TEQUILA SO

TECNOLOGÍA EXPLICADA CON MÉTODO

Herramientas gratuitas

Elegir, comprender y documentar antes de ejecutar

GUÍA PRÁCTICA ILUSTRADA · EDICIÓN 2026



Jocsan Laguna

Edición 2026 · Texto, ejercicios y diagramas en español claro

Fotografía de reconstrucción editorial; no representa un caso real.

HERRAMIENTAS GRATUITAS · GUÍA DE LECTURA

Cómo usar este manual

Una colección de programas no sustituye un método. Este manual reúne cinco herramientas porque responden preguntas distintas: FTK Imager para adquirir y previsualizar, Autopsy para analizar, ExifTool para metadatos, PhotoRec para recuperación por firmas y Volatility 3 para memoria.

> **Antes de ejecutar**
> La autorización y la preservación no dependen del precio del software. Leer una fuente puede exponer datos confidenciales; escribir en el destino equivocado puede destruir evidencia.

Qué contiene cada recurso

Recurso	Lectura correcta
Fotografía nueva	Reconstrucción editorial de un entorno de trabajo, no un caso real.
Captura oficial	Documentación de FTK Imager, Autopsy o ExifTool con atribución y versión.
Salida real de ExifTool	Resultado obtenido al ejecutar ExifTool 13.64 sobre 03_imagen_demo.png del laboratorio.
Ejercicio	Simulación con resultado esperado; no afirma ejecuciones que no se realizaron.

Reglas que evitan errores graves

- Autoriza antes de acceder, incluso cuando la técnica sea sencilla.
- Conserva el original y analiza una copia.
- Usa un destino separado para imágenes y archivos recuperados.
- Descarga solo desde el sitio oficial y verifica integridad cuando esté disponible.
- Registra versión, fecha, zona horaria, parámetros y operador.
- Distingue hallazgo, interpretación y conclusión.

Autor: Jocsan Laguna · Proyecto: Tequila SO · Revisión editorial y visual: 16 de noviembre de 2026.

MAPA DEL MANUAL

Contenido y recorrido de aprendizaje

Cómo usar este manual 2
Contenido y recorrido de aprendizaje 3
1. La herramienta se elige por la pregunta 4
2. FTK Imager: adquisición y vista previa 5
3. Autopsy: análisis, ingestas y cronología 6
4. ExifTool: metadatos concretos de archivos 7
5. PhotoRec: recuperación por firmas 8
6. Volatility 3: memoria bajo análisis 9
7. Un flujo de trabajo pequeño y auditable 10
8. Laboratorio ficticio y ejercicio de decisión 11
9. Ejercicios con resultados esperados 12
9. Ejercicios con resultados esperados 13
10. Plantillas de decisión y registro 14
11. Fuentes oficiales y versiones comprobadas 15
12. Créditos visuales y control editorial 16

Al terminar podrás

- Elegir una herramienta por la pregunta y no por la costumbre.
- Explicar qué puede y qué no puede demostrar cada programa.
- Leer una salida de ExifTool sin inventar campos ausentes.
- Distinguir adquisición, análisis, recuperación, memoria e informe.
- Resolver seis ejercicios con criterios explícitos de evaluación.

PREGUNTA · FUENTE · MENOR ALTERACIÓN

1. La herramienta se elige por la pregunta

Antes de abrir cualquier programa, escribe qué quieres saber, qué fuente tienes y qué no puedes alterar. La herramienta correcta es la que responde mejor con menor alteración, no la que tiene más funciones ni la que ya estaba instalada.

Pregunta	Herramienta	Resultado que sí puedes esperar	Lo que no demuestra
Necesito crear una imagen o revisar su contenido básico.	FTK Imager	Imagen, vista previa, exportación y verificación.	Un análisis completo del caso.
Necesito examinar archivos, actividad y cronología.	Autopsy	Artefactos, búsquedas, etiquetas, cronología e informes.	Autenticidad o autoría automática.
Necesito saber qué metadatos contiene un archivo.	ExifTool	Campos presentes y diferencias entre archivos.	Que fecha o ubicación sean necesariamente reales.
Necesito intentar recuperar contenido por firmas.	PhotoRec	Archivos recuperables desde una copia compatible.	Nombres, carpetas, totalidad ni éxito garantizado.
Necesito estudiar una captura de memoria.	Volatility 3	Procesos, conexiones y artefactos de esa captura.	El estado completo del sistema o su historia.

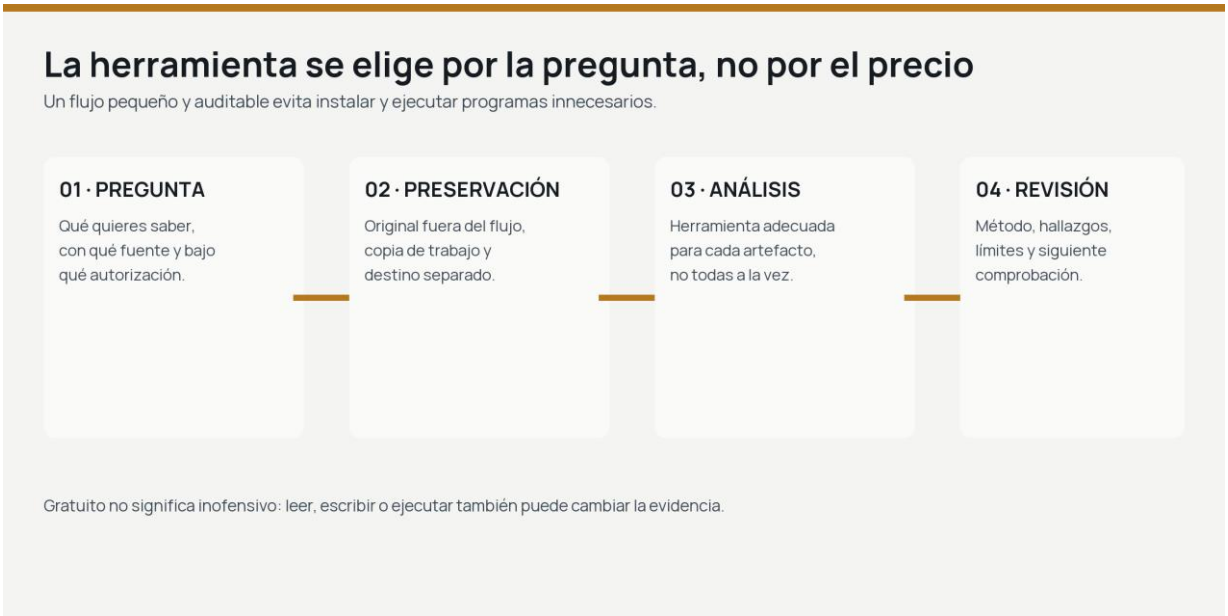


Figura 1. Un flujo pequeño y auditable empieza por pregunta y preservación, no por instalar programas. Diagrama propio.

Gratuito no significa inofensivo
Leer una fuente puede exponer datos; ejecutar una muestra puede activar malware; escribir en el destino equivocado puede destruir evidencia.

IMAGEN · VERIFICACIÓN · DESTINO

2. FTK Imager: adquisición y vista previa

FTK Imager crea imágenes, previsualiza archivos, exporta contenido y verifica integridad. La guía oficial 8.2 recomienda bloqueador de escritura de hardware para adquirir una unidad original. Montar una imagen no sustituye ese bloqueo.

Primer recorrido

1. Identifica fuente, autorización y destino separado.
2. Abre File > Create Disk Image.
3. Confirma origen por modelo, capacidad y serie, no solo por letra.
4. Elige formato, fragmentación y compresión adecuados al flujo posterior.
5. Activa verificación al crear y conserva el listado de contenido cuando proceda.
6. Revisa el resumen, los hashes y los errores de lectura.

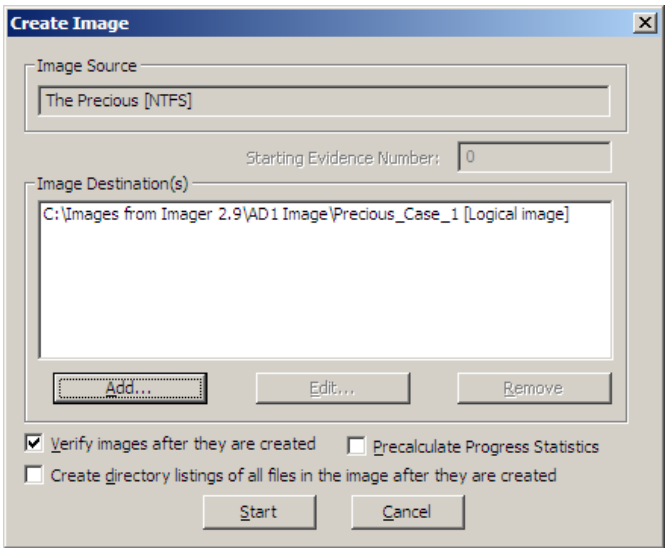


Figura 2. Destino, verificación al crear y listado de contenido. Captura de Exterro FTK Imager 8.2, guía oficial, pág. 74 del documento impreso.

No empieces por el análisis si todavía no sabes qué fuente es: la imagen creada no es la investigación terminada; todavía necesita revisión y contexto.

Consultar la guía oficial Exterro FTK Imager 8.2

CASO · MÓDULOS · TIMELINE

3. Autopsy: análisis, ingestas y cronología

Autopsy organiza un caso, añade fuentes, ejecuta ingestas y genera artefactos. La referencia de esta guía es 4.23.0. Crea el caso en una carpeta nueva, elige solo módulos necesarios y espera a que terminen antes de cerrar conclusiones.

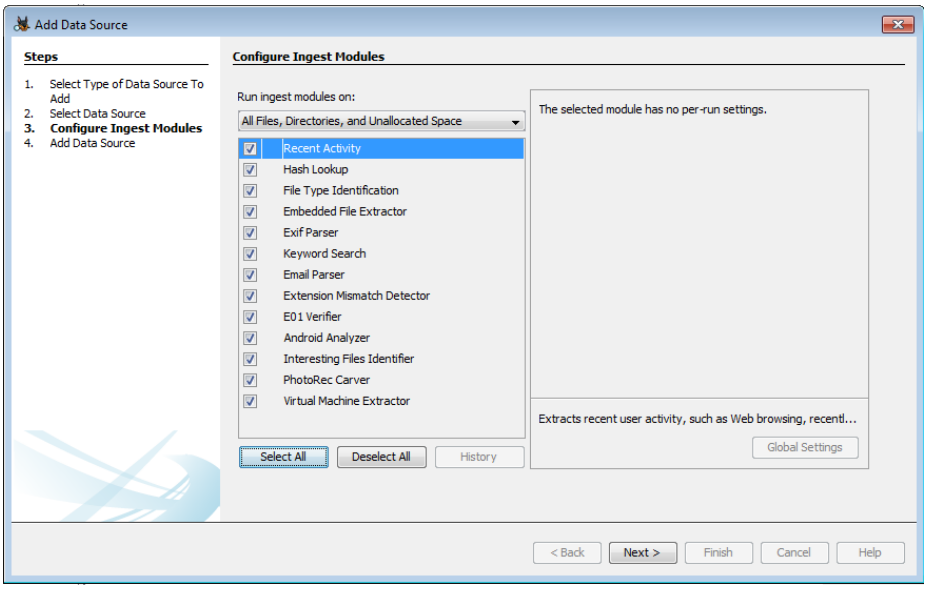


Figura 3. Selección de módulos de ingesta al añadir una fuente. Captura de Sleuth Kit Labs, documentación 4.23.0, CC BY-SA 3.0.

Primer recorrido

1. Crea un caso con una carpeta nueva.
2. Añade una imagen, un disco controlado o archivos lógicos autorizados.
3. Elige módulos según la pregunta, no todos por defecto.
4. Busca contenido, revisa su ubicación y etiqueta lo relevante.
5. Usa Timeline con ventana y zona horaria documentadas.
6. Genera un informe de elementos etiquetados y añade método y límites fuera del resultado automático.

> **Logical Files no equivale a un disco completo**
> Ese método no examina espacio no asignado ni archivos eliminados del dispositivo; úsalo para practicar con documentos autorizados, no para prometer recuperación.

Consultar documentación Autopsy 4.23.0

EXIFTOOL 13.64 · CAMPOS PRESENTES · AUSENCIAS

4. ExifTool: metadatos concretos de archivos

ExifTool lee, escribe y edita metadatos en muchos formatos. La referencia comprobada para esta edición es 13.64. La página oficial ofrece paquetes y sumas de comprobación; no uses copias de sitios ajenos.



Figura 4. Revisión de metadatos de una imagen y sus campos presentes. Reconstrucción editorial; no es una fotografía de evidencia.

Lectura básica, sin modificar archivos

Abre una terminal dentro de una copia del laboratorio y ejecuta los comandos. No inventa fecha, cámara ni ubicación si no existen. La imagen fue creada como demostración; su contenido y metadatos no representan una captura real.

```
exiftool 03_imagen_demo.png
exiftool -filename -imagesize -datetimeoriginal -gps:all -model 03_imagen_demo.png
exiftool -s 03_imagen_demo.png
```

ExifTool 13.64 · ejecución sobre archivo ficticio

```
$ exiftool -filename -imagesize -datetimeoriginal -gps:all -model 03_imagen_demo.png
File Name                       : 03_imagen_demo.png
Image Size                      : 1000x700
-- press ENTER --
```

Figura 5. Salida real de ExifTool 13.64 sobre 03_imagen_demo.png: nombre y tamaño presentes; los demás campos solicitados no aparecen. Ejecución realizada para esta edición.

La ausencia de campos también es información: no afirmes que existe una ubicación o un dispositivo de captura si el archivo no los contiene. Nunca escribas metadatos sobre el original para hacerlos coincidir con una hipótesis.

Consultar ExifTool, documentación y paquetes oficiales

RECUPERACIÓN · FIRMAS · DESTINO SEPARADO

5. PhotoRec: recuperación por firmas

PhotoRec busca datos mediante firmas de archivo incluso cuando el sistema de archivos está dañado o fue reformateado. Es gratuito, de código abierto y se distribuye junto con TestDisk. Su acceso es de solo lectura para el origen, pero debes elegir otro destino para los recuperados.

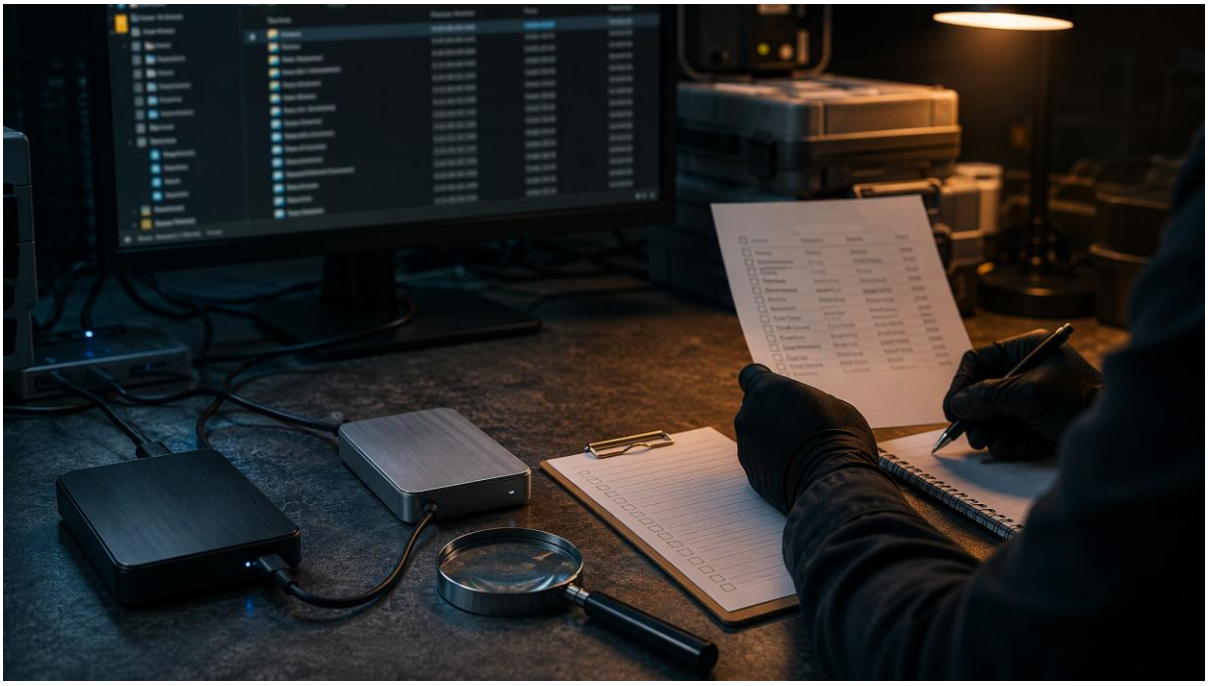


Figura 6. Revisión de resultados recuperables y su destino separado. Reconstrucción editorial; no es una recuperación real.

Recorrido responsable

1. Detén el uso de la fuente para reducir sobrescritura.
2. Crea una imagen o selecciona una copia de trabajo autorizada.
3. Ejecuta PhotoRec sobre esa copia, no sobre el original.
4. Elige otro destino para los resultados.
5. Revisa archivos recuperados, contenido y relación con la fuente.
6. Documenta qué se pudo leer y qué quedó incompleto.

> **PhotoRec no devuelve el pasado completo**
> Los nombres y las carpetas suelen perderse; la fragmentación puede producir archivos incompletos; recuperar contenido no demuestra quién lo creó ni qué sucedió.

Consultar PhotoRec y TestDisk en CGSecurity

CAPTURA · SÍMBOLOS · COMPLEMENTOS

6. Volatility 3: memoria bajo análisis

Volatility 3 analiza capturas de memoria mediante complementos. No sustituye la adquisición: necesitas una captura compatible y los símbolos adecuados para el sistema examinado. La captura y el análisis posterior son operaciones diferentes.



Figura 7. Captura y análisis de memoria tienen efectos, archivos y responsabilidades diferentes. Diagrama propio.

Ejemplos de lectura, no de este laboratorio

Estos comandos requieren una captura autorizada y compatible. El nombre memoria_demo.raw es ilustrativo: el paquete no distribuye una captura ni se afirma que los comandos se ejecutaron.

```
python vol.py -f memoria_demo.raw windows.info
python vol.py -f memoria_demo.raw windows.pslist
python vol.py -f memoria_demo.raw windows.netscan
```

> **Una captura muestra un momento, no toda la historia**
> Los procesos y conexiones visibles dependen del momento, la adquisición y la compatibilidad de los símbolos. No descargues dumps de orígenes desconocidos que puedan contener datos sensibles o malware.

Consultar Volatility 3 en GitHub y su documentación

MÉTODO · DECISIONES · EVIDENCIA DE TRABAJO

7. Un flujo de trabajo pequeño y auditable

Con cinco herramientas puedes cubrir un flujo básico sin acumular programas innecesarios. No es obligatorio usar todas en todos los casos: la navaja de Ockham también aplica aquí; elige la que responda mejor con menor alteración.

Etapa	Acción	Evidencia de trabajo
Autoridad	Delimitar objetivo, fuente y permisos.	Alcance, custodio y exclusiones.
Adquisición	Crear imagen o copia controlada.	Método, versión, fecha, destino y hash.
Revisión	Abrir fuente en FTK Imager y localizar archivos.	Ruta, formato y observaciones iniciales.
Análisis	Usar Autopsy con ingestas seleccionadas.	Artefactos, búsquedas, etiquetas y cronología.
Metadatos	Consultar ExifTool en copias concretas.	Campos presentes y diferencias, sin reescribir original.
Recuperación	Usar PhotoRec cuando la pregunta lo justifique.	Resultados revisados y límites de recuperación.
Memoria	Analizar una captura con Volatility cuando sea necesaria.	Fuente compatible, complementos y salidas.
Informe	Explicar método, hallazgos y límites.	Revisión reproducible y fuentes citadas.

La herramienta no decide por ti

Una lista de resultados no sustituye la explicación de por qué elegiste la fuente, el módulo, el parámetro y la siguiente comprobación.

PRÁCTICA · INVENTARIO · INTEGRIDAD

8. Laboratorio ficticio y ejercicio de decisión

El ZIP contiene documentos, un EML, una imagen y notas creadas para enseñar. No es una captura real de un caso. Calcula el hash del ZIP antes de descomprimirlo y compáralo con SHA256SUMS.txt.

Descargar Laboratorio_Forense_Jocsan.zip desde Tequila SO

Objeto	Decisión y lectura correcta
01_notas.txt	Añadir como Logical Files y buscar “lavanda” para practicar ubicación y contexto.
02_correo_demo.eml	Comprobar que el remitente usa dominio reservado; no afirmar envío real.
03_imagen_demo.png	Revisar campos existentes y ausentes con ExifTool; no asumir cámara o GPS.
04_documentos/datos-inventario.txt	Usar para clasificación e inventario, no como prueba de hechos reales.
05_navegador/history-demo.txt	Leer cronología manual; no abrir como base real de navegador.
metadatos-demo.json	Metadatos de enseñanza; relacionarlos con el objeto ficticio correspondiente.
SHA256SUMS.txt	Comprobar integridad del paquete antes de trabajar.

Salida de cinco líneas

- Fuente: qué carpeta y objeto elegiste.
- Método: qué herramienta y parámetros usaste.
- Hallazgo: qué aparece realmente en el archivo.
- Limitación: qué no puedes concluir con ese objeto.
- Siguiente comprobación: cómo revisas sin alterar más la fuente.

No ejecutes comandos de memoria sobre una captura inexistente
El laboratorio enseña lectura y análisis de archivos; la memoria requiere otra fuente autorizada y compatible.

PRÁCTICA 1–3 · ELEGIR Y COMPROBAR

9. Ejercicios con resultados esperados

Ejercicio 1 · La herramienta adecuada

Consigna: necesitas crear una imagen de una carpeta, revisar sus metadatos y buscar una palabra. Elige herramienta y orden, sin usar todas las demás por obligación.

Resultado esperado

FTK Imager para crear y previsualizar, ExifTool para campos concretos y Autopsy para ingestas y búsqueda. El orden documenta primero fuente y preservación, después análisis. No hace falta PhotoRec ni Volatility para esa pregunta.

Criterio: 1 punto por herramienta y 1 por orden y límite. Elegir todas las herramientas sin justificación no es un método.

Ejercicio 2 · Campos ausentes

Consigna: la salida de ExifTool muestra nombre y tamaño, pero no modelo, fecha original ni GPS. Explica qué puedes escribir y qué no.

Resultado esperado

Puedo afirmar nombre y dimensiones. No puedo afirmar cámara, fecha original o ubicación porque esos campos no aparecen. La ausencia se registra como limitación, no se rellena con valores imaginarios.

Criterio: 2 puntos por no inventar campos y 1 por registrar la ausencia como información.

Ejercicio 3 · Recuperación responsable

Consigna: una fuente parece dañada y necesitas recuperar archivos. Explica qué haces primero y dónde escribes los resultados.

Resultado esperado

Detener uso, preservar original, trabajar sobre imagen o copia autorizada y elegir otro destino para recuperados. PhotoRec puede encontrar contenido por firmas, pero no garantiza nombres, carpetas ni recuperación total.

Criterio: 2 puntos por preservación y destino separado; 1 por declarar límites.

PRÁCTICA 4–6 · ANÁLISIS E INFORME

9. Ejercicios con resultados esperados

Ejercicio 4 · Memoria inexistente

Consigna: alguien pide ejecutar Volatility sobre el laboratorio. Explica por qué no hay comando válido para ese paquete.

> **Resultado esperado**
> El ZIP no contiene captura de memoria. Volatility necesita una fuente compatible y símbolos adecuados. Se explica el comando solo como ejemplo, sin afirmar que se ejecutó ni descargar dumps desconocidos.

Criterio: 2 puntos por reconocer la ausencia de fuente y 1 por evitar descargas o ejecuciones inseguras.

Ejercicio 5 · Ingesta y cronología

Consigna: eliges módulos para buscar “lavanda” y revisar imágenes. Justifica tu elección y el período de Timeline.

> **Resultado esperado**
> Keyword Search para localizar la palabra y Picture Analyzer para campos EXIF compatibles. File Type Identification ayuda a identificar tipos. Timeline se limita a una ventana y zona horaria documentadas; no se interpreta una barra como intención.

Criterio: 1 punto por módulo, 1 por ventana y 1 por límite de interpretación.

Ejercicio 6 · Informe de cinco líneas

Consigna: redacta una salida con fuente, método, hallazgo, límite y siguiente comprobación.

> **Modelo de respuesta**
> Fuente: carpeta ficticia. Método: Logical Files, búsqueda y ExifTool sobre copia. Hallazgo: “lavanda” y tamaño de imagen. Límite: no hay fecha, GPS, memoria ni caso real. Siguiente comprobación: revisar informe, hash y contexto con otra persona.

Criterio: 1 punto por cada línea clara y limitada. Una respuesta extensa que oculta ausencias no obtiene puntuación completa.

PLANTILLAS · TRAZABILIDAD · REVISIÓN

10. Plantillas de decisión y registro

Campo	Contenido que debes capturar
Pregunta	Qué quieres demostrar y qué otra explicación admite los objetos.
Fuente	Tipo, origen, identificador, estado y relación con copia de trabajo.
Autoridad	Alcance, permisos, exclusiones y finalidad del examen.
Herramienta	Nombre, versión, módulos o complementos y parámetros.
Destino	Carpeta separada para imagen, exportaciones y recuperados.
Integridad	Algoritmo, objeto, valor y momento de cada comprobación.
Hallazgo	Archivo, ruta, contenido, fecha, resultado negativo e incidencia.
Límite	Campos ausentes, cobertura, fuentes no disponibles y alternativas.
Siguiente acción	Comprobación que discrimina hipótesis sin alterar más la fuente.

Revisión antes de entregar

- No hay comandos para fuentes inexistentes ni resultados inventados.
- Cada herramienta tiene una razón documentada para haber sido elegida.
- Cada exportación y derivado conserva relación con su origen.
- Los errores y ausencias permanecen visibles.
- Las fotografías editoriales no se presentan como evidencia real.

Control de calidad
El informe se revisa por identidad, cobertura, método y continuidad, no solo por presentación visual.

FUENTES · VIGENCIA · DOCUMENTACIÓN

11. Fuentes oficiales y versiones comprobadas

Documentación principal

1. Exterro FTK Imager 8.2 User Guide y canal oficial de descargas.

2. Autopsy 4.23.0: documentación de usuario.

3. ExifTool: sitio oficial, paquetes y documentación.

4. ExifTool Application Documentation.

5. PhotoRec ES, CGSecurity.

6. TestDisk Download.

7. Volatility 3: repositorio oficial.

8. Volatility 3: documentación generada.

9. ISO/IEC 27037 y NIST SP 800-86.

Versiones utilizadas en esta edición

- FTK Imager 8.2, sin declararla la versión más reciente.
- Autopsy 4.23.0, con capturas de su documentación oficial.
- ExifTool 13.64, verificado con ejecución real sobre 03_imagen_demo.png.
- PhotoRec y Volatility 3 se explican con documentación, sin afirmar ejecuciones no realizadas.

Control de versiones
Revisión editorial y de fuentes: 16 de noviembre de 2026. Las interfaces y los formatos cambian: consulta siempre documentación vigente antes de aplicar un procedimiento real.

IMÁGENES · LICENCIAS · CIERRE

12. Créditos visuales y control editorial

Recurso	Procedencia y uso
Portada y figuras 4 y 6	Fotografías nuevas creadas con apoyo de IA y revisadas visualmente. Reconstrucciones editoriales; no documentan casos reales.
Figura 2	Captura de Exterro FTK Imager 8.2 User Guide, página impresa 74.
Figura 3	Captura de Sleuth Kit Labs, Autopsy 4.23.0, licencia CC BY-SA 3.0.
Figura 5	Salida real de ExifTool 13.64 obtenida para esta edición con el archivo ficticio del laboratorio.
Figuras 1 y 7	Diagramas propios de flujo y memoria. No representan mediciones.
Identidad Tequila SO	Escudo original aportado para esta línea editorial. No implica aval institucional adicional.
Tipografías	Manrope, Source Serif 4 e IBM Plex Mono, utilizadas en la línea editorial del proyecto.

Control editorial

- Se añadieron fotografías, diagramas y capturas para cada herramienta.
- Se actualizó ExifTool a la versión vigente 13.64 y se comprobó su salida real.
- Se incluyeron seis ejercicios con resultados esperados y plantillas de trabajo.
- Se eliminaron páginas casi vacías y se mantuvieron visibles alcance y límites.
- Las traducciones no forman parte de este trabajo.

Antes de un caso real
Comprueba documentación vigente, autorización y cobertura. Esta guía es material educativo; no sustituye revisión profesional, autoridad ni asesoría jurídica.

La idea que debe quedar

La herramienta adecuada es la que responde tu pregunta con menor alteración. Conserva el original, registra cada decisión y deja que la evidencia —no la interfaz— determine hasta dónde puedes concluir.

Tequila SO · Jocsan Laguna · Edición 2026.