaciones sobre orden de volatilidad), se observa una **brecha relevante** entre lo que se considera ideal y lo que efectivamente se aplica en el contexto panameño:

- Los estándares insisten en la **documentación exhaustiva**, la designación de personal competente y el uso de herramientas verificadas; en la práctica, los entrevistados describen una realidad donde existen esfuerzos individuales, pero no siempre una política institucional clara.
- En materia de **preservación y adquisición**, los estándares recomiendan trabajar siempre sobre copias forenses y verificar integridad con hashes. Los participantes reconocen estas prácticas como “correctas”, pero admiten que no siempre se siguen de manera uniforme en todos los casos.
- Respecto a la **cadena de custodia**, los documentos internacionales la tratan como eje central; sin embargo, los testimonios reflejan que en Panamá todavía se observan registros incompletos, falta de controles en traslados y escasa sensibilización del personal no especializado.

En este sentido, el **procedimiento forense simulado** desarrollado en la investigación sirve como punto de comparación: al aplicar de manera ordenada la identificación del dispositivo, la adquisición bit a bit, el cálculo de hashes y el análisis en una herramienta especializada, queda en evidencia cuánto depende la calidad del proceso de contar con protocolos claros y de seguir los pasos de forma disciplinada.

4.3 Síntesis de hallazgos y vacíos detectados

De la integración de los resultados de las entrevistas y del procedimiento forense simulado se desprenden los siguientes hallazgos principales:

1. **Conciencia alta, implementación desigual**
   Los tres entrevistados tienen claro que la evidencia digital debe manejarse bajo criterios forenses, pero reconocen que **no todas las instituciones cuentan con lineamientos claros ni con personal suficientemente capacitado**.
2. **Protocolos fragmentados o inexistentes**
   No se observa un **marco unificado** que estandarice el manejo de evidencia digital en Panamá. Cada organización adapta sus propias prácticas, lo que genera variabilidad en la calidad técnica de los peritajes.
3. **Capacitación continua como necesidad prioritaria**
   La formación en informática forense, cadena de custodia digital y normativa aplicable se identifica como un **vacío crítico**, tanto en el ámbito técnico como en el jurídico.
4. **Limitaciones en recursos tecnológicos**
   La combinación de herramientas comerciales y gratuitas, sin una política clara de uso y documentación, supone un riesgo si no se acompaña de procedimientos bien definidos y verificación rigurosa de integridad.
5. **Vulnerabilidades en la cadena de custodia**
   La evidencia digital puede perder fuerza probatoria cuando no se registran adecuadamente las transferencias de custodia, los responsables y las condiciones de almacenamiento.

El **caso práctico simulado** confirma que, aun con una sola memoria USB, el proceso exige:

- registrar cuidadosamente la evidencia,
- adquirirla de forma forense,
- verificar hashes,
- analizarla con una herramienta especializada,
- y documentar cada acción.

Esto refuerza la idea de que, en el contexto panameño, la mejora del manejo de evidencia digital pasa tanto por **alinearse con estándares internacionales** como por **institucionalizar procedimientos y fortalecer la capacitación del personal**.

Capítulo V. Conclusiones y recomendaciones

5.1 Conclusiones generales sobre el manejo de evidencia digital

A partir del análisis del caso simulado y de las entrevistas realizadas a especialistas del ámbito académico, público y privado, se concluye que en Panamá existe una **clara conciencia de la importancia del manejo adecuado de la evidencia digital**, pero la implementación de buenas prácticas aún es **desigual y fragmentada**.

Los entrevistados coinciden en que la evidencia digital se ha convertido en un elemento central en las investigaciones actuales, pero señalan que **no todas las instituciones cuentan con protocolos formales**, manuales actualizados o formatos estandarizados para la cadena de custodia. En muchos casos, los procedimientos dependen de la experiencia individual del técnico o del criterio del equipo, más que de una política institucional clara.

El procedimiento forense simulado desarrollado en esta investigación permitió constatar, en un entorno controlado, que el manejo correcto de un solo dispositivo (como una memoria USB) exige: registrar adecuadamente la evidencia, adquirirla mediante una imagen forense, verificar su integridad con hashes y documentar cada acción. Esto refuerza la percepción de que **las debilidades no se encuentran tanto en el conocimiento básico de qué debe hacerse, sino en la sistematización y disciplina con que se aplica**.

En términos generales, los principales hallazgos apuntan a:

- **Déficit de protocolos unificados** de adquisición y custodia.
- **Capacitación insuficiente y no continua** en informática forense y derecho probatorio.
- **Limitaciones de recursos tecnológicos**, que obligan a combinar herramientas comerciales con software libre sin lineamientos uniformes.
- **Vulnerabilidades en la cadena de custodia**, especialmente cuando interviene personal no especializado.

5.2 Propuestas de mejora en los procesos de adquisición y custodia

En función de los hallazgos anteriores, se proponen las siguientes mejoras para fortalecer los procesos de adquisición y custodia de evidencia digital en el contexto panameño:

1. **Elaboración de protocolos institucionales estandarizados**
    - Diseñar y aprobar **procedimientos escritos** para identificación, preservación, adquisición, análisis y archivo de evidencia digital, tomando como referencia estándares internacionales y adaptándolos a la realidad local.
    - Incluir en dichos protocolos el uso obligatorio de formularios de **cadena de custodia digital**, con campos claros para registrar fechas, responsables, condiciones de almacenamiento y transferencias.
2. **Adquisición forense obligatoria sobre copias**
    - Establecer como principio que **ningún análisis debe realizarse sobre el dispositivo original**, sino sobre una **imagen forense** debidamente autenticada.
    - Incorporar en los lineamientos la verificación con **hashes (MD5, SHA-1 o superiores)** antes y después de la adquisición, documentando los valores en el expediente técnico.
3. **Fortalecimiento del registro documental**
    - Reforzar la cultura de **documentar cada acción** realizada sobre la evidencia: conexión del dispositivo, uso de herramientas, errores detectados, reintentos, generación de reportes.
    - Conservar los reportes generados por las herramientas forenses, así como capturas de pantalla y bitácoras de trabajo, como parte integral del expediente pericial.

4. **Mejoras en el manejo de la cadena de custodia**
    - Unificar modelos de formulario de cadena de custodia para todas las dependencias que manipulan evidencia digital.
    - Establecer que **ninguna transferencia de evidencia** (física o lógica) pueda realizarse sin firma y registro de la persona que entrega y la que recibe.

Estas medidas no requieren necesariamente cambios legislativos inmediatos, pero sí una **decisión institucional** de formalizar procedimientos y exigir su cumplimiento en cada caso.

5.3 Recomendaciones para la formación y acreditación de peritos informáticos

La investigación muestra que uno de los puntos más sensibles es la **formación y actualización del personal técnico y de los operadores de justicia**. Por ello, se plantean las siguientes recomendaciones:

1. **Programas de capacitación continua**
    - Implementar cursos y talleres periódicos sobre informática forense, cadena de custodia digital, análisis de dispositivos y uso de herramientas especializadas.
    - Incluir módulos específicos sobre el **marco jurídico panameño**, la Ley 51 sobre comercio electrónico, normas probatorias y la forma correcta de presentar la evidencia ante un juez.
2. **Acreditación y perfil del perito informático**
    - Definir un **perfil mínimo de competencias** para el perito informático, que incluya conocimientos técnicos, comprensión del proceso judicial y ética profesional.
    - Promover esquemas de **acreditación o certificación interna**, donde se reconozca formalmente a quienes cumplen con ciertos estándares de formación y experiencia.
3. **Articulación entre academia, sector público y privado**
    - Fomentar convenios entre universidades, instituciones públicas y empresas para desarrollar **laboratorios conjuntos, prácticas supervisadas y proyectos aplicados** que permitan a estudiantes y técnicos entrenarse en casos simulados similares al desarrollado en esta investigación.
    - Incentivar la participación de docentes y profesionales en la actualización de planes de estudio y en la construcción de guías técnicas locales.
4. **Sensibilización de operadores de justicia y personal no técnico**
    - Realizar jornadas de sensibilización dirigidas a fiscales, jueces, policías y personal administrativo sobre la **importancia de la evidencia digital y de la cadena de custodia**, de modo que comprendan por qué es crítico no manipular dispositivos sin instrucciones periciales.

Referencias bibliográficas

[1] S. Acurio Del Pino, *Manual de Manejo de Evidencias Digitales y Entornos Informáticos*, versión 2.0. Washington, DC, USA: Organización de los Estados Americanos, 2010. Ministerio Público de Panamá

[2] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 3rd ed. Burlington, MA, USA: Academic Press, 2011. Wikipedia

[3] B. Carrier, *File System Forensic Analysis*. Upper Saddle River, NJ, USA: Addison-Wesley, 2005. O'Reilly Media

[4] International Organization for Standardization, *ISO/IEC 27037:2012—Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*. Geneva, Switzerland: ISO, 2012. GitHub

[5] K. Kent, S. Chevalier, T. Grance, and H. Dang, *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2006. ResearchGate

[6] D. Brezinski and T. Killalea, "Guidelines for Evidence Collection and Archiving," RFC 3227, Internet Engineering Task Force, Feb. 2002. rfc-editor.org

[7] República de Panamá, "Ley 51 de 22 de julio de 2008, que define y regula los documentos electrónicos y las firmas electrónicas y adopta otras disposiciones sobre el comercio electrónico," *Gaceta Oficial Digital*, Panamá, 2008. SourceForge

[8] República de Panamá, "Ley 63 de 28 de agosto de 2008, que adopta el Código Procesal Penal y dicta disposiciones sobre su implementación," *Gaceta Oficial Digital*, Panamá, 2008. Scribd

[9] J. F. Buckridge, "Análisis crítico a la legislación regulatoria del comercio electrónico y firma digital en Panamá," *Revista Cathedra*, vol. 3, no. 2, 2017. revistas.umecit.edu.pa

[10] Exterro Inc., *FTK® Imager User Guide*, Version 4.7.1. Beaverton, OR, USA: Exterro, 2021. Wikipedia

[11] Sleuth Kit Labs, "Autopsy® Digital Forensics Platform – User Documentation," versión 4.21.0, 2023. [En línea]. Disponible: https://www.autopsy.com Autopsy

Anexos

Anexo 1. Guion de entrevista semiestructurada

Guion sugerido para entrevistas a especialistas y docentes:

1. ¿Qué experiencia tiene usted en el manejo de evidencias digitales en investigaciones o procesos judiciales?
2. Desde su perspectiva, ¿cuáles son las principales dificultades que se presentan al preservar y adquirir evidencia digital?
3. ¿Considera que en su institución existen protocolos claros sobre manejo de evidencia digital? Explique.
4. ¿Qué tan frecuente es la capacitación del personal en temas de informática forense y cadena de custodia?
5. ¿En qué medida cree usted que se aplican los estándares internacionales (ISO, NIST, RFC) en la práctica diaria?
6. ¿Percibe vacíos o necesidades de actualización en el marco legal panameño en relación con la prueba electrónica?
7. ¿Qué recomendaciones haría para mejorar la calidad de los peritajes informáticos y la valoración de la evidencia digital en los tribunales?

Anexo 2. Formato básico de cadena de custodia digital

Campos sugeridos para un formulario de cadena de custodia digital:

Código de evidencia: _____

Descripción del objeto: _____

Marca/Modelo: _____

Número de serie: _____

Fecha y hora de recolección: _____

Lugar de recolección: _____

Recolectado por (nombre y firma): _____

Entregado a (nombre y firma): _____

Fecha y hora de entrega: _____

Acciones realizadas sobre la evidencia (fecha, hora, responsable, descripción):

_____

_____

Condiciones de almacenamiento: _____

Observaciones: _____

Anexo 3. Estructura sugerida de informe pericial

1. Portada
   - Datos de la autoridad solicitante.

- Datos del perito.
- Identificación del caso.

2. Antecedentes
- Descripción breve de los hechos que dan origen al peritaje.
- Preguntas o puntos de pericia planteados por la autoridad.

3. Objetivo del peritaje
- Propósito específico del análisis.

4. Identificación de la evidencia
- Descripción detallada de los dispositivos y medios analizados.

5. Metodología
- Procedimientos de preservación, adquisición, verificación de integridad y análisis.
- Herramientas utilizadas.

6. Resultados
- Hallazgos técnicos presentados de manera ordenada y comprensible.

7. Conclusiones
- Respuestas a los puntos de pericia basadas en los resultados obtenidos.

8. Anexos
- Tabla de hashes.
- Copia de la cadena de custodia.
- Capturas de pantalla y registros relevantes.