UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERÍA
CARRERA DE SISTEMAS Y COMPUTACIÓN

PROYECTO DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS Y COMPUTACIÓN.

TRABAJO DE TITULACIÓN

CREACIÓN DE UNA GUÍA DE RECUPERACIÓN DE DATOS UTILIZANDO LA TÉCNICA FORENSE FILE CARVING PARA ORDENADORES WINDOWS

Autor(es):

Luis Felipe Borja Brito

Tutor:

PhD. Fernando Molina

Riobamba - Ecuador

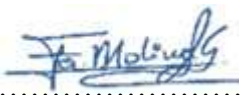
Año 2021

PAGINA DE ACEPTACIÓN

Los miembros del Tribunal de Graduación del proyecto de investigación de título: **CREACIÓN DE UNA GUÍA DE RECUPERACIÓN DE DATOS UTILIZANDO LA TÉCNICA FORENSE FILE CARVING PARA ORDENADORES WINDOWS** presentado por el Sr. Luis Felipe Borja Brito, dirigida por: PhD. Fernando Tiberio Molina Granja.

Una vez escuchada la defensa oral y revisado el informe final del proyecto de investigación con fines de graduación escrito en el cual se ha constatado el cumplimiento de las observaciones realizadas, remite la presente para uso y custodia en la biblioteca de la Facultad de Ingeniería de la UNACH.

Para constancia de lo expuesto firman:



PhD. Fernando Molina …….

Director del Proyecto Firma

Ing. Diego Reina …….

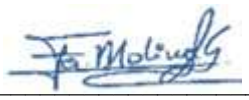
Miembro del Tribunal Firma

Ing. Gonzalo Allauca ……

Miembro del Tribunal Firma

DERECHOS DE AUTORÍA

La responsabilidad del contenido de este proyecto de Graduación corresponde exclusivamente al: Sr. Luis Felipe Borja Brito, bajo la dirección del PhD. Fernando Tiberio Molina Granja y el patrimonio intelectual de la misma a la Universidad Nacional de Chimborazo.



PhD. Fernando Molina Granja
060232807-2
Director del Proyecto

Luis Felipe Borja Brito
060411353-0
Autor

DEDICATORIA

El presente trabajo investigativo se lo dedico a mis padres, José Vicente Borja (+) y Rosa Elvia Brito, mis hermanos, quienes me han brindado su apoyo incondicional durante mi vida, por lo que les estoy eternamente agradecidos.

Luis Felipe Borja Brito

AGRADECIMIENTO

A Dios por la vida y a mi familia por el apoyo incondicional.

Un especial agradecimiento a los peritos especializados en el área de Informática Forense de la Fiscalía General del Estado, quienes me brindaron sus conocimientos esenciales para la consecución del presente trabajo investigativo.

También, expreso un profundo agradecimiento a mi tutor de tesis, PhD. Fernando Molina y miembros del tribunal Ing. Diego Reina e Ing. Gonzalo Allauca quienes, a través de sus copiosos conocimientos y experiencias, fueron importantes para el desarrollo del presente trabajo.

Y para terminar un agradecimiento infinito a la Universidad Nacional de Chimborazo, que, por medio de la Escuela de Ingeniería en Sistemas y Computación, me brindaron los conocimientos esenciales que me servirán durante mi vida profesional.

Luis Felipe Borja Brito

INDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

RESUMEN

En la actualidad, con la globalización, la sociedad se ha acostumbrado al uso diario de medios como ordenadores para la creación, almacenamiento y procesamiento de datos de información; por lo que se ve la necesidad de crear medios necesarios para la protección y recuperación de estos, por lo que es sumamente necesario establecer un mecanismo o guía que de manera clara indique al usuario la metodología correcta para la recuperación de archivos perdidos. En sí, el problema que se nos presenta actualmente es que los ordenadores más modernos tienen una alta capacidad de procesamiento y almacenamiento de datos, por lo que en muchas ocasiones esta información es desconocida por el propio usuario, y que en Ecuador, no existe métodos para esta recuperación de datos, por lo que es necesario la creación de esta guía enmarcada en la técnica forense File Carving, por cuanto nos indicará las directrices, recomendaciones y mejores prácticas para la recuperación de la información.

Es por lo cual que el presente trabajo investigativo, a través de un método deductivo, por medio del análisis bibliográfico de varias guías con estándares mundialmente conocidos para recuperación de datos como UNE 71505:2013, UNE 71506:2013, etc., y en base a un enfoque cualitativo a través del estudio de todas las actividades relaciones con la recuperación de datos mediante técnicas forenses, se pudo procesar los datos, llegando al resultado de la creación de una Guía de recuperación de datos con técnica forenses File Carving, con una aplicabilidad positiva a través de peritos informáticos.

Palabras clave: File Carving, Ordenador, Procesamiento de datos, Perito Informático, Recuperación de Datos.

ABSTRACT

Nowadays, globalization has made the community more adapted to the daily use of devices like computers to create, storage, and processing data information. Therefore, the creation of directions to protect and recover this data is really necessary, establishing an instrument or manual that indicates to the user the correct methodology to recover the lost files. Actually, the problem that we have experienced with most modern computers is the high processing and storage of data capacity. Still, in most cases, this information is unknown to the device user. Ecuador doesn't have any method to recover the data and lost files. It is unfortunate despite having supercomputers, so creating a new and helpful guide that provides the correct forensic technical assistance, "Data Carving," and the guidelines, recommendations, and best practices for information recovery and tools for testing. Not only research matters, but that's also why by using a deductive approach, and the bibliographic analysis as well the several guides with world-known standards for data recovery such as UNE 71505: 2013, UNE 71506: 2013, etc., regarding the qualitative approach, the related activities have been investigated by exanimating the data recovery using forensic techniques, the data might be processed, thus to the creation of a "Forensic Data Carving Manual", which is a standing opportunity to computer experts to improve their performance at work.

Keyword list: File Carving, Computer, Data Processing, Computer Expert, Data Recovery.

Reviewed by:
Mgs. Marcela González Robalino
English Professor
c.c. 0603017708

INTRODUCCIÓN

El desarrollo de los avances científicos ha estado estrechamente ligado con el progreso de la sociedad; es motivo por el cual cada ser humano con el pasar del tiempo debe adaptarse a cada uno de los avances tecnológicos que se le presenta en el camino.

Dentro del uso de los avances tecnológicos está el uso de medios como los ordenadores, que han sido una base esencial para la creación, desarrollo, procesamiento y almacenamiento de la información; motivo por el cual es necesario la creación de técnicas y/o métodos para que esta información pueda ser recuperada en caso de pérdida por algún daño.

Es importante resaltar que esta información se almacena utilizando alguna cualidad eléctrica, magnética u óptica de un material para representar un estado, 0 o 1. A esa unidad elemental de información la llamamos bit, y los datos se representan como secuencias de bits que toman significado de acuerdo como las interpretemos. Los sistemas de archivos son una serie de reglas y estructuras que permiten a un sistema operativo ordenar y organizar cómo se almacena la información en un dispositivo de almacenamiento, y funcionan en conjunto con los drivers de dispositivo para brindar una forma accesible de almacenar y acceder a los datos (archivos). Estos archivos almacenan información que contienen: bloques del dispositivo, fecha de creación y acceso, entre otros datos. Toda esta información administrativa se conoce con el nombre de metadatos. (Contanzo & Waimann, 2012).

Pero qué pasaría si la información almacenada en el disco duro es borrada por algún motivo ya sea por virus, daños mecánicos o defectos de fábrica, todos estos problemas toman relevancia cuando la recuperación de los datos se dificulta en gran medida. Casos como estos se deberían tomar en consideración para poder disminuir este riesgo. (Ninahualpa & Diaz, 2017)

Con estos problemas ahora viene la necesidad de buscar formas de recuperación de datos que hayan sido borrados, actualmente se encuentra disponible en el mercado varias herramientas, sin embargo, la existencia de una guía clara que indique al usuario como

debe hacerlo correctamente y que programas son los recomendados para este fin es el principal objetivo de esta investigación.

El propósito de esta investigación "Creación de una guía de recuperación de datos utilizando la técnica forense File Carving para ordenadores Windows", es plantear una guía que identifique el problema de la perdida de información y buscar la solución mediante la recuperación de los datos; por lo que en un contexto general la implementación de esta guía servirá a la sociedad en general, considerando la información obtenida de diferentes estudios que tienen relación con el tema.

La estructura del presente trabajo de investigación se dividirá en cuatro capítulos que son:

Capítulo I: Presenta el planteamiento del problema y su justificación y los objetivos.

Capítulo II: Presenta el estado del arte relacionado al tema de investigación.

Capítulo III: Presenta la metodología que se va a usar.

Capítulo IV: Presenta los resultados y análisis obtenidos mediante técnicas de recolección de información.

Independientemente de los capítulos, se presenta las conclusiones, recomendaciones y anexos de la investigación.

CAPÍTULO I

1. PLANTEAMIENTO DEL PROBLEMA

1.1. Problema y Justificación

Las computadoras hoy en día poseen una gran capacidad de procesamiento, como también de almacenamiento; llegando esta tener capacidades entre 60gb y 20tb, lo que se vuelve un problema, esto porque mientras más capacidad tenga la unidad de almacenamiento, tardará más tiempo el proceso de recuperación y escoger la información que es relevante para el investigador se vuelve complejo. En algunos casos la información que se logra almacenar en el disco duro es desconocida en su totalidad por los usuarios, convirtiéndose en un verdadero problema en la obtención de información privada, tanto para un agente externo (aplicación dañina, malware, hacker) como para un peritaje digital, en el supuesto caso en que el propietario esté involucrado en una controversia legal.

Sin embargo, para poder extraer la información de este tipo de dispositivos existen muchas técnicas o métodos, pero el de mayor eficacia es aquel que considera la recuperación de la información a través del sistema de ficheros del sistema operativo; el que incluso tiene la capacidad de poder encontrar información que fue modificada o borrada con anterioridad.

Ahora la interrogante sería ¿cómo el usuario podría recuperar la información borrada de su disco duro con diversas herramientas sin una guía que garantice la ejecución de ese proceso?

En Ecuador no existe documentos o guías que oriente a la persona interesada con técnicas necesarias para recuperar los datos de forma profesional. Igualmente, no brinda información de herramientas adecuadas que permita la recuperación de datos en su computadora. (Cuenca & Jaramillo, 2015)

Es así como la creación de esta guía de recuperación de datos aplicando la técnica forense File Carving permitirá aportar al mejoramiento del proceso de recuperación información, puesto que el usuario dispondrá de directrices, recomendaciones y mejores prácticas como resultado de un mejor uso de las herramientas dedicadas a este propósito.

1.2. Objetivos

General

Crear una guía de recuperación de datos utilizando la técnica forense File Carving que permita una mejor confiabilidad en el proceso de recuperación de la información.

Específicos

- Investigar y analizar el método File Carving y sus herramientas para el proceso de recuperación de datos en ordenadores Windows.
- Desarrollar la guía de recuperación de datos aplicando la técnica forense File Carving basado en la normativa nacional e internacional.
- Validar la guía de recuperación de datos en ordenadores Windows.

CAPÍTULO II

2. ESTADO DEL ARTE RELACIONADO A LA TEMÁTICA

2.1. Estado del arte

2.1.1. File Carving

Entre los beneficios que brinda el File Carving se puede indicar que se encuentra dentro de los procesos forenses en lo referente a recuperación de datos, así como también en la restauración y reconocimiento de archivos de interés que estén dañados o extraviados. En la actualidad, esta técnica genera copias de todos los archivos recuperados, haciendo que durante el proceso genere archivos basura. (Laurenson, 2013)

Existen diferentes algoritmos de Carving como las indicadas en la figura 1:

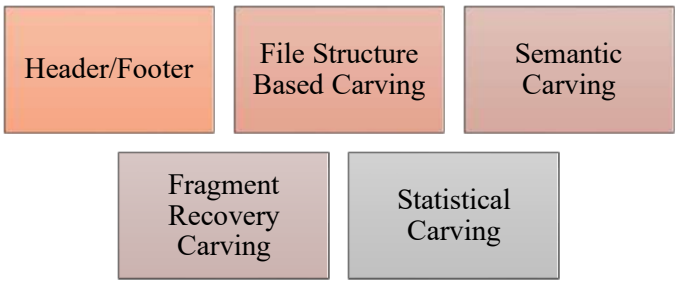


Figura 1: Algoritmos de Carving
Fuente: Elaboración propia.

- **Header/Footer**

Una de las técnicas más conocidas dentro de File Carving, permite la recuperación de archivos con la desventaja de generar falsos positivos.

- **File Structure Based Carving**

Se basa mediante formatos de archivos y estructuras, su enfoque es en la validación de archivos

- **Semantic Carving**

Es un conjunto de algoritmos encargados de aplicar medidas de interpretación de la información además de formar archivos coherentes.

- **Fragment Recovery Carving**

Algoritmo encargado de juntar diversos bloques por medio de métricas, donde identifica su formato de archivo y posteriormente analiza su reconstrucción basándose en un pool de bloques.

- **Statical Carving**

Toma decisiones en la reconstrucción de archivos en bloques analizados y el formato del archivo a reconstruir, todo esto mediante un cálculo estadístico. El propósito de esta técnica es buscar el inicio y el fin de los archivos como también de los bloques intermedios.

Para poder recuperar la información se puede aplicar cualquier tipo de métrica con el fin de evaluar el rendimiento, velocidad y calidad de los resultados. Estos algoritmos se lo pueden clasificar mediante Carving básico o Carving avanzado. Donde Carving básico incluye los algoritmos que únicamente pueden recuperar información de forma lineal (una detrás de otra) y Carving avanzado entra todo algoritmo que tenga la capacidad de recuperar datos fragmentados, ya sean estos desorganizados o incompletos. (Constanzo & Waimman, 2018)**.**

Métricas de Carving

Las métricas ayudan a comparar el rendimiento entre los algoritmos conocidos. Alguna de ellas son las siguientes:

- **Cantidad de archivos recuperados**

Es decir, los archivos que hayan sido obtenidos mediante Carver para el proceso de extracción.

- **Cantidad de archivos no recuperados**

Todo archivo que por algún motivo no pudo ser recuperado por Carving, esta medida solo debe ser tomada en cuenta cuando se conozca a profundidad la imagen analizada.

- **Cantidad de archivos validos recuperados**

Son los archivos que se logró recuperar por Carver y que posean información válida. Mediante la extensión de un archivo, esta medida ayuda a saber cuántos archivos recuperados existen.

- **Precisión del Carving y Carving Recall**

Indica el total de archivos recuperados, es decir, cuantos son válidos o se obtuvieron de forma parcial. Existe un cálculo para conocer la precisión por archivos válidos y parciales como la presentada a continuación:

$$ArchivosValidos = \frac{dat.recuperados\_validos}{total.recup}$$

$$ArchivosParcial = \frac{dat.recuperados\_parcial}{total.recup}$$

Durante el análisis, en Carving Recall indica cuantos archivos se logró recuperar, dando como resultado un cálculo para conocer archivos válidos o parciales.

$$CRecallValidos = \frac{dat.recuperados\_validos}{total.reales}$$

$$CRecallParcial = \frac{dat.recuperados\_parcial}{total.reales}$$

Se debe establecer claramente un punto de diferencia entre File Carving y Data Carving, por cuanto el primero lo que pretende realizar es una recuperación de bloque enteros de información, y que respeta su estructura misma; mientras que el segundo se encarga de recuperar fragmentos de datos más pequeños. (Di Ioro, Lamperti & Cistoldi, 2017)

El crecimiento exponencial de la tecnología de información ha surgido también en la comisión de delitos informáticos, y ahí es donde entran varias técnicas entre ellas *File Carving*, como métodos de recuperación de datos para peritos; que ha permitido una reconstrucción de la línea de tiempo de datos y a la vez realizar exámenes detallados de sistemas de archivos, con la única finalidad de obtener una respuesta viable como investigación forense. (Grijalva & Loarte, 2017).

La técnica File Carving resulta útil para la extracción de información en datos binarios que no están estructurados, esto lo convierte en un método innovador en el ámbito forense

digital, así como también aplicaciones educativas hacia estudiantes universitarios. (Cantrell & Runs, 2020).

2.1.2. Recuperación de datos

Los errores en el disco duro es la causa más común causante de la pérdida de información a nivel global, un 72% de personas tuvieron en algún momento problemas en su computadora personal, un 15% perdieron su información de su disco duro y finalmente el 13% surgieron en servidores tipo RAID, lo que evidencia que la perdida de información no solamente ocurre a personas naturales, también afecta al campo profesional. Recuperar los datos es el conjunto de fases y procedimientos con el fin de mitigar los factores que causa la pérdida de la información, el mayor porcentaje de perdida de información se viene evidenciado en los golpes y caídas que sufre la unidad de almacenamiento. (Ninahualpa, Pérez, Yoo, Guarda, Diaz & Piccilli; 2018).

La recuperación de datos es el proceso de analizar una unidad de almacenamiento con el objetivo de obtener la información extraviada ya sea por diversos motivos como lo indica la Tabla 1. Debe poseer una metodología para poder realizar la investigación y poder recuperar la información de forma correcta. (García, García & Meana, 2010)

Causas de pérdida de información

Algunas causas más conocidas son las siguientes:

Tabla 1: *Causas – Consecuencias*
Fuente: Elaboración propia

Causas	**Consecuencias**
Falla eléctrica	Error en el cabezal de lectura Daño en la placa lógica
Error de software	Sobreescritura de archivos Lectura inapropiada de la información
Error humano	Eliminación de archivos Destrucción de información
Malware	Daño en la integridad de la información
Desastres Naturales	Destrucción física de la unidad

Los daños lógicos son otras de las causas de la corrupción de datos, sobreescritura, borrado de archivos, etc. (García, García & Meana, 2010)

2.1.3. Herramientas forenses

Para Anandabrata, P., & Nasir, M, es importante implementar las técnicas forenses para la recuperación de datos, especialmente cuando falla o simplemente no obtiene el resultado deseado en la recuperación utilizando métodos tradicionales.
Las herramientas forenses que mejor se adapta en sistemas operativos Windows son las siguientes:

- PhotoRec / TestDisk: Soporte para recuperar archivos en diferentes medios de almacenamiento.
- Forensic Toolkit: Software forense dedicado a la recuperación de archivos.
- Scalpel: Es una aplicación de indexación con soporte para File Carving compatible en Linux y Windows.
- HxD: Permite visualizar datos de forma hexadecimal, incluyendo datos ocultos.

En contexto, esta técnica recupera datos relacionando con la estructura que lo compone además de su contenido, omite los metadatos que tiene el sistema de archivos. (Ninahualpa, Pérez, Yoo, Guarda, Diaz & Piccilli; 2018).

2.1.4. Unidades de almacenamiento

Alguno de los medios de almacenamiento más conocidos y usados en computadoras de escritorio y portátiles son los discos duros mecánicos y las unidades de estado sólido. Los discos duros mecánicos son medios de almacenamiento no volátiles es decir la información no se pierde una vez que esté apagado la computadora, y contiene toda la información que el usuario guarde. El dispositivo está compuesto por platos o discos unidos por un eje que gira a gran velocidad dentro de una caja metálica sellada además de un cabezal de escritura. Cuando el usuario guarda información en el disco duro, éste escribe en los platos una secuencia de unos y ceros a velocidades que se miden en microsegundos. (Espitia & Espitia, 2014)
Existe diferentes tipos de conectores como son:

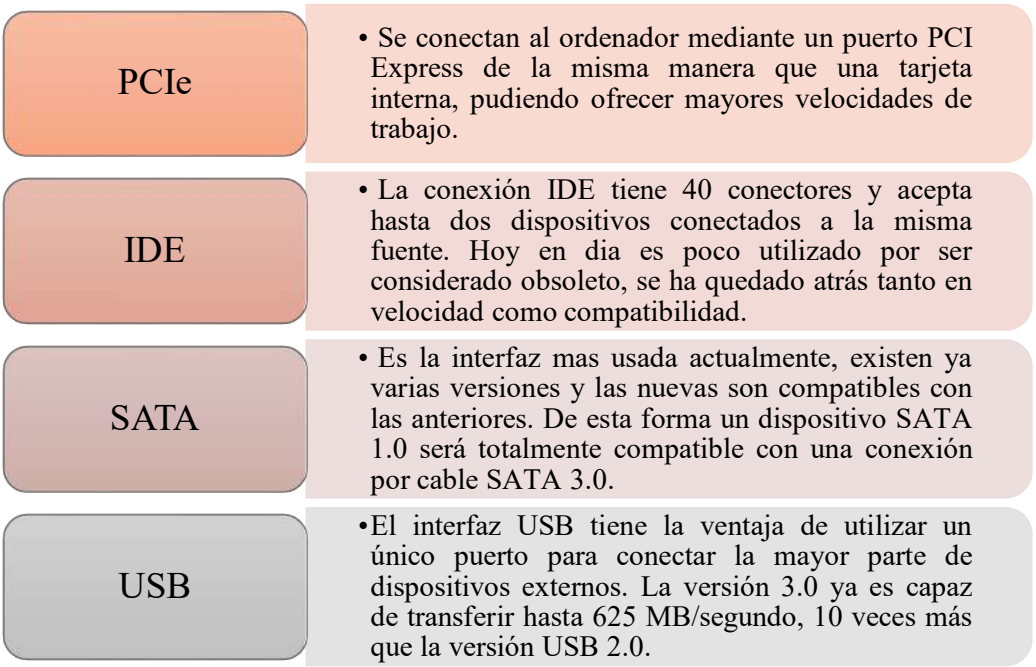


Figura 2: Tipo de interfaces de almacenamiento
Fuente: Elaboración propia

Con respecto a la capacidad de almacenamiento, en la actualidad se dispone de discos duros con capacidad que va desde gigas hasta teras, donde el costo final se ha vuelto económico con la llegada de las unidades sólidas. (Ruiz & Muñoz; 2014).

Las unidades de estado sólido son libres de partes mecánicas es decir no posee cabezal, disco magnético, imanes, entre otros; siendo reemplazados por memorias NAND no volátiles, posee un controlador de memoria cuya función es gestionar la velocidad de lectura y escritura de forma simultánea haciéndolo más robusto a fallos. (Ruiz & Muñoz; 2014).

Algunas de sus características que se diferencia a los discos duros tradicionales: (Ninagualpa, 2018)

- Interfaz del controlador: Permite que el dispositivo sea reconocido por el sistema operativo host.
- Interfaz NAND flash: Referente al diseño en la configuración de la memoria.
- Bus Host: Interfaz de los dispositivos SSS (Solid State Storage).
- Factor forma: Indica el tamaño y la proporción disponibles, como tarjetas o módulos de estado sólido.

- Memoria no volátil: Conectado directamente al bus de memoria en el sistema.
- Test SSS: Compara los SSS en busca de características en común.
- Tiempo de escritura y lectura baja.
- Bajo consumo de energía y temperatura.
- Libre de ruido por ausencia de partes mecánicas.
- Resistentes a golpes, caídas y vibraciones.

2.1.5. Análisis forense

Durante el análisis forense implica la utilización de técnicas y análisis especializados que ayuden a preservar, mantener, obtener toda la información válida para posteriormente ser presentado dentro de un proceso legal. Permite además brindar soporte al momento de presentarse un conflicto en relación con la seguridad y protección de los datos. (Pereyra & Eterovic, 2014).

Todo investigador debe conocer la importancia de seguir estándares para el buen manejo de la información, como es el caso de la norma ISO 27001 donde se debe aplicar los 3 pilares importantes durante el proceso como son: (Amutio, 2012)

- **Confidencialidad**: La información no se divulgará a personas o sistemas no autorizados. En esencia, solo la autorización correcta y verificada puede acceder a las propiedades de esta información.
- **Integridad**: La calidad de la información debe ser correcta y no modificada, los datos deben ser exactamente iguales a los datos generados sin necesidad de manipulación por parte de terceros. La integridad se pierde cuando la información presente alguna modificación; una práctica para preservar la integridad es usar una firma digital.
- **Disponibilidad**: La información no debe ser divulgada a personas o sistemas no autorizados, solo la autorización correcta y verificada puede acceder a las propiedades de esta información.

Tipo de análisis forense

Se puede clasificar según el tipo de análisis forense. Teniendo en cuenta este aspecto, se pueden determinar tres tipos de análisis:

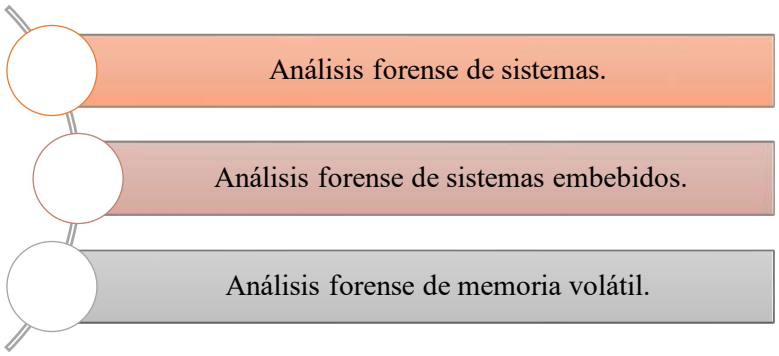


Figura 3: Análisis forense
Fuente: Elaboración propia

2.1.6. Guías de análisis forense digital

- **Guía de toma de evidencias en entornos Windows**. Guía desarrollada por Asier Martínez y publicada por el Instituto Nacional de Ciberseguridad (incibe) en 2014, proporciona información relacionada con el análisis forense digital en sistemas operativos Windows. Enfocado principalmente en la toma de evidencias, ofreciendo a detalle el proceso a seguir, explica en que consiste la toma de evidencias, cuál es su funcionalidad, que fases existen, las metodologías para llevarlo a cabo, entre otros. Este documento está dirigido a profesionales en el ámbito informático que no están familiarizados con el proceso de análisis forense digital. (Martínez, 2014)
- **Electronic Crime Scene Investigation: A Guide for First Responders**. Guía desarrollada por John Ashcroft y publicado por el Departamento de Justica de los Estados Unidos, destinada a ayudar a las fuerzas del orden público estatales y locales, responsables de preservar una escena electrónica del crimen y de reconocer, recopilar y salvaguardar evidencia digital. Mediante el uso de esta guía, brinda soporte a los investigadores en la toma de decisiones durante la escena del crimen electrónico, adquiriendo un mejor nivel de experiencia. Las

circunstancias de las escenas del crimen individuales y las leyes federales, estatales y locales pueden dictar acciones o un orden particular de acciones que no sean los descritos en esta guía. (Ashcroft, 2010)

- **Forensic Examination of Digital Evidence: A Guide for Law Enforcement**. Guía desarrollada por John Ashcroft y publicado por el Departamento de Justica de los Estados Unidos, ofrece recomendaciones sobre cómo las fuerzas del orden y los investigadores de la escena del crimen deben manejar la evidencia digital. Enfocado en la evidencia de teléfonos celulares o computadoras utilizando técnicas adecuadas para analizar los datos de manera forense. Esta guía se puede utilizar para los agentes del orden que no siguieron las recomendaciones en el manejo de este tipo de evidencia. (Ashcroft, 2010)

2.1.7. Estándares conocidos

- **RFC 3227**

Todo documento RFC reúne propuestas de diversos investigadores en diferentes temas, el objetivo es establecer un modelo a seguir en diferentes procesos como también la creación o la ejecución de algún tipo de protocolo.

El RFC 3227 tiene todas las directrices necesarias para la recolección de evidencias y su correcto almacenamiento, por lo que sirve como un modelo estándar para la obtención de información con seguridad.

Existe pasos a seguir durante la recolección de datos aplicando esta norma como indica la figura 4:

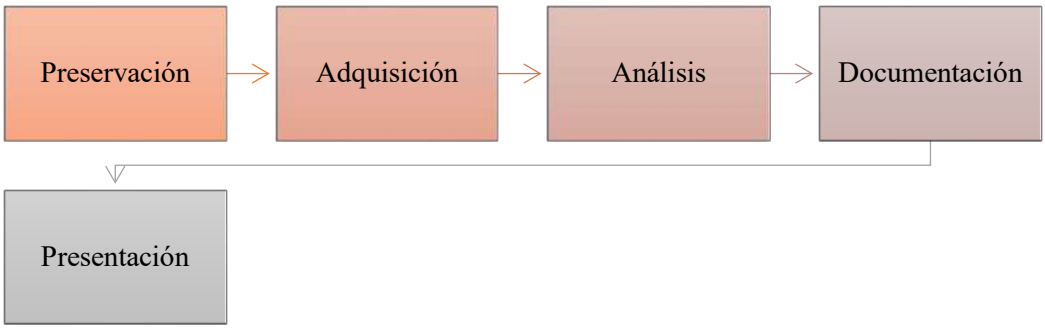


Figura 4: Proceso de análisis forense RFC 3227
Fuente: Elaboración propia.

Así que la RFC 3227 viene con información completa que ayuda durante todo el proceso, entrega información de diferentes apartados clave del análisis forense, por tal razón es considerado uno de los documentos referentes. (Martínez, 2014).

- **ISO/IEC 27037:2012**

Esta norma se compone de varias directrices enfocadas en el manejo de la evidencia digital, de igual manera brinda guías enfocadas a dispositivos móviles, computadoras, área de infraestructura de red entre otros. (Coronel, Areniz, Cuesta & Rico; 2020)
Las directrices indicadas por esta norma están englobadas en la figura 5:

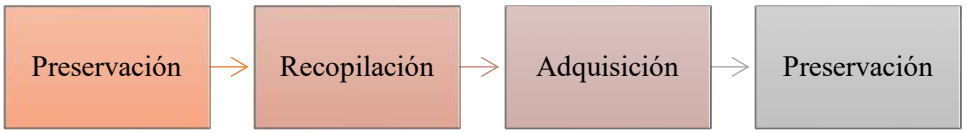


Figura 5: Proceso de análisis forense ISO/IEC 27037:2012
Fuente: Elaboración propia.

- **UNE 71505 y 71506**

Normas publicadas por la Asociación Española de Normalización y Certificación, el objetivo de estas normas es brindar respuestas a incidencias de seguridad ya sean estas en empresas y/o entidades. Usando estas normas se vuelve más completo y confiable las pruebas digitales, donde conlleva a la obtención de la causa del problema e identificar si es de carácter intencional o negligente. (Coronel, Areniz, Cuesta & Rico; 2020)
Las directrices indicadas por estas normas están englobadas en la figura 6:

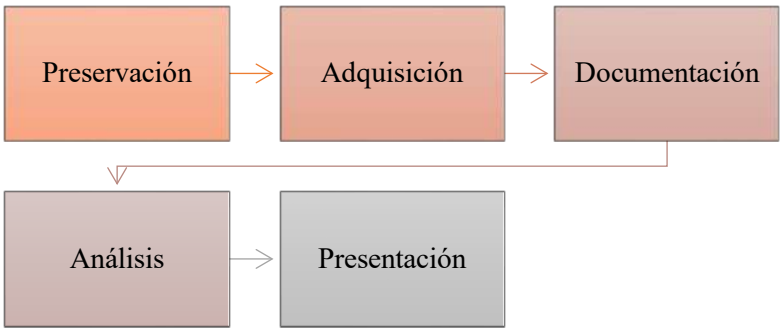


Figura 6: Proceso de análisis forense UNE 71505 y 71506
Fuente: Elaboración propia.

- **ISO/IEC 27042:2015**

La norma ISO/IEC 27042 publicada en 2015, ayuda con el análisis e interpretación de la evidencia digital, es decir, engloba la validez, reproducibilidad y repetibilidad. (Coronel, Areniz, Cuesta & Rico; 2020).

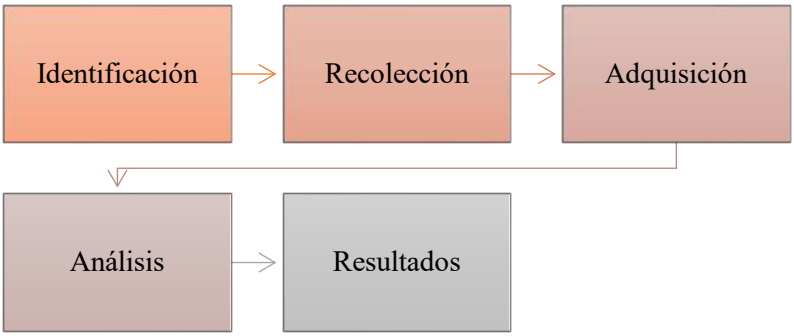


Figura 7: Proceso de análisis forense ISO/IEC 27042:2015
Fuente: Elaboración propia.

- **RFC 4810**

Estándar a seguir durante la preservación de la información del objeto y determinados archivos que se hayan creado en algún determinado tiempo, permite además comprobar la integridad del o los archivos desde cuando se creó hasta la presentación como evidencia. Define de igual manera el tipo de sistema de archivo que puede dar soporte y sus requisitos los cuales se deben cumplir. (Alamillo, 2016)

- **RFC 4998**

La RFC 4998 define como objetivo la preservación de la información, demuestra la existencia e integridad durante el periodo de intervención. Esta norma incluye los requisitos que debe tener un registro de evidencias e indica que sistemas de ficheros pueden dar soporte en varios escenarios, con la finalidad de brindar soporte al perito informático. (Alamillo, 2016).

- **RFC 6283**

La norma RFC 6283 establece directrices para demostrar la existencia, integridad y validez de información durante periodos indeterminados de tiempo. Define la sintaxis en lenguaje extensible de marcas XML y pasos que deben seguirse en la creación de evidencias íntegras de información de largo periodo al objeto. (Alamillo, 2016).

- **ISO/IEC 27040:2015**

Esta norma ayuda con una orientación técnica detallada sobre cómo definir un nivel adecuado de mitigación de riesgos, implementando un enfoque probado y coherente para la planificación, diseño, documentación e implementación de la seguridad del almacenamiento de datos. Durante la seguridad de almacenamiento, se aplica a la protección de la información del lugar donde esta almacenado y durante la transferencia de dicha información a través de los vínculos de comunicación asociados con el almacenamiento. (ISO, 2015).

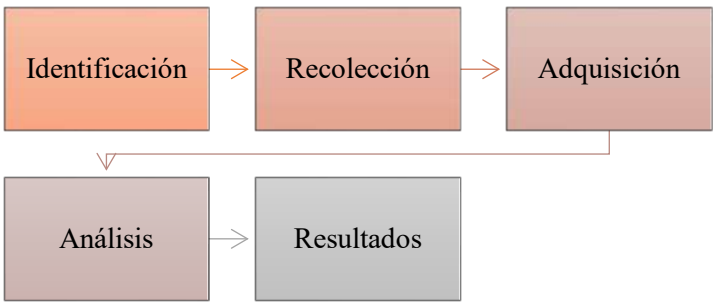


Figura 8: Proceso de análisis forense ISO/IEC 27040:2015
Fuente: Elaboración propia.

2.1.8. Recolección de evidencias

Debe ser lo más detallado posible para garantizar que no haya información ambigua y minimizando la toma de decisiones. La evidencia digital es sumamente frágil y puede ser alterada, dañada o destruida por una mala manipulación o inspección incorrecta, por lo que se deben tomar precauciones especiales para conservar dicha evidencia, de lo contrario podría inutilizarlo o sacar conclusiones incorrectas. Como todas las demás

pruebas, deben manejarse con cuidado y procesarse de manera que preserve su valor probatorio, lo que implica no solo la integridad física del artículo o equipo, sino también los datos electrónicos que contiene. Por lo tanto, ciertos tipos de pruebas informáticas requieren una recogida, embalaje y transporte especiales. Se debe tener en cuenta la protección de los datos que puedan ser susceptibles de daño o alteración por campos electromagnéticos (como los generados por electricidad estática, imanes, transmisores de radio y otros dispositivos).

CAPÍTULO III

3. METODOLOGÍA

Para la presente investigación primero se realizó una Revisión bibliográfica, sobre el método File Carving y sobre los estándares mundialmente aceptados para la manipulación y recopilación de evidencias digitales (UNE 71505:2013, UNE 71506:2013, RFC 3227, RFC 4810, ISO/IEC 27037:2012, ISO/IEC 27040:2015, ISO/IEC 27042:2015, RFC 4998 y RFC 6283); posteriormente se realizó un análisis de la normativa ecuatoriana que permitió definir los parámetros legales en función del tema de estudio y de la confiabilidad del proceso.

A través de la revisión bibliográfica se organiza y analiza la información para simplificar la creación de una guía de recuperación de datos utilizando la técnica forense, para finalmente validarla utilizando la técnica de validación de juicio de expertos.

3.1. Hipótesis

La utilización de una guía de recuperación de datos utilizando la técnica forense File Carving permitirá una mejor confiabilidad en el proceso de recuperación de la información.

3.2. Identificación de variables

3.2.1. Variable Independiente

- Utilización de una guía de recuperación de datos utilizando la técnica forense File Carving.

3.2.2. Variable Dependiente

- Confiabilidad en el proceso de recuperación de la información.

3.3. Tipo de Estudio

Para llevar a cabo la creación de la guía de recuperación de datos utilizando la técnica forense File Carving para ordenadores Windows, la investigación se basó en un enfoque

cualitativo, debido a que pretende partir del análisis de las actividades relacionadas con la recuperación de datos mediante técnicas forenses. De acuerdo con este enfoque, se utilizó diversos tipos de investigación como las mencionadas a continuación:

3.3.1. Según el objeto de estudio

- **Investigación aplicada**: Partiendo de tres guías de análisis forense globalmente utilizadas, se realizó un estudio comparativo y una evaluación basada en 10 parámetros de estudio, permitiendo generar una nueva propuesta de guía adaptada a la normativa vigente y leyes del Ecuador. Posterior a esto, se generó un caso de estudio con el objetivo de aplicar la nueva guía y así observar el grado de recuperación de la información y el tiempo que toma hacerlo.

3.3.2. Según la fuente de investigación.

- **Investigación Bibliográfica**: Se recolectó información de diversas fuentes, guías relacionadas con el análisis forense y la normativa vigente en el Ecuador. Para lo cual se revisó diversos artículos científicos, libros digitales entre otros, específicamente se enfocó en las guías seleccionadas, el Código Orgánico Integral Penal vigente del Ecuador, norma ISO 27001 y el Manual de Manejo de Evidencias Digitales y Entornos Informáticos.

3.3.3. Según el nivel de conocimientos

- **Investigación Descriptiva:** Durante el desarrollo de la guía se implementó diferentes apartados, mismos que contienen procedimientos de forma ordenada basadas en las guías seleccionadas previamente. Dichos apartados son: Dispositivos electrónicos, Introducción al análisis forense, Directrices para la recolección de datos, Procedimiento de recolección de datos, Empaquetado, almacenamiento y transporte de la información, Análisis de evidencias, Recuperación de datos: Técnica forense, Documentación y reportes.

Dentro del apartado “Recuperación de datos: Técnica forense” se mencionó algunas herramientas forenses disponibles de forma gratuita para este fin como es PhotoRec, Autopsy, Scalpel y HxD, mismas que actúan como recomendación para el proceso de recuperación de datos.

3.3.4. Técnica de investigación

- **Técnica documental**: Se recopiló la información necesaria por medio de las guías seleccionadas que son: “Guía de toma de evidencias en entornos Windows”, la misma que detalla el análisis forense digital; “Electronic Crime Scene Investigation: A Guide for First Responders”, en la que se recopila información referente al peritaje informático dentro del entorno de la criminalística; “Forensic Examination of Digital Evidence: A Guide for Law Enforcement”, realiza un análisis de la evidencia digital con un enfoque legal. Es por lo cual, a través de la recopilación de esta información documental se obtuvo una guía aplicable a la legislación ecuatoriana.
- **La Encuesta:** Se desarrolló dos encuestas, la primera consta de diez preguntas formuladas en concordancia con la normativa vigente, la misma fue dirigida a peritos informáticos, con el objetivo evaluar la guía propuesta. (**Anexo 2**) La segunda encuesta consta de quince preguntas dividas en tres segmentos; el primer segmento está relacionado con el grado de recuperación de la información, el segundo segmento está relacionado con el tiempo de recuperación de la información, y finalmente el tercer segmento engloba preguntas de ámbito general; mediante la implementación de esta encuesta ayudó a conocer si la guía adaptada cumple con su objetivo. (**Anexo 3**)

  Las dos encuestas propuestas fueron elaboradas en base al método Delphi, las mismas que han sido propuestas al panel de expertos (peritos informáticos) con el objetivo de obtener un resultado viable deseado.

3.4. Según el método a utilizar

- **Método Deductivo:** A partir del análisis de tres guías estandarizadas a nivel mundial, se logró obtener como resultado la presente "Guía de recuperación de datos utilizando la técnica forense File Carving en ordenadores Windows", adaptada a la normativa vigente del Ecuador.

3.5. Operacionalización de variables

Tabla 2: *Operacionalización de variables*
Fuente: Elaboración propia

Objetivos	Hipótesis	Variables	Definición Conceptual	Indicadores
Objetivo General: Crear una guía de recuperación de datos utilizando la técnica forense File Carving que permita una mejor confiabilidad en el proceso de recuperación de la información **Objetivos Específicos:** • Investigar y analizar el método File Carving y sus herramientas para el proceso de recuperación de datos en ordenadores Windows. • Desarrollar la guía de recuperación de datos aplicando la técnica forense File Carving basado en la normativa nacional e internacional. • Validar la guía de recuperación de datos en ordenadores Windows.	La creación de una guía de recuperación de datos utilizando la técnica forense File Carving permitirá una mejor confiabilidad en el proceso de recuperación de la información.	**Independiente:** Creación de una guía de recuperación de datos utilizando la técnica forense File Carving	Guía diseñada para ayudar a los usuarios con directrices y procedimientos necesarios para la recuperación de los datos mediante el uso de software forense, utilizando la técnica File Carving.	• Preservación • Adquisición • Análisis • Documentación • Presentación
		Dependiente: Confiabilidad en el proceso de recuperación de la información.	La recuperación de datos es el proceso de restablecer datos borrados de diversas formas como puede ser error humano, daño físico de la unidad de almacenamiento, falla del sistema, etc.	• Juicio de expertos • Porcentaje de recuperación • Tiempo de recuperación

3.6. Procesamiento y Análisis

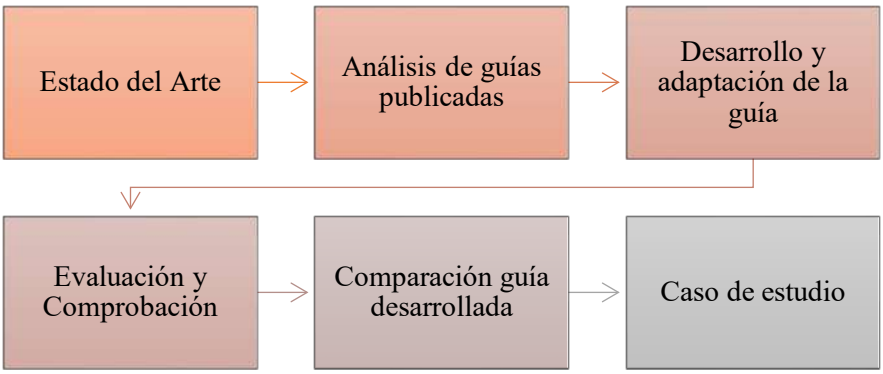


Figura 9: Procedimiento y Análisis
Fuente: Elaboración propia

Durante estado del arte, contiene conceptos de investigaciones realizadas en artículos científicos, libros digitales, uno de ellos es: "Restauración de datos y el File Carving". En el análisis de guías publicadas previamente se escogió las siguientes: "Guía de toma de evidencias en entornos Windows", "Electronic Crime Scene Investigation: A Guide for First Responders", "Forensic Examination of Digital Evidence: A Guide for Law Enforcement", donde se analizó cada una de ellas y posterior a esto, se comparó con la normativa ecuatoriana vigente, la norma ISO 27001; con el objetivo de obtener su porcentaje de cumplimiento. Una vez realizado este proceso, se desarrolló la guía basado en las guías anteriormente mencionadas y adaptado a la normativa, esta se encuentra divido en diferentes apartados. Para la evaluación de la guía, se aplicó una encuesta dirigida a peritos informáticos donde se califica cada apartado cuya calificación va desde el 1 al 3. (**Anexo 2**) Finalizado la evaluación, se extrajo los resultados haciendo un promedio total por cada pregunta donde se obtuvo la suma y el porcentaje final. Con este valor, se comparó con el valor obtenido previamente de las guías seleccionadas y se obtuvo un valor superior de confiabilidad. Para observar si la guía cumple con su objetivo, se desarrolló un caso de estudio ficticio que permita aplicar el uso de esta guía y con la aplicación de una encuesta dirigido a peritos, obtener el porcentaje de archivos recuperados y el tiempo tomado durante este proceso. (**Anexo 3 y 4**)

3.7. Desarrollo de la guía

Fase I – Investigación: Dentro de la comparación de las guías escogidas, se identificó que apartados son relevantes para la implementación en la nueva guía y cuales no constan para adaptarlo con las normas ecuatorianas vigentes.

Fase II – Diseño: La guía desarrollada se encuentra divida en los siguientes apartados basada en el contenido de las guías seleccionadas.

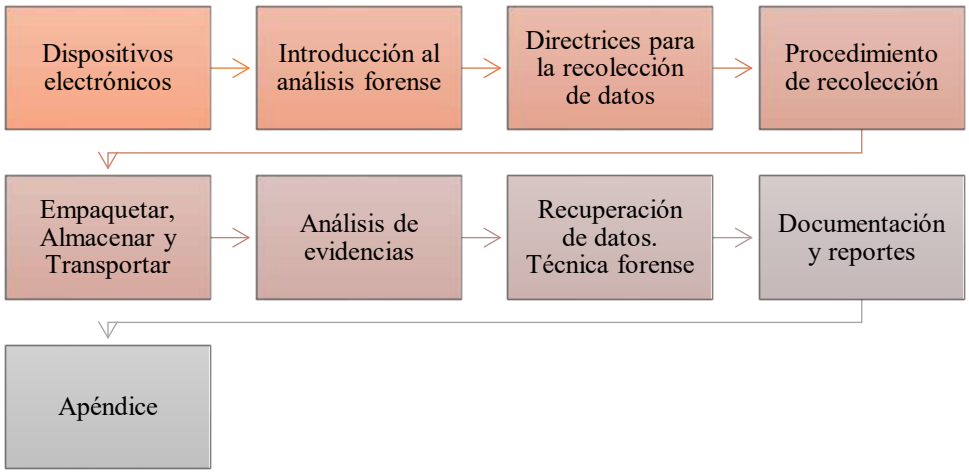


Figura 10: Apartados de la guía
Fuente: Elaboración propia

Fase III – Desarrollo: Se procedió con el desarrollo del contenido de cada apartado, utilizando como base la información obtenida de las guías comparadas, el estado del arte, la norma ISO 27001, Manual de Manejo de Evidencias Digitales y Entornos Informáticos.

Fase IV – Evaluación: Durante la evaluación, se aplicó la encuesta a trece peritos informáticos legamente autorizados, cada pregunta de la encuesta tiene relación con la normativa ecuatoriana (**Tabla 3**). Durante la verificación, se generó un caso de estudio ficticio con el objetivo de aplicar la guía adaptada, además de aplicar una encuesta a diecisiete peritos informáticos legamente autorizados para conocer el porcentaje de

archivos recuperados y el tiempo que tomó el proceso. La calificación de estas encuestas va desde el 1 al 3 donde 1= No Cumple, 2= Cumple Parcialmente, 3= Cumple Totalmente.

CAPITULO IV

4. RESULTADOS Y DISCUSION

En el siguiente capítulo se procede a indicar, en primer lugar, los resultados obtenidos durante la comparación de tres guías de recuperación de datos mundialmente aceptadas, las cuales son "Guía de toma de evidencias en entornos Windows" (Martínez, 2014), "Electronic Crime Scene Investigation" (Ashcroft, 2001) y "Forensic Examination of Digital Evidence (Ashcroft, 2004) para obtener el porcentaje de cumplimiento con la normativa ecuatoriana vigente. (**Anexo 5**)

Se desarrolló un guía de recuperación de datos utilizando la técnica forense File Carving para ordenadores con sistema operativo Windows, dirigida a peritos informáticos calificados por el Consejo de la Judicatura del Ecuador. Una vez finalizado, se procede con la evaluación y verificación, mediante dos encuestas dirigidas a peritos informáticos legalmente autorizados **(Anexo 2 y 3)**; cada pregunta que compone la encuesta de evaluación están planteadas de acuerdo con diversas normas establecidas en el artículo 500 del COIP, la norma ISO 27001 y el Manual de Manejo de Evidencias Digitales y Entornos Informáticos; para la segunda encuesta, cada pregunta están planteadas de acuerdo con el porcentaje de recuperación de la información y el tiempo que toma recuperar.

Finalmente, con el resultado de la encuesta de evaluación, se compara con los datos obtenidos de las tres guías base de la investigación, teniendo como resultado que la guía propuesta mejora la confiablidad al momento de realizar un análisis forense aplicado a equipos con sistema operativo Windows. Con el resultado de la encuesta de verificación, se obtiene el porcentaje de archivos recuperados y el tiempo que toma hacerlo con la aplicación de la guía.

4.1. Resultados

4.1.1. Resultado 1: Comparación entre guías.

Tabla 3*: Comparación guías mundialmente conocidas.*
Fuente: Elaboración propia

	REQUERIMIENTO BASE LEGAL	GUÍA 1 1-3	GUÍA 2 1-3	GUÍA 3 1-3
1	Durante la investigación, se debe conservar la autenticidad e integridad de los medios probatorios.	3	3	3
2	En todos los casos, existirá una cadena de custodia debidamente asegurada que demuestre que los medios no han sido modificados durante la pericia.	3	2	3
3	Deberá establecerse por escrito los pasos dados en el procedimiento pericial	2	2	3
4	El análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de técnicas digitales forenses.	3	3	3
5	Cuando el contenido digital se encuentre almacenado en sistemas y memorias volátiles o equipos tecnológicos que formen parte de la infraestructura critica del sector público o privado, se realizará su recolección, en el lugar y en tiempo real, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.	2	3	3
6	Cuando el contenido digital se encuentre almacenado en medios no volátiles, se realizará su recolección, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.	3	2	3
7	Cuando se recolecte cualquier medio físico que almacene, procese o transmita contenido digital durante una investigación, registro o allanamiento, se deberá identificar e inventariar cada objeto individualmente, fijará su ubicación física con fotografías y un plano del lugar, se protegerá a través de técnicas digitales forenses y se trasladará mediante cadena de custodia a un centro de acopio especializado para este efecto.	2	3	2
8	Confidencialidad: Cuando una o más personas ganan acceso no autorizado a la información.	3	1	1
9	Integridad: La información podrá ser modificada solamente por aquellos con derecho a cambiarla.	3	3	3
10	Disponibilidad. La información deberá estar disponible en el momento en que los usuarios autorizados requieran acceder a ella.	2	2	2
	TOTAL	26	24	26
	Porcentaje de cumplimiento	**86.7%**	**80%**	**86.7%**

Análisis: Se comparó tres guías mundialmente conocidas con la base legal vigente y así observar el porcentaje de cumplimiento. Donde la guía 1 da como resultado un 86.7% de cumplimiento, la guía 2 un 80% y finalmente la guía 3 un 86.7%.

4.1.2. Resultado 2: Desarrollo de la guía.

Análisis: Una vez finalizado la comparación inicial y observado el porcentaje de cumplimiento, se desarrolló la guía adaptada a los parámetros legales, basado en la información contenida en las 3 guías seleccionadas y adaptando de mejor manera a la normativa legal vigente. (**Anexo "1"**)

4.1.3. Resultado 3: Evaluación de la guía.

Pregunta 1: ¿La guía indica como preservar la autenticidad e integridad de los medios probatorios?

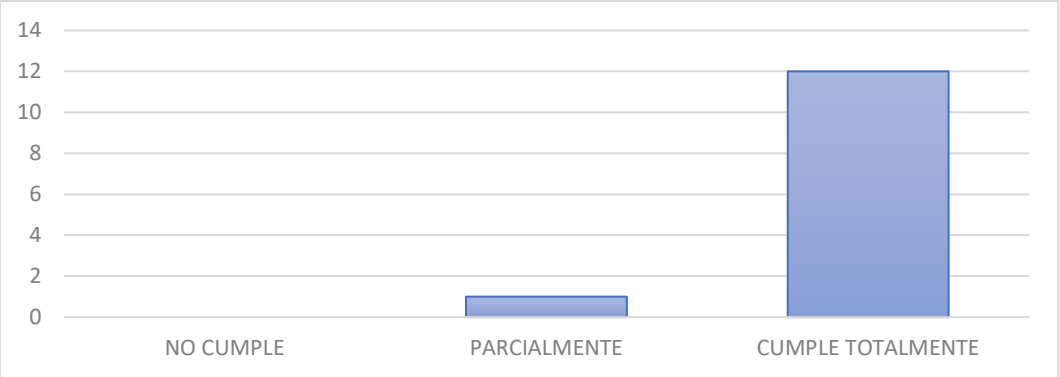


Figura 11: Evaluación - Pregunta 1
Fuente: Elaboración propia.

Análisis: La figura 7 indica que, de un total de 13 encuestados que respondieron la encuesta, 12 están totalmente de acuerdo con el cumplimento de la preservación, la autenticidad e integridad de los medios probatorios; mientras que un solo encuestado manifiesta que se cumple de forma parcial.

Pregunta 2: ¿Explica la guía la cadena de custodia que seguirán los medios para garantizar que no se han modificado durante la pericia?

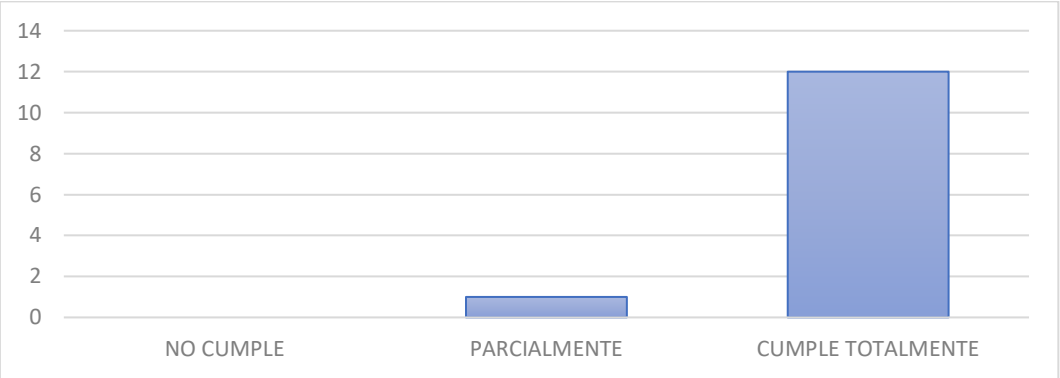


Figura 12: Evaluación - Pregunta 2
Fuente: Elaboración propia.

Análisis: La figura 8 indica que, de un total de 13 encuestados, 12 están totalmente de acuerdo con el cumplimento de la implementación de una cadena de custodia que

seguirán los medios para garantizar que no se han modificado durante la pericia; mientras que un solo encuestado manifiesta que cumple de forma parcial.

Pregunta 3: ¿La guía indica los pasos a seguir durante el procedimiento pericial?

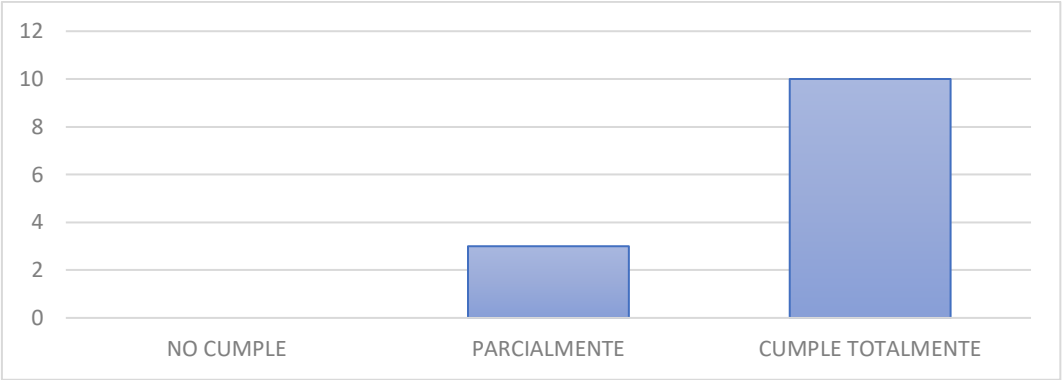


Figura 13: Evaluación - Pregunta 3
Fuente: Elaboración propia.

Análisis: La figura 9 indica que, de un total de 13 encuestados, 10 están totalmente de acuerdo con el cumplimento de los pasos a seguir durante el procedimiento pericial; mientras que 3 encuestados manifiestan que cumple de forma parcial.

Pregunta 4: ¿Enuncia la guía las técnicas forenses que se emplearán para el análisis, valoración, recuperación y preservación de la información digital almacenada en dispositivos o sistemas informáticos?

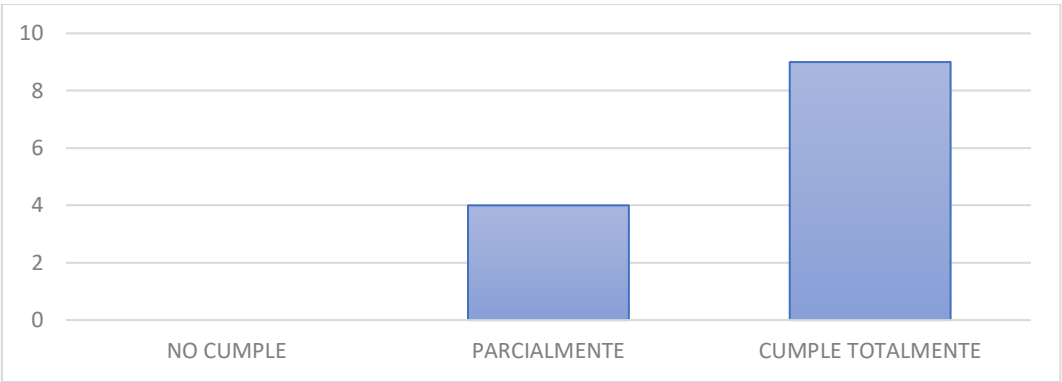


Figura 14: Evaluación - Pregunta 4
Fuente: Elaboración propia.

Análisis: La figura 10 indica que, de un total de 13 encuestados, 9 están totalmente de acuerdo con el cumplimento de las técnicas forenses que se emplearán para el

análisis, valoración, recuperación y preservación de la información digital almacenada en dispositivos o sistemas informáticos; mientras que 4 encuestados manifiestan que cumple de forma parcial.

Pregunta 5: ¿Indica la guía los pasos a seguir durante la recolección de datos en tiempo real con técnicas digitales forenses, de equipos tecnológicos que formen parte de la infraestructura crítica del sector público o privado y explica la cadena de custodia?

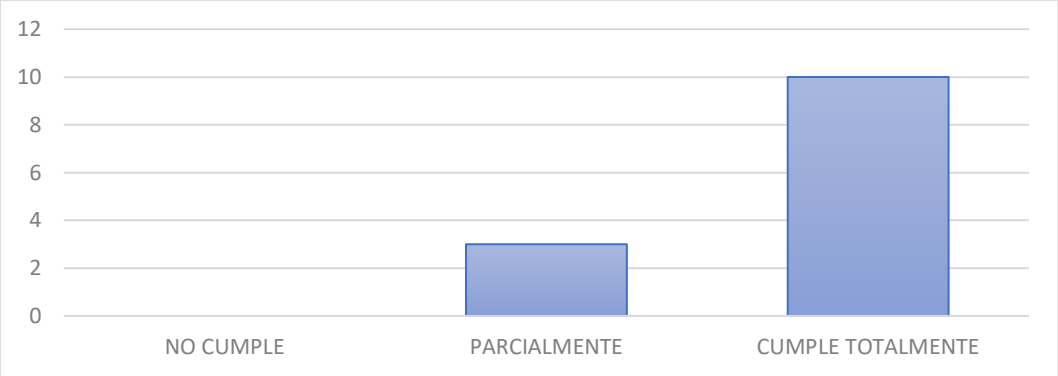


Figura 15: Evaluación - Pregunta 5
Fuente: Elaboración propia.

Análisis: La figura 11 indica que, de un total de 13 encuestados, 10 están totalmente de acuerdo con el cumplimento de los pasos a seguir durante la recolección de datos en tiempo real con técnicas digitales forenses, de equipos tecnológicos que formen parte de la infraestructura crítica del sector público o privado y explica la cadena de custodia; mientras que 3 encuestados manifiestan que cumple de forma parcial.

Pregunta 6: ¿Indica la guía como preservar la integridad del contenido digital cuando este se encuentre almacenado en medios no volátiles?

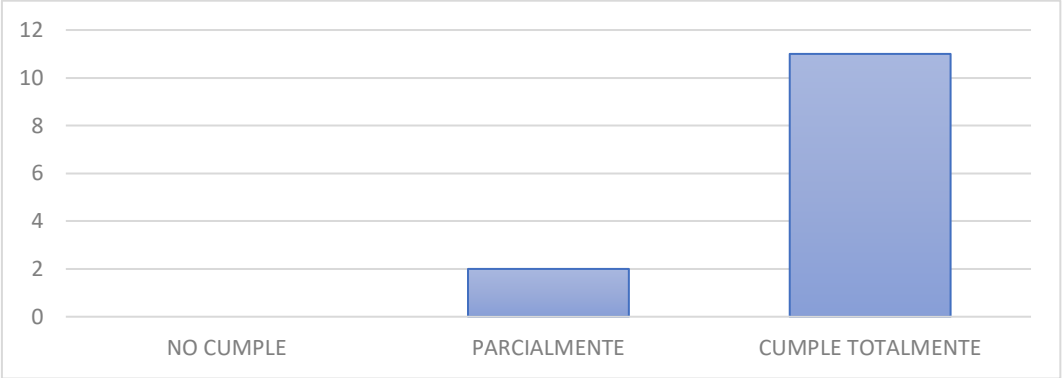


Figura 16: Evaluación - Pregunta 6
Fuente: Elaboración propia.

Análisis: La figura 12 indica que, de un total de 13 encuestados, 11 están totalmente de acuerdo con el cumplimento con la preservación de la integridad en el contenido digital cuando este se encuentre almacenado en medios no volátiles; mientras que 2 encuestados manifiestan que cumple de forma parcial.

Pregunta 7: ¿Ayuda la guía a identificar e inventariar cada objeto individualmente durante una investigación, cumpliendo los requerimientos estipulados en el Art. 500 del COIP?

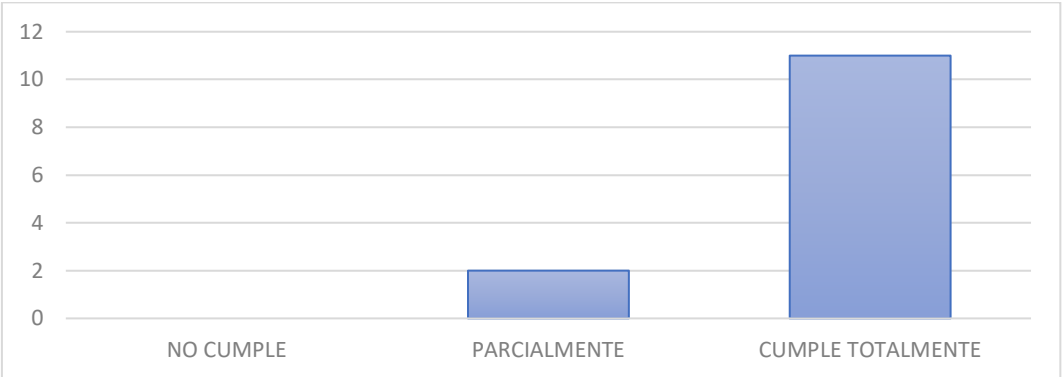


Figura 17: Evaluación - Pregunta 7
Fuente: Elaboración propia.

Análisis: La figura 13 indica que, de un total de 13 encuestados, 11 están totalmente de acuerdo con el cumplimento en la identificación e inventariado de cada objeto de forma individual durante una investigación, cumpliendo los requerimientos estipulados en el Art. 500 del COIP; mientras que 2 encuestados manifiestan que cumple de forma parcial.

Pregunta 8: ¿La guía menciona la importancia de la confidencialidad durante la obtención de la información?

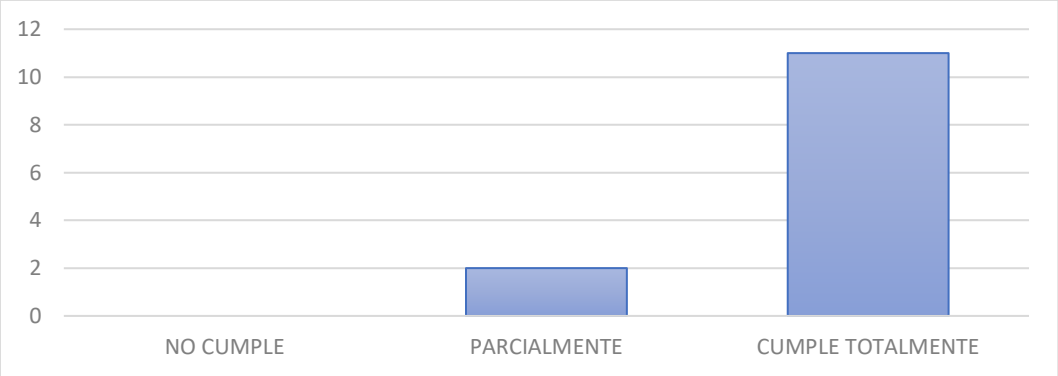


Figura 18: Evaluación - Pregunta 8
Fuente: Elaboración propia.

Análisis: La figura 14 indica que, de un total de 13 encuestados, 11 están totalmente de acuerdo con el cumplimento de la importancia de la confidencialidad durante la obtención de la información; mientras que 2 encuestados manifiestan que cumple de forma parcial.

Pregunta 9: ¿La guía menciona la importancia de la integridad de la información obtenida y aclara quienes tienen derecho a cambiarla si es necesario?

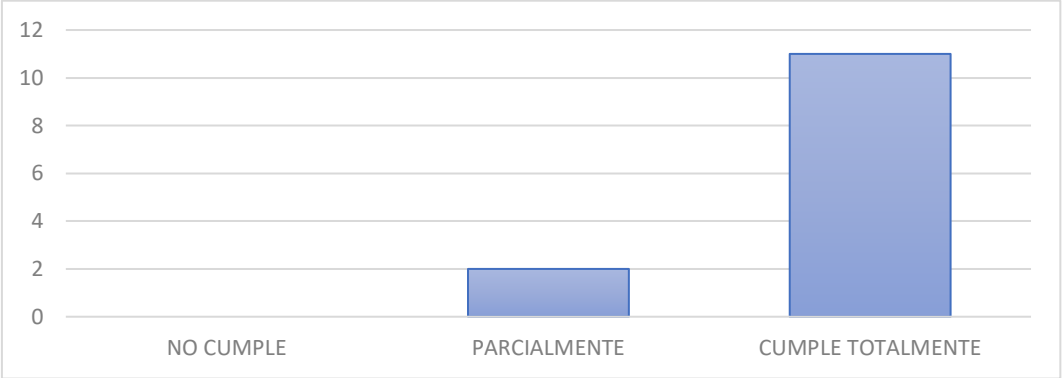


Figura 19: Evaluación - Pregunta 9
Fuente: Elaboración propia.

Análisis: La figura 15 indica que, de un total de 13 encuestados, 11 están totalmente de acuerdo con el cumplimento de la importancia de la integridad de la información obtenida y aclara quienes tienen derecho a cambiarla si es necesario; mientras que 2 encuestados manifiestan que cumple de forma parcial.

Pregunta 10: ¿Aclara la guía la importancia de la disponibilidad de la información obtenida durante un proceso pericial, para usuarios con acceso autorizado?

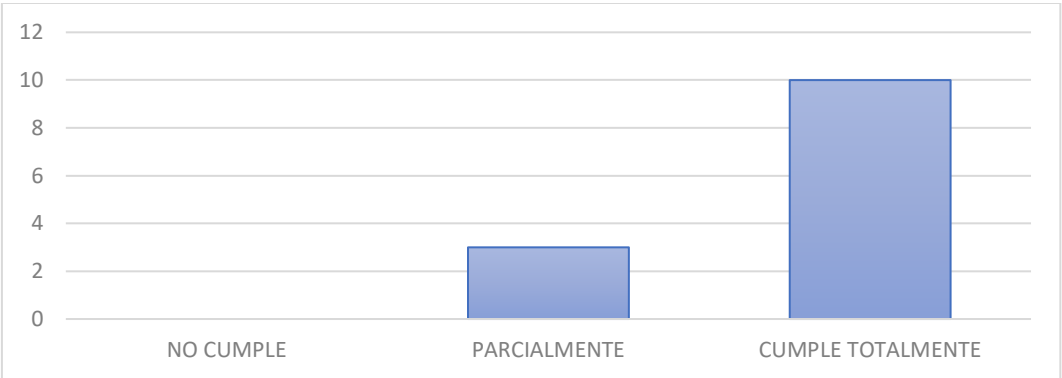


Figura 20: Evaluación - Pregunta 10
Fuente: Elaboración propia.

Análisis: La figura 16 indica que, de un total de 13 encuestados, 10 están totalmente de acuerdo con el cumplimento de la importancia de la disponibilidad de la

información obtenida durante un proceso pericial, para usuarios con acceso autorizado; mientras que 3 encuestados manifiestan que cumple de forma parcial.

Resumen global de los resultados

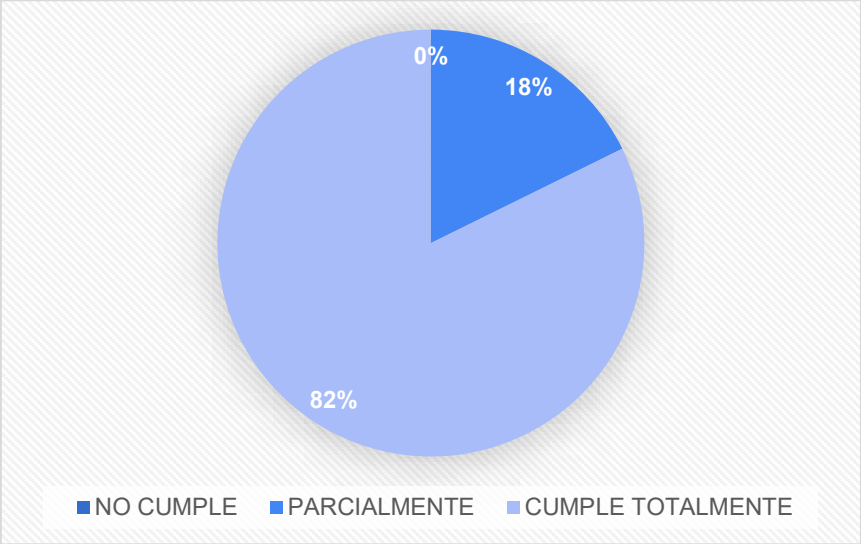


Figura 21: Resumen global
Fuente: Elaboración propia

En resumen, la figura 17 muestra de forma general los resultados obtenidos de la encuesta aplicada a peritos informáticos calificados, donde refleja porcentajes favorables, obteniendo un 82% Cumple Totalmente, un 18% Cumple Parcialmente y 0% No Cumple.

Con estos resultados se puede confirmar que la "Guía de recuperación de datos utilizando la técnica forense File Carving en ordenadores Windows" cumple con un porcentaje de confiabilidad alto con relación a la guías seleccionadas, y ayuda en la recuperación de información a peritos informáticos, adquiriendo mejores habilidades en el proceso y toma de decisiones.

4.1.4. Resultado 4: Comparativa y análisis final.

Tabla 4: *Comparación guía final*
Fuente: Elaboración propia

	REQUERIMIENTO BASE LEGAL	GUÍA 1 1-3	GUÍA 2 1-3	GUÍA 3 1-3	GUÍA TESIS 1-3
1	Durante la investigación, se debe conservar la autenticidad e integridad de los medios probatorios.	3	3	3	2,92
2	En todos los casos, existirá una cadena de custodia debidamente asegurada que demuestre que los medios no han sido modificados durante la pericia.	3	2	3	2,92
3	Deberá establecerse por escrito los pasos dados en el procedimiento pericial	2	2	3	2,77
4	El análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de técnicas digitales forenses.	3	3	3	2,69
5	Cuando el contenido digital se encuentre almacenado en sistemas y memorias volátiles o equipos tecnológicos que formen parte de la infraestructura critica del sector público o privado, se realizará su recolección, en el lugar y en tiempo real, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.	2	3	3	2,77
6	Cuando el contenido digital se encuentre almacenado en medios no volátiles, se realizará su recolección, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.	3	2	3	2,85
7	Cuando se recolecte cualquier medio físico que almacene, procese o transmita contenido digital durante una investigación, registro o allanamiento, se deberá identificar e inventariar cada objeto individualmente, fijará su ubicación física con fotografías y un plano del lugar, se protegerá a través de técnicas digitales forenses y se trasladará mediante cadena de custodia a un centro de acopio especializado para este efecto.	2	3	2	2,85
8	Confidencialidad: Cuando una o más personas ganan acceso no autorizado a la información.	3	1	1	2,85
9	Integridad: La información podrá ser modificada solamente por aquellos con derecho a cambiarla.	3	3	3	2,85
10	Disponibilidad. La información deberá estar disponible en el momento en que los usuarios autorizados requieran acceder a ella.	2	2	2	2,77
	TOTAL	26	24	26	28,23
	Porcentaje de cumplimiento	**86.7%**	**80%**	**86.7%**	**93.3%**

Análisis: Previo a la comparación inicial, se volvió a comparar esta vez con la nueva guía y así observar si dicha guía supera o no el porcentaje inicial que es 86.7%. Finalmente, la guía desarrollada dio como resultado un 93.3% superando al porcentaje obtenido previamente, basado en el resultado de 13 peritos informáticos encuestados.

4.1.5. Resultado 5: Verificación de la guía

Pregunta 1: ¿Considera que la guía menciona buenas prácticas a seguir con relación a la seguridad de la información?

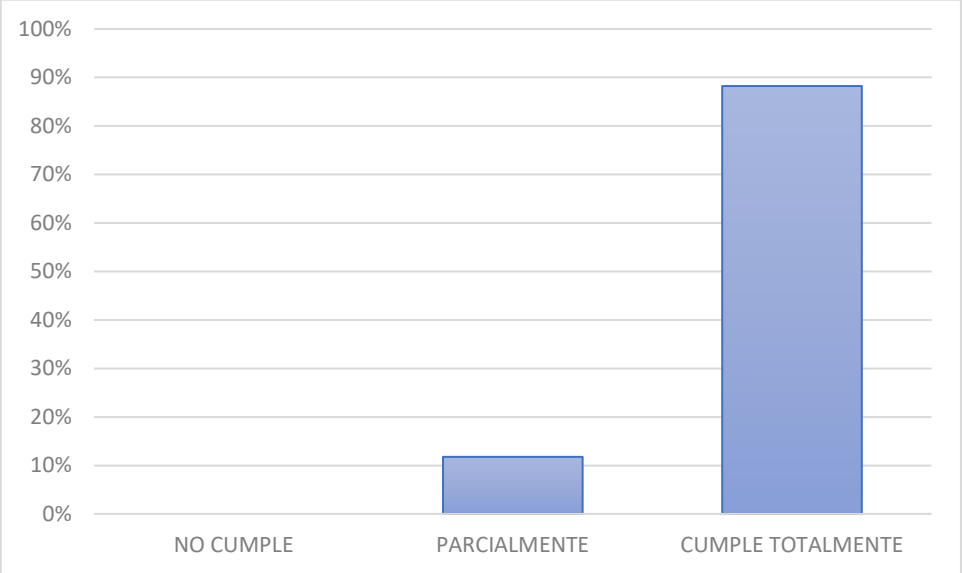


Figura 22: Verificación – Pregunta 1
Fuente: Elaboración propia

Análisis: De un total de diecisiete peritos encuestados, un 88% consideran que la guía menciona buenas prácticas a seguir con relación a la seguridad de la información; mientras que un 12% consideran que cumple de forma parcial.

Pregunta 2: ¿Considera que esta guía menciona directrices a seguir durante la integridad de datos, necesarios para el caso de estudio?

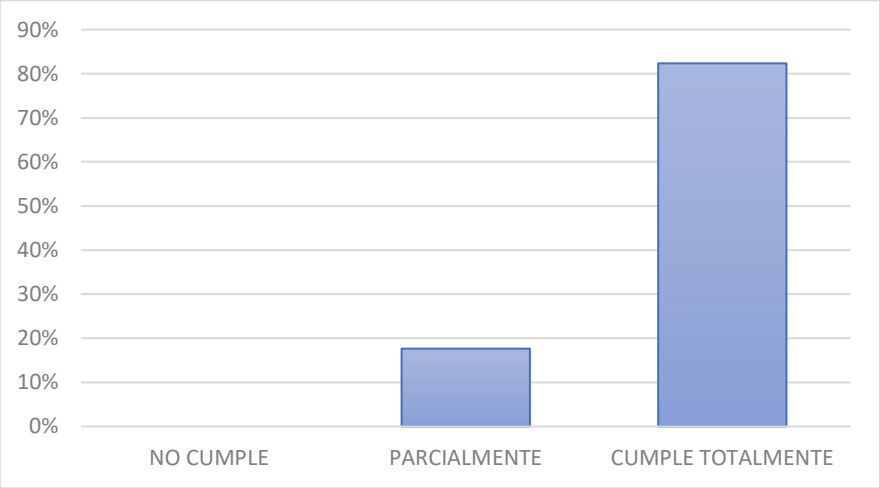


Figura 23: Verificación – Pregunta 2
Fuente: Elaboración propia

Análisis: De un total de diecisiete peritos encuestados, un 82% consideran que la guía menciona directrices a seguir durante la integridad de datos, necesarios para el caso de estudio; mientras que un 18% consideran que cumple de forma parcial.

Pregunta 3: ¿Cree que esta guía influye de manera positiva en la recuperación de archivos de manera eficaz ayudando al caso de estudio?

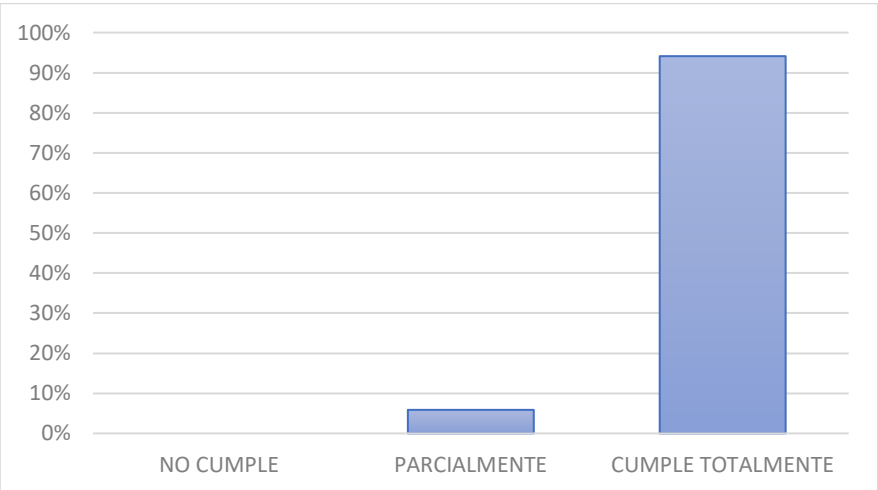


Figura 24: Verificación – Pregunta 3
Fuente: Elaboración propia

Análisis: De un total de diecisiete peritos encuestados, un 94% consideran que la guía influye de manera positiva en la recuperación de archivos de manera eficaz ayudando al caso de estudio; mientras que un 6% consideran que cumple de forma parcial.

Pregunta 4: ¿Cree que esta guía menciona sobre la confiabilidad de la información y su aplicación para el caso de estudio?

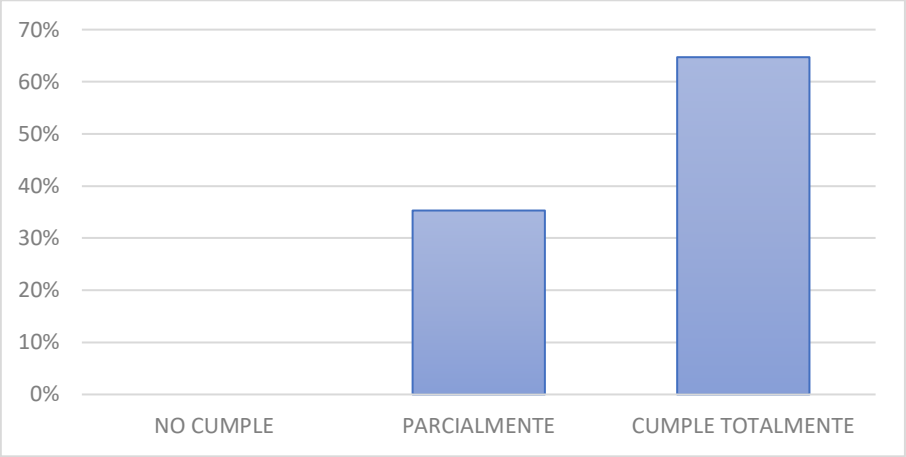


Figura 25: Verificación – Pregunta 4
Fuente: Elaboración propia

Análisis: De un total de diecisiete peritos encuestados, un 65% consideran que la guía menciona sobre la confiabilidad de la información y su aplicación para el caso de estudio; mientras que un 35% consideran que cumple de forma parcial.

Pregunta 5: ¿Considera que la recuperación de datos aplicando técnicas forenses tiene un grado aceptable en la obtención de la información perdida?

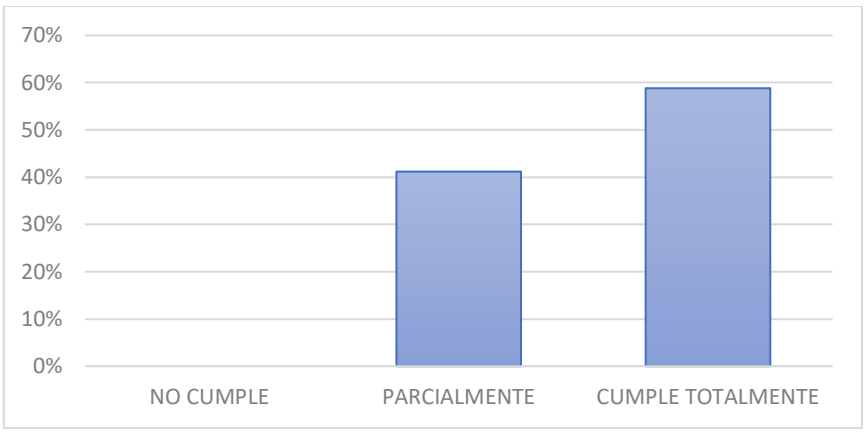


Figura 26: Verificación – Pregunta 5
Fuente: Elaboración propia

Análisis: De un total de diecisiete peritos encuestados, un 59% consideran que la recuperación de datos aplicando técnicas forenses tiene un grado aceptable en la obtención de la información perdida; mientras que un 41% lo consideran de forma parcial.

Pregunta 6: ¿Considera que la obtención de datos es de relevancia para una investigación y así tener un informe forense estructurado?

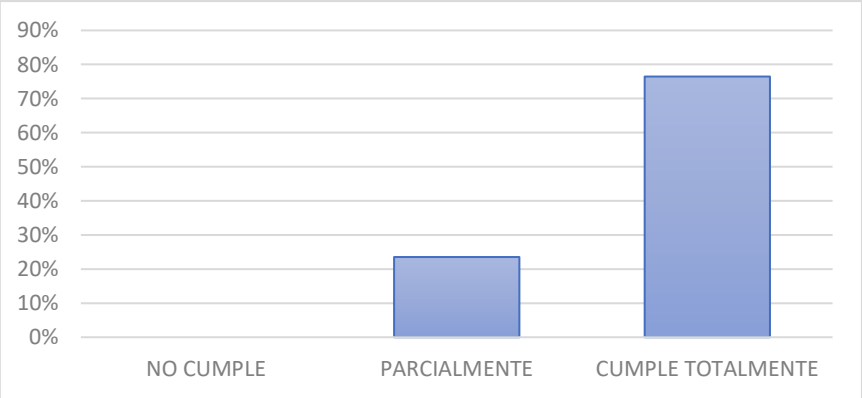


Figura 27: Verificación – Pregunta 6
Fuente: Elaboración propia

Análisis: De un total de diecisiete peritos encuestados, un 76% consideran que la obtención de datos es de relevancia para una investigación y así tener un informe forense estructurado; mientras que un 24% lo consideran de forma parcial.

Pregunta 7: ¿Considera que la guía tiene un grado de importancia durante de recuperación de datos?

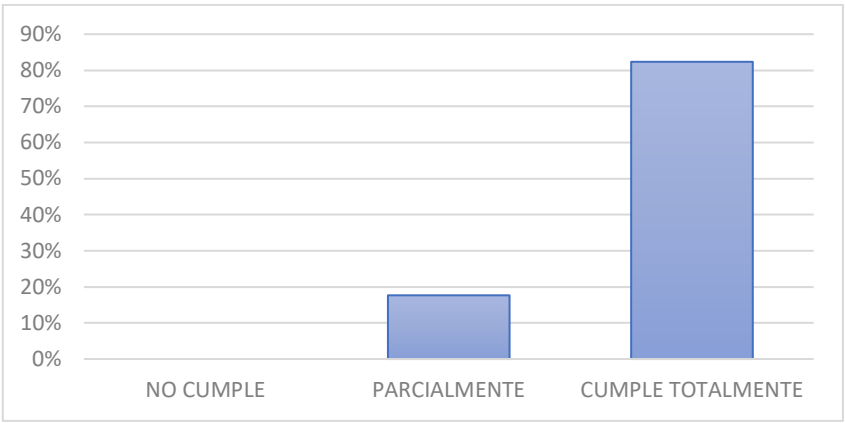


Figura 28: Verificación – Pregunta 7
Fuente: Elaboración propia

Análisis: De un total de diecisiete peritos encuestados, un 82% consideran que la guía tiene un grado de importancia durante de recuperación de datos; mientras que un 18% lo consideran de forma parcial.

Pregunta 8: ¿Considera que el tiempo empleado durante la recuperación de la información en el caso de estudio se redujo utilizando la guía?

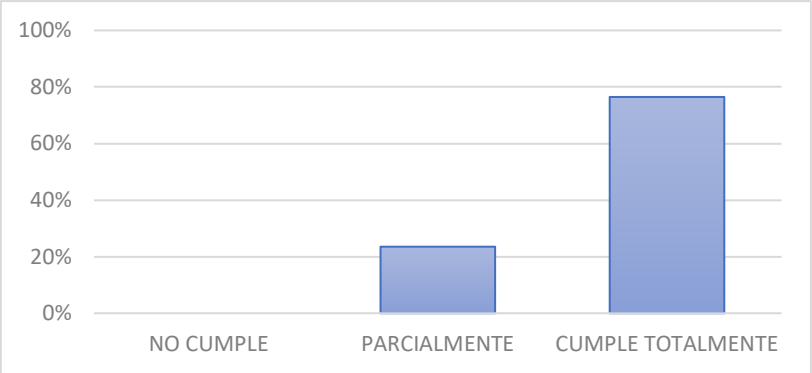


Figura 29: Verificación – Pregunta 8
Fuente: Elaboración propia

Análisis: De un total de diecisiete peritos encuestados, un 76% consideran que el tiempo empleado durante la recuperación de la información en el caso de estudio se redujo utilizando la guía; mientras que un 24% lo consideran de forma parcial.

Pregunta 9: ¿Considera que el proceso de documentación presentado en el caso de estudio reduce el tiempo de recolección de datos forenses con la utilización de la guía?

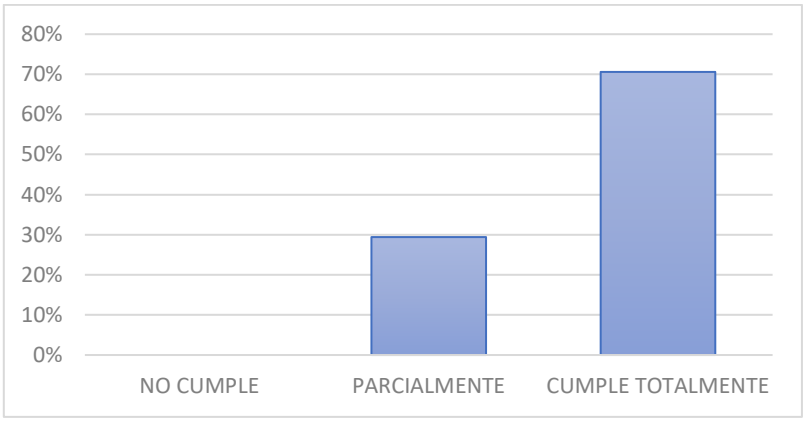


Figura 30: Verificación – Pregunta 9
Fuente: Elaboración propia

Análisis: De un total de diecisiete peritos encuestados, un 71% consideran que el proceso de documentación presentado en el caso de estudio reduce el tiempo de recolección de datos forenses con la utilización de la guía; mientras que un 29% lo consideran de forma parcial.

Pregunta 10: ¿Considera que se redujo el tiempo empleado durante el proceso de análisis presentado en el caso de estudio con la ayuda de la guía?

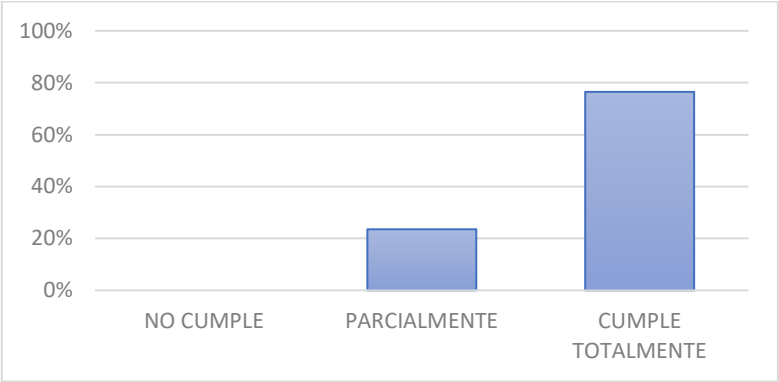


Figura 31: Verificación – Pregunta 10
Fuente: Elaboración propia

Análisis: De un total de diecisiete peritos encuestados, un 76% consideran que se redujo el tiempo empleado durante el proceso de análisis presentado en el caso de estudio con la ayuda de la guía; mientras que un 24% lo consideran de forma parcial.

Pregunta 11: ¿Considera que se redujo el tiempo utilizado durante el proceso de transporte de la información aplicando la guía?

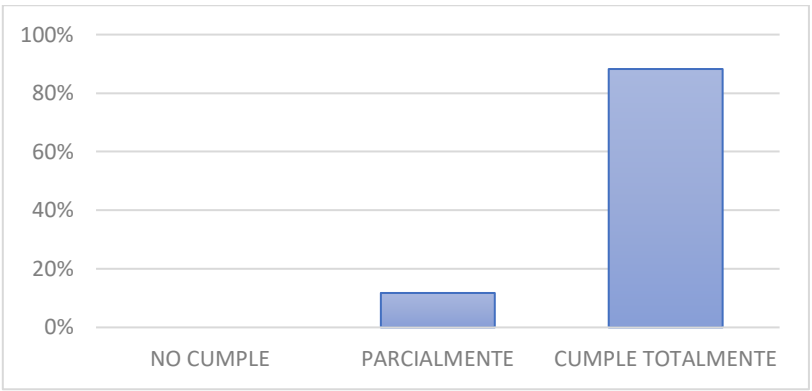


Figura 32: Verificación – Pregunta 11
Fuente: Elaboración propia

Análisis: De un total de diecisiete peritos encuestados, un 88% consideran que se redujo el tiempo utilizado durante el proceso de transporte de la información aplicando la guía; mientras que un 12% lo consideran de forma parcial.

Pregunta 12: ¿Considera que se redujo el tiempo utilizado en el análisis de evidencias de la información aplicando la guía?

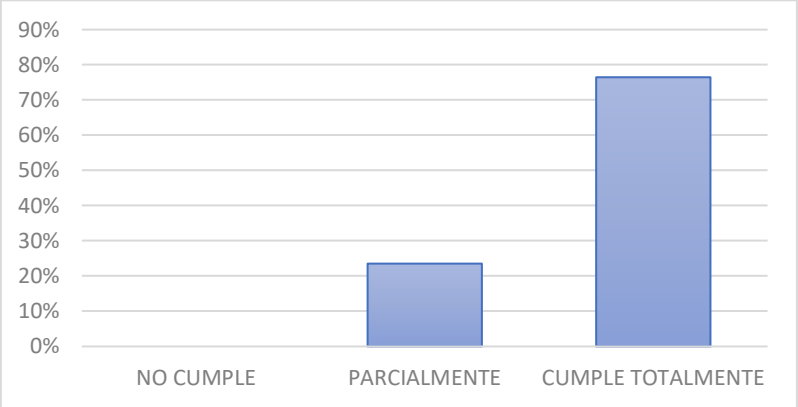


Figura 33: Verificación – Pregunta 12
Fuente: Elaboración propia

Análisis: De un total de diecisiete peritos encuestados, un 76% consideran que se redujo el tiempo utilizado en el análisis de evidencias de la información aplicando la guía; mientras que un 24% lo consideran de forma parcial.

Pregunta 13: ¿Considera que se redujo el tiempo utilizado durante el reporte de datos aplicando la guía?

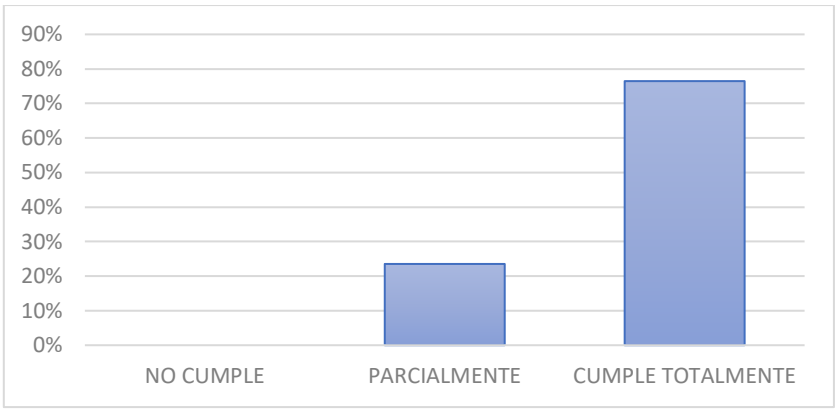


Figura 34: Verificación – Pregunta 13
Fuente: Elaboración propia

Análisis: De un total de diecisiete peritos encuestados, un 76% consideran que se redujo el tiempo utilizado durante el reporte de datos aplicando la guía; mientras que un 24% lo consideran de forma parcial.

Pregunta 14: ¿Considera que la guía utilizada es eficiente y eficaz dentro del área relacionada al peritaje en el país?

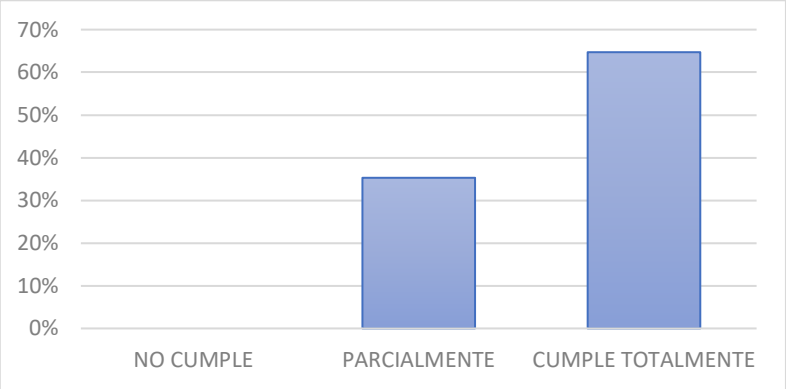


Figura 35: Verificación – Pregunta 14
Fuente: Elaboración propia

Análisis: De un total de diecisiete peritos encuestados, un 65% consideran que la guía utilizada es eficiente y eficaz dentro del área relacionada al peritaje en el país; mientras que un 35% lo consideran de forma parcial.

Pregunta 15: ¿Considera que es viable la aplicación de esta guía dentro de la legislación ecuatoriana en comparación con otras guías que conozca?

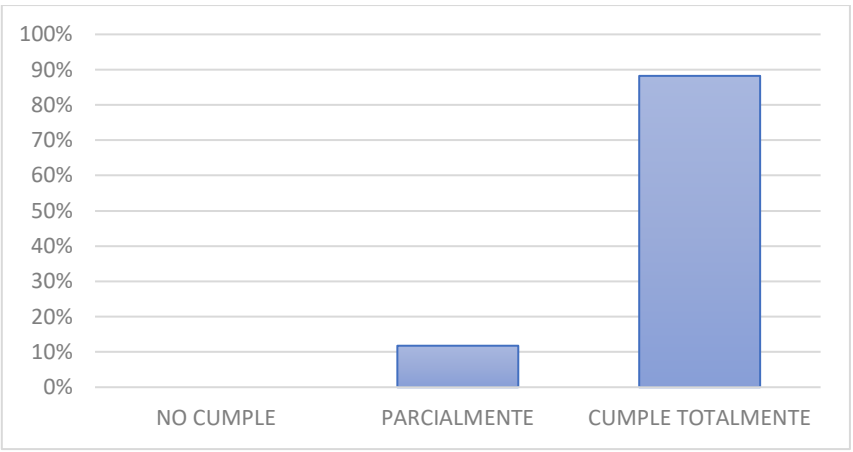


Figura 36: Verificación – Pregunta 15
Fuente: Elaboración propia

Análisis: De un total de diecisiete peritos encuestados, un 88% consideran que es viable la aplicación de esta guía dentro de la legislación ecuatoriana en comparación con otras guías que conozca; mientras que un 12% lo consideran de forma parcial.

4.1.6. Comprobación de la hipótesis

Como consecuencia del presente trabajo investigativo se pudo comprobar que los modelos actuales en lo referente a las tres guías que se analizaron cumplen de manera general con el 84,5% de los requerimientos técnico y legales en Ecuador.

Tabla 5: *Comprobación de requerimientos técnicos y legales*
Fuente: Elaboración propia

REQUERIMIENTO TÉCNICO MAYOR A 80%	GUÍA 1	GUÍA 2	GUÍA 3	GUÍA TESIS
>24	26	24	26	28,23
80%	**86.7%**	**80%**	**86.7%**	**93.3%**

Se puede observar que la presente guía obtiene un 93,3%, cumpliendo con los requerimientos legales y técnicos propuestos en Ecuador, llegando a la siguiente constatación que se detalla en la siguiente gráfica:

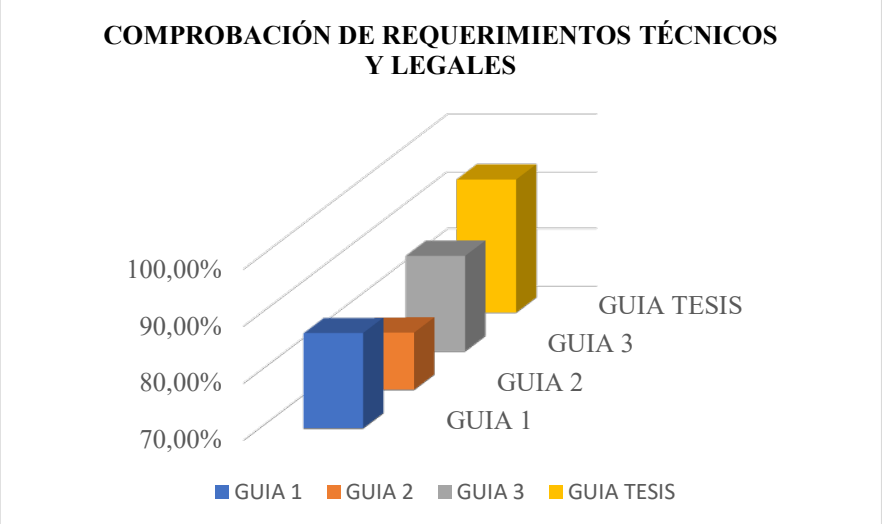


Figura 37: Comprobación de requerimientos técnicos y legales
Fuente: Elaboración propia

Si los requerimientos técnicos y legales en Ecuador nos indican que deben superar el 80% para que las guías sean confiables, la presente guía que se expone en este trabajo investigativo llegó al 93,3%, por lo que esta guía es confiable.

Además, es importante indicar que se pudo obtener el porcentaje en los parámetros de tiempo y recuperación de datos, por lo que la misma es viable en la adaptación al peritaje informático en Ecuador y que se expone a continuación:

Tabla 6: *Comprobación del porcentaje de recuperación*
Fuente: Elaboración propia

PORCENTAJE DE RECUPERACIÓN DE ARCHIVOS	NO CUMPLE/PARCIALMENTE	CUMPLE TOTALMENTE
	7,29%	92,71%

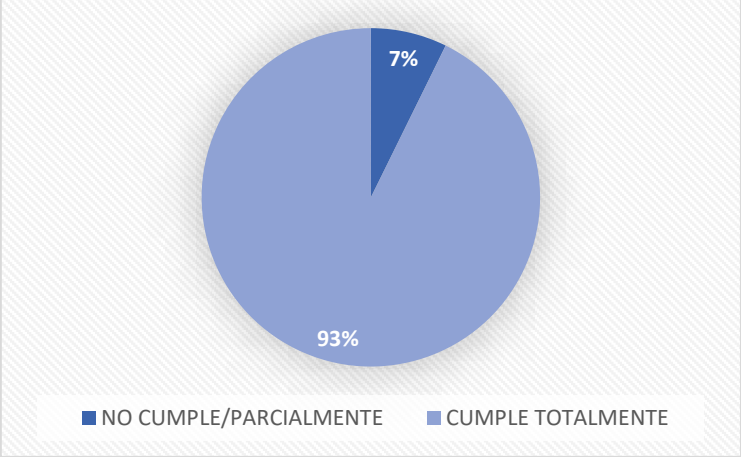


Figura 38: Porcentaje de recuperación
Fuente: Elaboración propia

En primer lugar, la figura 38 muestra de forma general los resultados obtenidos de la encuesta aplicada a peritos informáticos calificados en función del porcentaje de información recuperada, donde refleja porcentajes favorables, obteniendo un 93% Cumple Totalmente, un 7% Cumple Parcialmente/No Cumple.

Tabla 7: *Comprobación del porcentaje de recuperación en función del tiempo*
Fuente: Elaboración propia

TIEMPO DE RECUPERACIÓN DE ARCHIVOS	NO CUMPLE/PARCIALMENTE	CUMPLE TOTALMENTE
	7,50%	92,50%

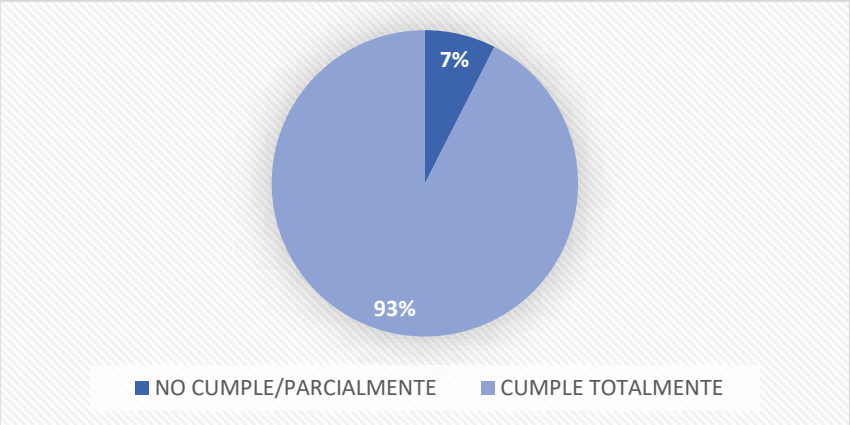


Figura 39: Tiempo de recuperación
Fuente: Elaboración propia.

Por otro lado, la figura 39 muestra de forma general los resultados obtenidos de la encuesta aplicada a peritos informáticos calificados en función del tiempo del proceso de recuperación, donde refleja porcentajes favorables, obteniendo un 93% Cumple Totalmente, un 7% Cumple Parcialmente/No Cumple.

En resumen, cumpliendo con los parámetros exigidos dentro del método Delphi a través de las respuestas brindadas por los peritos informáticos, se pudo observar que el porcentaje de recuperación de archivos (92,71%) y el tiempo de recuperación (92,50%); en concordancia con la comprobación de requerimientos técnicos legales (93,3%), llega a valores altos y fiables, por lo que la presente guía es viable y aplicable en la legislación ecuatoriana, con lo cual se llegó a comprobar la hipótesis planteada.

CONCLUSIONES

Después de haber concluido con el proceso de investigación para la creación de una guía de recuperación de datos utilizando el método File Carving adaptada a la normativa vigente del Ecuador, se ha llegado a las siguientes conclusiones:

- Se pudo estudiar a profundidad la técnica forense File Carving, con el fin de obtener un modelo sistémico y poder sacar los aspectos más relevantes para el análisis de la recuperación de datos en ordenadores Windows.
- Se pudo desarrollar la guía utilizando la técnica forense y adaptado a la normativa legal vigente que a la final servirá para los peritos dentro del campo laboral.
- Se logró realizar un cotejamiento entre las guías mundialmente conocidas con la legislación penal nacional incluyendo además normativas internacionales en relación a la información digital.
- Se pudo validar la presente guía a través de expertos en la rama de la informática forense, por lo que se llegó al paso final, que es su uso en ordenadores con sistema operativo Windows.
- Se evidenció, que este material investigativo, va a ser de mucha utilidad dentro del campo de la informática forense, por cuanto es una herramienta útil en el ámbito legal y educativo.
- Se pudo obtener los porcentajes de 93,3% en requerimientos técnicos legales, 92,50% en componentes de tiempo de recuperación y 92,71% en componentes de recuperación de archivos, obteniendo como resultado una guía viable en su aplicación y ejecución en el campo de la Informática Forense en Ecuador.

RECOMENDACIONES

- Se recomienda a peritos informáticos, impartir seminarios de estudio de técnicas forenses existentes, dirigida a estudiantes de la carrera de Ingeniería en Sistemas y Computación, con el objetivo de incentivar y promover la investigación en esta área.
- Se recomienda el uso de esta guía en el ámbito legal, por cuanto va a ser de mucha utilidad dentro de la rama de los delitos informáticos, contra el estado, o la intimidad personal, etc.
- Brindar apoyo a proyectos investigativos aplicados en la rama de la informática forense.
- Implementar este modelo investigativo para las futuras generaciones, por cuanto será de utilidad para estudiantes de Ingeniería en Sistemas como de Derecho.

BIBLIOGRAFÍA

Alamillo, J. (2016). Estándares nacionales e internacionales que puede seguir un perito informático para realizar el análisis forense de una evidencia y para la elaboración de un peritaje informático.

Amutio, G., & Candau, J. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Ashcroft, J. (2001). Electronic Crime Scene Investigation: A Guide for First Responders. U.S. *Department of Justice Office of Justice Programs.*

Ashcroft, J. (2004). Forensic Examination of Digital Evidence: A Guide for Law Enforcement. U.S. *Department of Justice Office of Justice Programs.*

Ashcroft, J. (2010). *National Institute of Justice*. Obtenido de https://nij.ojp.gov/library/publications/forensic-examination-digital-evidence-guide-law-enforcement

Asier, M. (2014). Guía de toma de evidencias en entornos Windows. . *Instituto Nacional de Ciberseguridad.*

Cajamarca, B., & Grijalva, J. (2018). Desarrollo de una guía metodológica para el análisis forense en equipos de cómputo con Sistema Operativo Mac OS X. *Revista Publicando*, 24-67.

Cantrell, G. (2019). Teaching Data Carving Using The Real World Problem of Text Message Extraction From Unstructured Mobile Device Data Dumps. *The Journal of Digital Forensics, Security and Law.*

Constanzo, B., & Waimann, J. (2012). El estado actual de las Técnicas de File Carving y la necesidad de Nuevas Tecnologías que implementen Carving Inteligente.

Coronel-Rojas, L., & al, e. (2020). Definición de una metodología de adquisición de evidencias digitales basada en estándares internacionales. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 266-282.

de Becerra, G., Caraballo, G., & Babativa, D. (2016). Escala para medir actitudes hacia la investigación (eacin): validación de contenido y confiabilidad. *Aletheia* , 104-121.

Di Iorio, A. e. (2017). El rastro digital del delito: aspectos técnicos, legales y estratégicos de la Informática Forense.

Espitia, J., & Espitia, W. (2014). Análisis forense en discos duros magnéticos y de estado sólido.

Garrote, P., & Rojas, M. d. (2015). La validación por juicio de expertos: dos investigaciones cualitativas en Lingüística aplicada. *Revista Nebrija de lingüística aplicada a la enseñanza de lenguas*, 124-139.

Gómez-Luna, E., & al, e. (2014). Metodología para la revisión bibliográfica y la gestión de información de temas científicos, a través de su estructuración y sistematización. *Dyna* , 158-163.

Grijalva-Lima, J. S., & Loarte-Cajamarca, B. (2017). Modelo para el análisis forense y la legalización de evidencia digital atípica en procesos judiciales en Ecuador.

Jaramillo, D., & Cuenca, J. (2015). Guía metodológica de análisis forense informático en dispositivos móviles con sistema operativo Android.

Jimenez, V., Chavez, W., & Chavez, A. (2018). Análisis forense y sus herramientas.

Laurenson, T. (2013). Performance analysis of file carving tools. *IFIP International Information Security Conference*.

Martínez, M., & March, T. (2015). Caracterización de la validez y confiabilidad en el constructo metodológico de la investigación social. *REDHECS* , 107-127.

Muñoz, A. (2016). Estudio y aplicación de técnicas forenses y de prevención en entornos Cloud.

Ninahualpa, G., Díaz, J. Y., & Piccirilli, D. (2017). Data restoration and file carving. *IEEE*.

Ninahualpa, G., Perez, C., Yoo, S. G., Guarda, T., Diaz, J., & Piccirilli, D. (2018). Restoring data in solid state devices damaged by crushing and falling, using file carving technique. *IEEE*.

Pereyra, D. (2014). Desarrollo de una guía de asistencia para el Análisis Forense informático en un Ambiente Piloto. *XVI Workshop de Investigadores en Ciencias de la Computación*.

Pérez, C. (2018). Estudio comparativo de técnicas file carving para la recuperación de información perdida por daños de impacto y humedad en dispositivos de almacenamiento SSD.

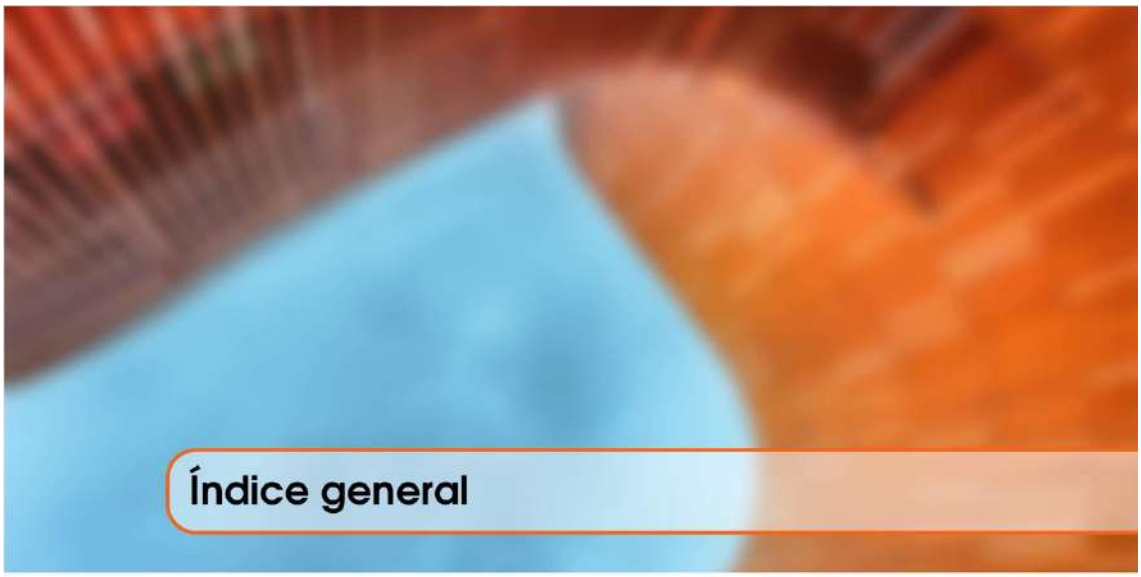
Quiña, G.-N., Yoo, S. G., & Guarda, T. (2019). Recuperación de Datos en Dispositivos de Almacenamiento SSD Utilizando File Carving. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 490-498.

Rodríguez, F., & Doménech, A. (2011). La informática forense: el rastro digital del crimen. *Derecho y Cambio Social* , 21.

ANEXOS

ANEXO 1: GUÍA DE RECUPERACIÓN DE DATOS DESARROLLADA.

Publicado, Agosto 2020



Índice general

1. Sobre la guía

Este documento va orientado a profesionales del sector informático específicamente a peritos informáticos que estén familiarizados con el proceso de análisis forense digital y que pudieran acabar enfrentándose a algún tipo de incidente que requiera realizar. Además de servir como una guía práctica de los pasos que se deben tomar cuando ocurre un incidente, con el fin de recolectar la evidencia necesaria para el análisis posterior para llegar a una solución al incidente en sí.

Contiene información relacionada con la recuperación de datos utilizando técnicas forenses, y en concreto utilizando File Carving en entornos Windows. Se centra en el proceso de toma de evidencias, realizándose las pruebas sobre Windows. No solo proporciona una perspectiva global del proceso, explica la composición del proceso, su propósito, las distintas etapas que constituyen el proceso, el método de implementación del proceso, etc., sino que también proporciona una perspectiva específica sobre la obtención de evidencia.

Las herramientas mencionadas en algunos capítulos son versiones gratuitas con el fin de que todo procedimiento no suponga un coste adicional en cuanto a licencias se refiere.

2. Dispositivos electrónicos

2.1 Computadoras

Una computadora es equipo electrónico cuya función es procesar la información siguiendo instrucciones almacenadas en su interior y finalmente obtener resultados esperados. La lista de instrucciones se llama programa y el medio de almacenamiento interno se llama memoria de computadora, todo equipo consta de una carcasa, placa base, CPU y almacenamiento de datos, con un teclado externo y mouse.[1]

- **Usos principales:** Orientado para todo tipo de funciones informáticas y almacenamiento de información, incluido el procesamiento de textos, cálculos, comunicaciones y gráficos.
- **Evidencia potencial:** La evidencia se encuentra más comúnmente en archivos que se almacenan en discos duros y dispositivos y medios de almacenamiento.

2.2 Componentes

2.2.1 CPU

La unidad central de procesamiento (CPU) es una parte esencial de la computadora, puede recuperar y ejecutar instrucciones además de proporcionar la capacidad de programación junto con la memoria y los dispositivos de entrada/salida. El microprocesador se encuentra en la caja de la computadora en una placa de circuito impreso con otros equipos electrónicos y consta de una unidad aritmética y lógica (ALU), una unidad de control y varios registros. La CPU a menudo se conoce como procesador para en forma de abreviación, la ALU realiza operaciones aritméticas, operaciones lógicas y operaciones relacionadas de acuerdo con las instrucciones del programa.[2]

Normalmente una CPU se puede dividir en tres partes:

- **Memoria principal:** Dispositivo electrónico en el que se almacena el programa que determinará la actuación y lo datos que serán manejados por la CPU.
- **Unidad de control:** Coordina y controla las operaciones que se hagan con los datos. Lee los datos necesarios de la memoria y activa los circuitos necesarios de la ALU.
- **Unidad lógico-aritmética (ALU):** Realiza las operaciones aritméticas y lógicas con los datos que recibe de la unidad de control; procedentes de la memoria principal.

2.2.2 Memorias

La memoria principal almacena temporalmente datos y programas generando un puente entre el sistema operativo, software, procesador y otros dispositivos para que estos intercambien información. Los datos almacenados en estas memorias son de tipo binario y generalmente no se retiene cuando la computadora está apagado (memoria volátil), toda información que contenga el disco deben primero cargarse en la memoria y luego ser ejecutados por el microprocesador. Existe diversos

estándares que ofrecen distintas prestaciones, donde actualmente el estándar más usado es la memoria DDR4.[1]

A continuación se especifica las características clave de cada tipo:

- **Memoria DDR:** Es la versión más antigua y se utiliza en equipos que montan procesadores Pentium 4 y Athlon en sus generaciones más antiguas. Rondan los 400 MHz.
- **Memorias DDR2:** Todavía están bastante extendidas, utilizados en equipos con sockets LGA775 y AM2. Se venden con frecuencias de hasta 1.066 MHz y tienen un precio muy elevado en comparación con el estándar actual, la DDR4.
- **Memorias DDR3:** Fue superada por la DDR4 pero todavía se comercializa, tiene una fuerte presencia ya que se ha utilizado con los sockets LGA1150 (Core 4000) y AM3+ (FX). La velocidad máxima que ofrecen los kits que encontramos en el mercado ronda los 2.400 MHz, aunque algunos modelos concretos consiguen acercarse a los 3 GHz.
- **Memorias DDR4:** Es el estándar actual, ofrece mayor rendimiento. Podemos encontrar kits con velocidades de más de 4 GHz.

Dispositivos de control de Acceso

2.2.3 Escáneres biométricos, Tarjetas inteligentes

La tarjeta inteligente se refiere a la integración de un microprocesador en sus componentes, lo que le permite interactuar con cálculos complejos y almacena información en varios tipos de memoria (RAM, ROM Y EEPROM) por lo que esta tarjeta resulta se buena para procesar información compleja. El chip puede llevar uno o dos microprocesadores; el segundo se encarga de realizar operaciones criptográficas, como firmas electrónicas o códigos de acceso o número de identificación personal (PIN).[3]

El reconocimiento de huellas dactilares es otra de las técnicas más usadas a nivel mundial, desarrollado por John Evangelist Purkinje quien en 1823 realizó los primeros estudios y años más tarde, Sir Francis Galton comenzó sus observaciones para utilizar las huellas como identificadores personales. Una huella dactilar generalmente consta de una serie de líneas negras que representan crestas y una serie de espacios en blanco que representan valles. El reconocimiento de huellas dactilares se basa principalmente en la ubicación y dirección de las crestas, bifurcaciones, deltas, valles y los puntos finales de las crestas.[4]

2.2.4 Cámaras digitales

Una cámara digital es un dispositivo que se utiliza para capturar imágenes fotográficas y video, la principal diferencia con las cámaras "analógicas", está en que los sistemas digitales no necesitan de una película para guardar la información gracias a que posee un sensor electrónico. No existe procesos químicos para registrar la información y transformarla en foto, es por ello que se sustituye por una interpretación en datos numéricos de la información que transporta la luz.[5]

Las características principales son:

- **Resolución:** Capacidad del sensor en capturar los píxeles.
- **Zoom analógico:** Capacidad para ampliar la escena de los lentes que compone la cámara.
- **Pantalla:** Longitud en diagonal, generalmente son pantallas TFT.
- **Alimentación:** Puede ser pilas o baterías, dependiendo del modelo.
- **Sensibilidad:** Capacidad del fotosensor en obtener la luz del exterior

2.2.5 PDA, Organizadores eléctricos

Un asistente digital (PDA) es una pequeña computadora en red que se puede colocar en la palma de su mano, pueden incluir características como la informática, teléfono / fax, buscapersonas, redes, y otras características. Los PDA han estado en desarrollo durante muchos años, comenzando con la primera generación de dispositivos, como Apple Newton y Palm Pilot, posee funciones como calendario y funciones de toma de notas.

Algunos no contienen unidades de disco, pero pueden contener ranuras para tarjetas de PC que pueden contener un módem, disco duro u otro dispositivo. Los sistemas operativos de PDA incluyen Apple iPhone OS, Symbian OS, Palm, Windows CE, Windows Mobile, Blackberry y Google Android. [6]

2.2.6 Discos duros

Los discos duros son dispositivos de almacenamiento no volátil en el que se instalan todos los programas e información necesaria para interactuar con la computadora, es una de las partes más importantes de cualquier sistema informático. El dispositivo está compuesto por platos o discos unidos por un eje que gira a gran velocidad dentro de una caja metálica sellada además de un cabezal de escritura. Cuando el usuario guarda información en el disco duro, éste escribe en los platos una secuencia de unos y ceros a velocidades que se miden en micro segundos.[7]

Se debe considerar el tipo de interfaz que posee como son:

- **PCIe:** Estos discos duros se conectan al ordenador mediante un puerto PCI Express de la misma manera que una tarjeta interna, pudiendo ofrecer mayores velocidades de trabajo.
- **IDE:** La conexión IDE tiene 40 conectores y acepta hasta dos dispositivos conectados a la misma fuente. Hoy en dia es poco utilizado por ser considerado obsoleto, se ha quedado atrás tanto en velocidad como compatibilidad.
- **SATA:** Es la interfaz mas usada actualmente, existen ya varias versiones y las nuevas son compatibles con las anteriores. De esta forma un dispositivo SATA 1.0 será totalmente compatible con una conexión por cable SATA 3.0.
- **USB:** El interfaz USB tiene la ventaja de utilizar un único puerto para conectar la mayor parte de dispositivos externos. La versión 3.0 ya es capaz de transferir hasta 625 MB/segundo, 10 veces más que la versión USB 2.0. Es el estándar más utilizado en los discos duros externos por su versatilidad.

2.2.7 Tarjeta de memoria

Inventada por Toshiba en la década de 1980, las tarjetas de memoria son dispositivos de almacenamiento de datos electrónicos en estado sólido, cuya característica es evitar perder la información cuando se extraiga la tarjeta del computador o de otro dispositivo. Esta capacidad de retener datos

es la clave para las aplicaciones de tarjetas de memoria flash y poder almacenar cientos de imágenes o archivos en general.[8]

Se utiliza en una variedad de dispositivos como son:

- Cámaras de video
- Teléfonos móviles
- PDA's
- Sistemas de geolocalización
- Computadoras personales
- Otros

2.3 Componentes de red

2.3.1 Tarjeta de red - NIC

NIC es el hardware central utilizado para la conexión de red, puede transmitir señales en la capa física y paquetes de datos en la capa de red. Aunque tradicionalmente, las NIC están asociadas con PC, computadoras portátiles y servidores, las NIC pueden existir en casi cualquier dispositivo de red, como impresoras, teléfonos y escáneres.

En algunos equipos de red, existen módulos reemplazables que permiten diferentes tipos de conexión, donde finalmente también se los considera NIC. No importa en qué capa se encuentre el controlador de interfaz de red, este actúa como intermediario entre el ordenador/servidor y la red de datos. [9]

2.3.2 Routers y Switches

Router

Un router es un dispositivo electrónicos utilizado en sistemas informáticos basados en red, diseñado para enrutar comunicaciones según su direccionamiento de capa 3 OSI, donde usa la

dirección de red para determinar la red a la que enrutar el mensaje y luego envía el mensaje de acuerdo con su método.

Todo router puede aplicar algo de inteligencia a su enrutamiento y, mover las comunicaciones a una red más rápida o menos congestionada según sea necesario (según la información disponible), siempre que haya varias rutas entre el enrutador y la red de destino. [9]

Switch

Los switch son componentes centrales de la red utilizados en el área de redes, ubicado en la capa 2 y 3 del modelo OSI dado que enrutan la comunicación entre los dispositivos de red. Se considera un enrutador multicapa cuando operan en la capa 2 y 3.

El conmutador básico es un dispositivo OSI de capa 2, y debido a la caída en el precio de la tecnología necesaria para agregar funciones de OSI capa 3, este tipo de conmutador es cada vez más raro. [9]

2.3.3 Servidores

Los servidores son computadoras que brinda algún servicio para otros ordenadores conectados a él, tienen capacidad de almacenamiento y energía (RAM, procesador) para que otros (clientes) los usen, y su función principal es administrar los servicios en la red. Cualquier computadora incluyendo un portátil, se puede configurar como servidor. [10]

Tipos de servidores

Clase	Descripción
Servidor proxy	Generalmente usados para acceso a la red, contiene firewalls con reglas para permite la navegación.
Servidor web	Se encarga de almacenar sitios web, publicarlos, otorga seguridad y permite libre administración.
Servidor de correo	Encargado de gestionar correos de una empresa, todo en un solo lugar.
Servidor de base de datos	Posibilita el manejo de grandes cantidades de datos y la generación de reportes.
Servidor de impresión	Permite el uso de impresoras conectadas en red, gestionar la petición de los clientes y administrar las peticiones de los usuarios.
Servidor de directorios	Almacena los datos de los usuarios en la red.

Cuadro 2.1: Tipo de servidores

2.3.4 Cable UTP

Los cables de red es un medio físico o elemento físico que proporciona la posibilidad de conectar diversos sistemas electrónicos a otros dispositivos informático entre sí, es ideal para cableado LAN, fácil de instalar y económico. Estos equipos pueden ser como ejemplo computadoras conectadas a un router, de modo que se pueda establecer una vinculación donde se genere un viaje de información entre los equipos y dispositivos conectados.[10]

Cada uno de los 8 hilos de cobre individuales del cable UTP está cubierto con material aislante y cada par de hilos está trenzado, pueden variar de acuerdo a la categoría que pertenezcan:

CATEGORÍA	VELOCIDAD	FRECUENCIA	VELOCIDAD
CAT. 5	100 Mbps	100 MHz	15.5 MB/s
CAT. 5E	1.000 Mbps	100 MHz	150.5 MB/s
CAT. 6	1.000 Mbps	250 MHz	150.5 MB/s
CAT. 6A	10.000 Mbps	500 MHz	1.25 GB/s
CAT. 7	10.000 Mbps	600 MHz	1.25 GB/s
CAT. 7A	10.000 Mbps	1.000 MHz	1.25 GB/s
CAT. 8	40.000 Mbps	2.000 MHz	5 GB/s

Cuadro 2.2: Categoría cable UTP

La velocidad determina la velocidad máxima soportada por cada cable, en diferentes categorías soportan la misma velocidad donde parecen ser iguales, sin embargo se debe tener en cuenta otros parámetros como es la frecuencia. La frecuencia define la potencia de la red, y suele establecer el ancho y rango de pérdida de datos a lo largo del cable.

2.4 Otros dispositivos electrónicos

2.4.1 Impresoras

La impresora permite escribir en papel los resultados obtenidos en el ordenador, algunas impresoras contienen un búfer de memoria, lo que permite recibir y almacenar documentos de varias páginas mientras están en funcionamiento. Existen diferentes tipos: térmicos, láser, inyección de tinta, impacto, matriciales, etc.

Las impresoras suelen aceptar hojas sueltas o papel continuo (en el caso de las matriciales) con perforaciones laterales para un mejor arrastre. Algunos modelos también pueden contener un disco duro. [11]

Tipos de impresoras:

- Impresoras matriciales
- Impresoras de chorro de tinta (Inkjet)
- Impresoras láser
- Otros

2.4.2 Escáneres

El escáner es un dispositivo óptico que permite a una imagen introducir directamente en la computadora mediante el seguimiento de la imagen punto a punto. Esta imagen se almacena en un archivo en un formato estándar, generalmente en formato TIFF (Tag Image File Format), o en otro tipo de formato como es PCX, BMP, GIF y JPG. [11]

Características:

- **Tamaño:** A0, A3, A4, otros.

- **Resolución:** Existen en 400, 600, 1200, 2400ppp (puntos por pulgada).
- Brinda soporte para operar en conjunto con diversos programas con soporte OCR (Reconocimiento óptico de caracteres).

2.4.3 Teléfonos

Un teléfono posee una base ya sea alámbrica o inalámbrica, su función básica es permitir conversaciones bidireccionales entre dos partes remotas. Para ello, el teléfono debe tener un auricular y un micrófono en el auricular o "tubo", obtiene energía de una batería interna, eléctrica o directamente desde el sistema telefónico.[12]

Tipo de teléfonos

- Teléfonos alámbricos.
- Teléfonos inalámbricos.
- Teléfonos satelital.
- Teléfonos móviles.
- Teléfonos inteligentes.

2.4.4 Relojes digitales

Los relojes inteligentes poseen un sistema operativo similar a un teléfono móvil, y pueden sincronizarse con ellos o trabajar de forma independiente, generalmente proporcionan varios tipos de sistemas de notificación para notificar a los usuarios de mensajes, llamadas, citas, etc.

Además almacena información adicional como libretas de direcciones, calendarios de citas, correo electrónico y notas. Permiten la instalación y ejecución de aplicaciones, cuentan con múltiples sensores que interactúan con el entorno y la capacidad de sincronizar información con computadoras.[13]

2.4.5 GPS

Los sistemas de posicionamiento global son sistemas autónomos, proporcionan información sobre viajes, todo esto a través de información de destino, puntos de paso y rutas. Utilizan diferentes sistemas de referencia para expresar la posición de sus satélites. [14]

Segmentos:

- Segmento de usuario.
- Segmento de control.
- Segmento espacial.

3. Introducción al análisis forense

Este capítulo analiza la extracción y el análisis de evidencia digital. La extracción se refiere a la recuperación de datos de los medios y el análisis se refiere a interpretar los datos recuperados y su ubicación en un formato lógico y útil.[15] Los conceptos proporcionados están destinados a ayudar a los examinadores a desarrollar procedimientos y estructurar la revisión de la evidencia digital.

Estos conceptos no pretenden ser exhaustivos y se reconoce que no todas las técnicas siguientes pueden usarse en una situación. El examinador decide si elige el método apropiado. Cabe destacar la importancia de seguir estándares para el buen manejo de la información, como la norma ISO 27001 donde se debe aplicar los 3 pilares importantes durante el proceso como son:

- **Confidencialidad:** La información no se divulgará a personas o sistemas no autorizados. En esencia, solo la autorización correcta y verificada puede acceder a las propiedades de esta información. [16]
- **Integridad:** La calidad de la información debe ser correcta y no modificada, los datos deben ser exactamente iguales a los datos generados sin necesidad de manipulación por parte de terceros. La integridad se pierde cuando la información presente alguna modificación, una practica para preservar la integridad es usar una firma digital. [16]
- **Disponibilidad:** La información no debe ser divulgada a personas o sistemas no autorizados, solo la autorización correcta y verificada puede acceder a las propiedades de esta información. [16]

3.1 Tipos de análisis forense

Se puede clasificar según el tipo de análisis forense. Teniendo en cuenta este aspecto, se pueden determinar tres tipos de análisis:

- Análisis forense de sistemas.
- Análisis forense de sistemas embebidos.
- Análisis forense de memoria volátil.

Esta guía como se ha indicado anteriormente, se centra en la recuperación de archivos en computadoras con plataformas Windows, analizando el estado del sistema de antemano.

3.2 Características

El procedimiento de análisis forense debe poseer las siguientes características:

- **Verificable:** Se debe poder comprobar la veracidad de las conclusiones extraídas a partir de la realización del análisis.
- **Reproducible:** Se deben poder reproducir en todo momento las pruebas realizadas durante el proceso.
- **Documentado:** Todo el proceso debe estar correctamente documentado y debe realizarse de manera comprensible y detallada.
- **Independiente:** Las conclusiones obtenidas deben ser las mismas, independientemente de la persona que realice el proceso y de la metodología utilizada.

3.3 Fases

El procedimiento de análisis forense consta de las siguientes fases:

Figura 1: Fases del análisis forense

- **Preservación:** Garantiza que no se pierdan las evidencias que deben ser recopiladas para su posterior análisis. Aspectos críticos como que no se apaguen los equipos para poder preservar la información volátil o la correcta rotulación de los elementos a analizar se realizan durante esta fase.
- **Adquisición:** Corresponde a la etapa en la que se recopilan las evidencias. Una evidencia puede ser definida como cualquier prueba que pueda ser utilizada en un proceso legal, aunque no siempre sea así.
- **Análisis:** Durante el análisis de la información recopilada se debe tener presente el tipo de incidente al que se pretende ofrecer respuesta.
- **Documentación:** Se debe realizar dicha fase de una manera muy metódica y detallada. Se pueden realizar, entre otras, las siguientes acciones:
  - Fotografiar las pruebas.
  - Cadena de custodia.
  - Documentar todos y cada uno de los pasos realizados durante el proceso, manteniendo una bitácora con fechas y horas de cada acción realizada sobre las evidencias.
  - Elaborar dos tipos de informe de conclusiones: uno ejecutivo y uno técnico.
- **Presentación:** Durante la presentación de la información es importante ya que se deben hacer accesibles y comprensibles las conclusiones que se han obtenido del proceso del análisis forense. Para ello, es recomendable seguir las siguientes pautas:
  - Preparar una presentación de manera pedagógica que sea fácilmente comprensible.
  - Detallar las conclusiones.
  - Explicar de manera clara el proceso que se ha llevado para la obtención de las evidencias.
  - Evitar las afirmaciones no demostrables o los juicios de valor.
  - Elaborar las conclusiones desde un punto de vista objetivo.

  A manera de observación, to.das estas fases no son secuenciales sino que están entrelazadas entre sí.

3.4 Metodología y guías

Existen diferentes metodologías o guías a la hora de realizar un análisis forense tales como la UNE 71505:2013, UNE 71506:2013, RFC 3227, RFC 4810, ISO/IEC 27037:2012, ISO/IEC

27040:2015, ISO/IEC 27042:2015, RFC 4998 y RFC 6283, si bien todas tienen aspectos comunes. Como referencia para este documento se va a tomar la norma RFC 3227 «directrices para la recopilación de evidencias y su almacenamiento», el cual refleja de una manera completa el proceso de actuación y las pautas que se deben seguir a la hora de realizar un análisis de éste tipo.**[17]**

Finalmente, las siguientes guías que se pueden utilizar como referencia para aquellas personas que deseen conocer a profundidad del tema:

- Toma de evidencias en entornos Windows
- Electronic Crime Scene Investigation: A Guide for Law Enforcement
- Forensic Examination of Digital Evidence: A Guide for Law Enforcement
- La norma ISO 27001: Aspectos clave de su diseño e implantación
- Manual de Manejo de Evidencias Digitales y Entornos Informáticos
- Introducción a la Informática Forense

4. Directrices para la recolección de datos

4.1 Principios para la recolección de evidencias

Existe una gran cantidad de incidentes relacionados con la seguridad informática:

- **Robo de información:** El robo de información privada es una de las mayores preocupaciones de usuarios y empresas.
  Existen muchas prácticas que permiten el robo de información, como monitorear el tráfico de la red mediante rastreadores, interceptar correos electrónicos o simplemente insertar un pendrive y copiar información privada.
- **Fraude:** Existen multitud de ejemplos de fraudes a través de Internet, entre los que destacan:
  - Falsas ofertas de empleo
  - Estafas de loterías y sorteos
  - Falsas herencias.
  - Fraudes de inversiones y créditos.
  - Descargas que facturan servicio de SMS Premium.
- **Malware:** El malware es otro incidente más común al que puede enfrentarse un analista forense, la especialización del mercado durante los últimos años ha incrementado enormemente este tipo de volumen de transacciones.
  Cuando se trata de amenazas, en algunos casos se ha alcanzado un alto grado de madurez.
- **Accesos no autorizados:** Según un estudio de ThreatTrack Security, además de explotar las vulnerabilidades del software para ganar privilegios y así poder acceder a carpetas o documentos de información confidencial, el acceso no autorizado a páginas con contenido pornográfico es también uno de los principales motivos de las infecciones informáticas de las empresas.
- **Uso inapropiado de recursos:** En las empresas, el uso inadecuado de los recursos es una práctica bastante común.
  El imprimir documentos personales o descargar contenidos audiovisuales como películas o series son los ejemplos más habituales.

4.1.1 Acciones que debe evitarse

Para evitar invalidar el proceso de recolección de información, se deben evitar las siguientes medidas para mantener su integridad en los resultados obtenidos, y así poder ser utilizados en experimentos cuando sea necesario:

- No apague la computadora hasta que se haya recopilado toda la información volátil.
- No confíe en la información proporcionada por los programas del sistema, ya que pueden estar dañados. La información debe recopilarse de los medios protegidos a través de programas específicos para su fin.
- No ejecute programas que modifiquen la fecha y hora de acceso a todos los archivos del sistema.

4.1.2 Principios del peritaje

Actualmente en el país se considera algunas reglas o normas que el perito debe tomar en cuenta durante su labor como es:

- **Admisible:** Para que la prueba tenga efecto judicial, debe cumplir con lo establecido en la ley vigente.
- **Objetivo:** Los expertos deben ser objetivos y respetar la ética profesional.
- **Auténtico:** Debe ser posible demostrar que la evidencia corresponde al incidente involucrado.
- **Completo:** Debe corresponder a la información completa, no de forma parcial.
- **Inalterable:** En todos los casos, existirá una cadena de custodia bien mantenida, lo que demuestra que no se realizaron cambios en los medios durante el período de dure la pericia.
- **Confiable:** No hay duda de que la forma de obtener la evidencia y las operaciones posteriores puede cuestionar su autenticidad y precisión.
- **Creíble:** Debe ser creíble y fácil de entender por el tribunal.
- **Documentar:** Las gestiones realizadas en el procedimiento pericial deben determinarse por escrito.
  - Observe y registre la escena física, como la posición del mouse y la posición relativa entre otros componentes.
  - Registre el estado y la ubicación del sistema informático, incluido el estado de energía de la computadora. Por ejemplo, si el sistema de la computadora está caliente, eso podría indicar que está encendido o que se apagó recientemente.
  - Grabe toda la escena para crear un registro visual, como lo muestra el primer respondedor. Si es posible, se debe inspeccionar toda la habitación dentro de los 360 grados de cobertura.
  - Tome fotografías de la parte frontal de la computadora, la pantalla del monitor y otros componentes. También haga un registro de lo que aparece en la pantalla del monitor.

5. Procedimiento de recolección

5.1 Principios

Debe ser lo más detallado posible para garantizar que no haya información ambigua y minimizando la toma de decisiones. La evidencia digital es sumamente frágil y puede ser alterada, dañada o destruida por una manipulación o inspección incorrecta, por lo que se deben tomar precauciones especiales para preservar dicha evidencia. De lo contrario, podría inutilizarlo o sacar conclusiones incorrectas.

Como todas las demás pruebas, las pruebas informáticas deben manejarse con cuidado y procesarse de manera que se preserve su valor probatorio, lo que implica no solo la integridad física del artículo o equipo, sino también los datos electrónicos que contiene.

Por lo tanto, ciertos tipos de pruebas informáticas requieren una recogida, embalaje y transporte especiales. Se debe tener en cuenta la protección de los datos que puedan ser susceptibles de daño o alteración por campos electromagnéticos (como los generados por electricidad estática, imanes, transmisores de radio y otros dispositivos).

5.2 Equipos electrónicos y pruebas periféricas

Los siguientes dispositivos electrónicos pueden contener evidencia potencial relacionada con actividades delictivas. Si es necesario acceder a la información del dispositivo, la manipulación del dispositivo deben registrarse en cada momento para mantener la autenticidad de la información.

* Grabadoras de audio
* Celulares
* Discos compactos (CD-ROM)
* Dispositivos extraíbles
* Cámaras digitales
* Máquinas de fax
* Teléfonos convencionales
* Cables
* Tarjetas de memoria
* Impresoras
* Escáneres
* Dispositivos de almacenamiento extraíble
* Puntos de acceso

5.3 Procedimiento

Los siguientes puntos describen los pasos básicos:

- Proteja la evidencia digital de acuerdo con las pautas departamentales.
- Registre la configuración de hardware y software del sistema a examinar.
- Verificar el funcionamiento del sistema informático del examinador con el objetivo de incluir hardware y software.
- Retire la carcasa de la computadora a examinar para permitir su acceso físico a dispositivos de almacenamiento.
- Identifique el o los dispositivo de almacenamiento que se analizarán. Dichos dispositivos pueden ser internos, externos o ambos.
- Registre los dispositivos de almacenamiento interno y la configuración del hardware. Estos pueden ser por ejemplo:
  - Características del disco duro (modelo, tamaño, interfaz, localización, etc.).
  - Componentes internos (tarjeta de video, tarjeta de red, tarjeta de sonido, etc.).
- Desconecte el dispositivo de almacenamiento para evitar destruir, dañar o alterar sus datos.
- Utilice el arranque controlado para recuperar información de configuración del sistema sospechoso.
  - Realice un arranque controlado para capturar la información del CMOS/BIOS y probar sus funciones.
  - Realice un segundo arranque controlado para probar las funciones de la computadora y el disco de arranque forense.
  - Vuelva a conectar el dispositivo de almacenamiento y realice un tercer arranque controlado para capturar la información de configuración de la unidad del CMOS/BIOS.
- Apagar el sistema.
- En lo posible, retire el dispositivo de almacenamiento del sujeto y use el sistema del examinador para la recolección. Cuando conecte dispositivos relacionados al sistema del examinador, configure el dispositivo de almacenamiento para que sea reconocido.
- En casos especiales, puede decidir no eliminar el dispositivo de almacenamiento del sistema correspondiente por los siguientes motivos:
  - Sistemas portátiles. Puede resultar complejo acceder a la unidad del sistema o simplemente no poder utilizar cuando se separe del sistema original.
  - Disponibilidad de equipos. El examinador no está autorizado a utilizar el equipo necesario.
  - Almacenamiento en red. Es posible que deba usar equipo de red para obtener los datos.
- Al obtener la evidencia, asegúrese que el equipo de almacenamiento del examinador esté limpio desde el punto de vista forense.
- Si usa protección contra escritura por hardware:
  - Instalar dispositivo de protección contra escritura.
  - Inicie el sistema utilizando el sistema operativo controlado por el examinador.
- Si usa protección contra escritura por software:
  - Inicie el sistema utilizando el sistema operativo controlado por un inspector.
  - Habilitar la protección contra escritura.
- Capture el número de serie electrónico del dispositivo y los datos específicos del host accesibles a otros usuarios.
- Usar herramientas de software y hardware apropiadas para obtener evidencia del tema para el dispositivo de almacenamiento del examinador.
  - Software de copia independiente.
  - Software para el análisis forense.
  - Dispositivos de hardware dedicados.

- Verifique que la adquisición de información haya sido exitosa, comparando los valores conocidos del original y la copia o comparando el original y la copia sector por sector.

5.3.1 Reproducible

Esté preparado para reproducir con precisión los métodos utilizados, y dichos métodos hayan sido probados por expertos independientes. La evidencia electrónica debe recopilarse de acuerdo con las pautas departamentales, en ausencia de pautas departamentales que describan los procedimientos de recolección de evidencia electrónica.

5.3.2 Consideraciones generales

- ¿Dónde está la evidencia? Enumere los sistemas involucrados en el incidente y cuales de ellos se debe obtener la evidencia.
- Proteja la evidencia digital de acuerdo con las pautas departamentales.
- Establecer qué es relevante. En caso de duda, es mejor recopilar mucha información en lugar de una pequeña cantidad de información.
- Retire el estuche de la computadora que se revisará para permitir el acceso físico al dispositivo de almacenamiento.
- Fijar el orden de volatilidad para cada sistema.
- Obtener la información de acuerdo al orden establecido.
- Comprobar el grado de sincronización del reloj del sistema.
- A medida que realiza los pasos de recopilación, pregúntese qué más se puede utilizar como prueba.
- Desconecte el dispositivo de almacenamiento para evitar daños o alteración de los datos.
- No olvide a las personas involucradas. Escriba dónde están las personas, qué están haciendo, qué están observando y cómo reaccionan.

5.4 Software forense

Existen diferentes herramientas para algunas tareas en específico ya sea estos de pago o no, es así que el examinador puede armar un kit de herramientas necesarias dependiendo de la situación. Por ejemplo un kit dedicado para recuperar información como el presentado a continuación:

Herramienta	URL
FTK Tools	https://accessdata.com/products-services/forensic-toolkit-ftk
Autopsy	https://www.autopsy.com/
WinHex	https://www.x-ways.net/winhex/
PhotoRec	https://www.cgsecurity.org/wiki/PhotoRec

Cuadro 5.1: Software forense

6. Empaquetar, Almacenar y Transportar

Las medidas tomadas no deben agregar, modificar o destruir datos almacenados en computadoras u otros medios. Todo ordenador resulta ser frágiles, sensible a la temperatura, la humedad, las vibraciones físicas, la electricidad estática y las fuentes magnéticas.

Se deben tomar precauciones durante el empaquetado, transporte y almacenamiento de la evidencia electrónica. Para mantener la cadena de custodia de evidencia electrónica, documentar su empaque, transporte, y almacenaje.

6.1 Cadena de custodia

La cadena de custodia es un sistema de garantía basado en el principio de identidad y tiene como objetivo asegurar la autenticidad de las evidencias que se utilizarán como prueba en el proceso. Para situaciones específicas, la información mínima procesada en la cadena de custodia es la siguiente:

a. Hoja de ruta, que registra los datos principales sobre la descripción de la evidencia, fecha, hora, custodio, identidad, ubicación y firma, indicando quién recibió y quién entregó.
b. Recibos personales guardados por cada custodio y datos similares a la hoja de ruta.
c. Etiquetas adheridas a los contenedores de pruebas, como bolsas de plástico, sobres de papel, sobres de papel manila, botellas, cajas de cartón, etc.
d. Etiquetas con la misma información que los rótulos, pero con una cuerda atada a una bolsa de papel kraft, frasco o caja de cartón o bolsa de fibra.
e. Registro de entrada y salida o cualquier otro sistema o sistemas informáticos que deban llevarse en los laboratorios de análisis, en las fiscalías y departamento de investigadores.

6.1.1 Interrogantes durante el proceso

Una vez visto la información que se maneja en la cadena de custodia, se debe plantear también algunas preguntas durante este proceso como pueden ser:

- ¿Dónde?, ¿cuándo? y ¿quién? descubrió y recolectó la evidencia.
- ¿Dónde?, ¿cuándo? y ¿quién? manejó la evidencia.
- ¿Quién ha custodiado la evidencia?, ¿cuánto tiempo? y ¿cómo la ha almacenado?

- Si la evidencia cambia de custodia, indicar cuándo y cómo se realizó el intercambio, incluyendo número de albarán, etc.

6.2 Proceso de empaquetado

Si se recopilan varios sistemas informáticos, se debe etiquetar cada sistema para que se pueda volver a montar como está. Por ejemplo:

SISTEMA	CONTENIDO
Ordenador 1	Mouse
	Keyboard
	Monitor
	Placa base
Ordenador 2	Mouse
	Keyboard
	Monitor
	Placa base

Cuadro 6.1: Etiquetado por sistema

a. Antes del embalaje, asegúrese que todas las pruebas electrónicas recopiladas se hayan registrado, marcado e inventariado correctamente.
b. Preste atención a la evidencia potencial o rastreable y tome medidas para preservarla.
c. Utilice un embalaje antiestático ya sea este papel o bolsas de plástico antiestáticas, con el objetivo de embalar los medios magnéticos. Evite el uso de materiales que generen electricidad estática, como bolsas de plástico convencionales.
d. Evite arrugar, doblar o rayar los soportes informáticos, como disquetes, CD-ROM y cintas.
e. Asegúrese que todos los contenedores que se utilizan durante el procedimiento para almacenar pruebas estén etiquetados correctamente.

6.3 Proceso de transporte

a. Mantenga las fuentes magnéticas alejadas de la evidencia electrónica. Como ejemplos se encuentran los transmisores de radio, los imanes de los altavoces y los asientos con calefacción, entre otros.
b. Toda prueba electrónica se debe evitar almacenarlo en vehículos durante un período de tiempo. Todo ambiente que presente calor, frío o humedad excesivos pueden dañar la evidencia electrónica.
c. Toda computadora y otros componentes deben estar asegurados en el vehículo con el fin de evitar golpes o vibraciones (si no están empaquetados en contenedores), la computadora puede colocarse en el piso del vehículo, el monitor puede colocarse en el asiento con la pantalla hacia abajo y asegurarse con un cinturón de seguridad.
d. Mantenga en todo momento la cadena de custodia en todas las pruebas que sean transportadas.

6.4 Proceso de almacenamiento

La información debe almacenarse en un dispositivo que haya demostrado su seguridad y permita la detección de intentos de acceso no autorizados. Tenga en cuenta que debido al almacenamiento a largo plazo, es posible que se pierdan pruebas potenciales como la fecha, la hora y la configuración del sistema.

Sabiendo que toda batería tiene un periodo de vida corto, esto puede llevar a la pérdida de datos cuando presente fallas, por lo tanto, el personal apropiado ya sean estos encargados de custodio de pruebas, jefe de laboratorio, examinador forense, entre otros, deben ser informados si existe algún dispositivo alimentado por baterías para su atención inmediata.

a. Asegúrese de realizar un inventario de toda la evidencia siguiendo las políticas departamentales.
b. Almacene la evidencia en un área segura lejos de la temperatura y la humedad extrema. Protéjalo de fuentes magnéticas, humedad, polvo y otras partículas o contaminantes dañinos.

6.5 Herramientas necesarias

- Se deben utilizar herramientas externas al sistema dado que dichas herramientas pueden estar dañadas.
- Se debe intentar utilizar herramientas que eviten cambiar lo menos posible el escenario, las herramientas de interfaz gráfica y las herramientas que ocupan mucha memoria.
- El programa utilizado para recopilar pruebas debe estar ubicado en un dispositivo de solo lectura (CDROM, USB, etc.).
- Se debe preparar un conjunto de utilidades adecuadas para el sistema operativo que está utilizando.
- Entre otras cosas, el conjunto de herramientas de análisis debe incluir los siguientes tipos de herramientas:
  - Software diseñado para verificar el estado del sistema.
  - Software para ejecutar copias bit por bit.
  - Software que realice listados y analizar procesos.

7. Análisis de evidencias

7.1 Introducción

Uno de los principales desafíos a la hora de realizar un análisis forense es tener muy claro los tipos de eventos a los que nos enfrentamos y, a partir de ahí, comprender qué información hay que recopilar y cómo proceder. Aunque hay algunos aspectos en común, el análisis forense en malware no es lo mismo que el análisis forense en fraude, por lo cual los investigadores se enfocan en diferentes métodos para encontrar evidencia.

El proceso forense se puede realizar de diferentes formas, por un lado esta todo método basado en software y por el otro el método basado en hardware, donde existe una gran cantidad de dispositivos diseñados específicamente para realizar diversas tareas y con alta eficiencia. La presente guía está diseñada para ayudar a peritos informáticos o en áreas relacionadas a la informática forense, por lo cual en este caso se utilizará el método basado en software, especialmente software libre, con el fin de evitar el pago de licencias por su uso.

Al examinar la evidencia digital, se aplican los principios generales de recolección de evidencia, y diferentes tipos de casos y medios pueden requerir diferentes métodos de inspección. Para este propósito, las personas que realizan el examen de evidencia digital deben estar capacitadas. Este capítulo trata sobre la extracción y el análisis de evidencia digital donde la extracción se refiere a la recuperación de datos de los medios y el análisis a interpretar los datos recuperados y su ubicación en un formato lógico.

7.2 Análisis forense por categorías

La siguiente categorías debería ayudar a los investigadores a determinar hallazgos en común durante el análisis forense y determinar a que tipo pertenece. Estas categorías ayudaran de igual forma a definir el alcancen del análisis a realizar.

7.2.1 Fraude en subastas

* Libreta de direcciones
* Calendario
* Información del cliente
* Software de cámara digital
* Registros financieros
* Archivos de imagen
* Registro de actividad en internet
* Software de acceso a instituciones financieras en línea
* Registros telefónicos

7.2.2 Intrusión informática

* Archivos de configuración
* Programas ejecutables
* Registro de actividad en internet
* Registro de chats en internet
* Archivos de texto (nombre de usuario y contraseñas)

7.2.3 Fraude económico (en línea, falsificación)

* Calendario
* Cheques, moneda
* Información del consumidor
* Correos, notas, correspondencia
* Captura de firmas
* Registros de actividad en la red
* Software de acceso a instituciones financieras en línea

7.2.4 Robo de identidad

Herramientas de hardware y software
* Backdrops
* Generadores de tarjeta de créditos
* Cámaras digitales

Plantillas de identificación
* Imágenes digitales para identificación
* Firmas electrónicas
* Firmas escaneadas

Robo de identidad relacionada a la actividad en internet
* Documentos borrados
* Archivos del sistema y file slack
* Actividad en sitios de falsificación por la www

Instrumentos negociables
* Números de tarjetas de crédito
* Cheques personales
* Documentos de transferencia (activos)
* Cheques de negocio

7.2.5 Piratería de software

* Archivos de imagen certificados por software
* Números de serie
* Registro de actividad en la red
* Información y herramientas de software para craqueo

7.2.6 Fraude en telecomunicaciones

* Software de clonado * Número de serie electrónico (ESN), Número de identificación móvil (MIN)
* Actividad en internet * Registros telefónicos

7.3 Procedimiento

Al analizar toda evidencia, considere los siguientes pasos:

1. **Preparación:** Prepare uno o más directorios de trabajo en un medio separado donde pueda recuperar y/o extraer documentos probatorios.
2. **Extracción:** Existen dos tipos diferentes de extracción, como es la extracción física y extracción lógica. Donde la fase de extracción física identifica y restaura los datos en toda la unidad de almacenamiento, independientemente del sistema de archivos. La extracción lógica identifica y restaura archivos según el sistema operativo instalado, el sistema de archivos y/o programas instalados.

Extracción física

En esta etapa, independientemente del sistema de archivos de la unidad, los datos se extraen de la unidad a nivel físico. Esto puede incluir los siguientes métodos: búsqueda de palabras clave, tamaño de archivo y extracción de la tabla de particiones y espacio no utilizado de la unidad física.

- Realizar una búsqueda por palabras claves en la unidad física puede resultar útil porque permite que el analizador extraiga datos que el sistema operativo y el sistema de archivos pueden no conozcan.
- Utilizar File Carving por medio de herramientas especializadas resulta bueno para recuperar y extraer archivos y datos disponibles en la unidad física donde el sistema operativo y el sistema de archivos pueden no reconocer.
- Verifique la estructura de la partición para identificar el sistema de archivos existente y determinar si se ha considerado el tamaño completo del disco duro.

Extracción lógica

En esta etapa, la extracción de datos de la unidad se basa en el sistema de archivos existente en la unidad y puede incluir datos de áreas como archivos activos, archivos eliminados, file slack y espacio de archivos no asignado.

- Extraiga la información del sistema de archivos para obtener las características tales como estructura del directorio, atributos de los archivos, el nombre del archivo, la fecha y hora, el tamaño y la ubicación del archivo.
- Al comparar el valor hash calculado con el valor hash autenticado, se realiza la reducción de datos para identificar y eliminar archivos conocidos.
- Extraiga archivos relacionados con la inspección. La forma de lograr esto puede basarse en el nombre y la extensión del archivo, el encabezado del archivo, el contenido del archivo y la ubicación en la unidad.
- Recuperar archivos borrados.
- Extraiga datos comprimidos, cifrados y protegidos con contraseña.
- Extracción de file slacks (Espacio de almacenamiento de datos desde el final del archivo hasta el final del clúster).
- Extracción del espacio no asignado.

3. **Análisis de datos extraídos:** El análisis puede requerir la inspección de solicitudes de servicio, incluir la autoridad legal para buscar evidencia digital, pistas de investigación y/o pistas de análisis. Además de interpretar los datos extraídos para determinar su relevancia para el caso, algunos ejemplos pueden incluir fechas límite, aplicaciones y archivos, propiedad y posesión, entre otros.

Análisis por línea de tiempo (Timeframe)
Es útil para determinar cuándo ocurre un evento en un sistema informático y ayuda a asociar el uso de la computadora con respecto a la o las personas cuando ocurre un evento.
Se pueden utilizar dos métodos:

- Revisar la fecha y hora que existe en los metadatos del sistema de archivos, mencionando por ejemplo, última modificación, último acceso, creación, cambio de estado, y así poder relacionar los archivos relevantes con períodos de tiempo para la investigación.
- Revise los registros de aplicaciones y sistemas que puedan existir, esto puede incluir registros de errores, instalación, conexión, etc.

Análisis de ocultación de datos (Data hiding)
Sabiendo que en todo datos existe la posibilidad de poder ocultarlo en el sistema informático, el análisis de ocultación de datos otorga soporte en detección y recuperación de dichos datos. De igual forma existe varios métodos a tomar en cuenta como son:

- Asocie el encabezado del archivo a la extensión de archivo correspondiente, esto ayudara a identificar las diferencias, si presenta alguna discrepancia puede indicar que el usuario efectivamente esta ocultando datos de forma intencionada.
- Visite el Área protegida del anfitrión (HPA), si existe datos creados por el usuario en HPA esto indicaría un intento de ocultar datos.
- Estenografía, el usuario puede ocultar información en archivos de imágenes, sonidos o en canales encubiertos a través de métodos y técnicas computacionales.

Análisis de archivos y aplicaciones
Muchos programas y documentos pueden contener información relevante con la investigación y proporcionar información sobre la capacidad del sistema y la experiencia del usuario. Como puede ser:

- Observe los nombres de cada archivo con el fin de determinar si es o no relevante y sus patrones.
- Analizar el contenido de los archivos.
- Identifica el número y tipo de sistemas operativos (si existiera mas de uno).
- Relacionar los archivos obtenidos como las aplicaciones instaladas.
- Tenga en cuenta la relación entre archivos, es decir, el historial de navegación con los archivos caché o archivos de correo con el correo adjunto, por mencionar algunos ejemplos.
- Identificar tipos de archivos desconocidos y con ello se determinara si representa algún valor a la investigación.
- Analizar la configuración hecha por el usuario.

Posesión y propiedad
Existen casos donde se debe identificar a la persona que creó, modificó o accedió a un archivo, pueden basarse en algunos factores como son:

- Colocar al sujeto en la computadora en una fecha y hora en particular, puede ayudar a determinar la propiedad y la posesión (Análisis por timeframe).
- Los archivos de interés pueden estar localizados en ubicaciones no predeterminadas, por ejemplo, directorios creados por el usuario. (Análisis de archivos y aplicaciones).
- El nombre del archivo puede indicar el contenido del archivo y este podría llegar a ser un dato probatorio. (Análisis de archivos y aplicaciones).
- Los datos ocultos se interpretaría como un intento del usuario de evitar la detección. Si se logran recuperar las contraseñas para obtener acceso a archivos cifrados y protegidos con contraseña, estas contraseñas pueden indicar posesión o propiedad. (Análisis de ocultación de datos - Data hiding).
- El contenido de un archivo puede indicar la propiedad o la propiedad al incluir información específica del usuario. (Análisis de archivos y aplicaciones).

4. **Conclusión:** Los resultados que se espera obtener de cualquiera de estos pasos pueden no ser suficientes para sacar conclusiones, el objetivo es servir de apoyo haciendo una correlación entre los resultados para proporcionar una descripción más completa. Finalmente en el proceso de inspección, asegúrese de considerar completamente los resultados de la extracción y el análisis.

8. Recuperación de datos. Técnica forense

Introducción

La información tiende a mantenerse en la unidad incluso si el usuario lo borra, por lo cual si el respectivo borrado de información no se lo hace de forma correcta, facilitará el uso de diversas técnicas para el análisis y recuperación que permitan acceder a dicha información.

Durante el trascurso del capítulo se mencionarán varias técnicas relacionadas con Carving como File Carving y Data Carving, incluyendo conceptos generales, características, herramientas, etc. Esta información brindara un mejor comprensión del tema.

8.1 Conceptos Generales

8.1.1 Disco Duro Magnéticos HDD

Figura 8.1: Interior disco duro magnético

Considerado como un dispositivo de almacenamiento no volátil con el objetivo de almacenar información, ya sea esta programas, imágenes, musica, entre otros. Se compone principalmente por discos, un cabezal de lectura, una controladora; los discos están enlazados mediante un eje

giratorio donde generalmente alcanza velocidades de 5200rpm o 7200rpm dependiendo del modelo, y sellado al vacío en una caja metálica. Operan en diferentes interfaces donde puede ser SATA, IDE, SCSI, entre otros y actualmente existe en el mercado tamaños que van desde gigabytes a terabytes inclusive llegando a unidades más altas.[7]

Algunas observaciones a tener en cuenta con relación a los componentes que contiene son:

- Todo disco puede incluir varios platos magnéticos dependiendo de la capacidad de almacenamiento, esto puede ser 2, 4 o hasta 7.
- Si el cabezal realiza la lectura de algún sector, el controlador realiza un test de errores y su posible corrección.
- Cada disco duro posee un espacio de almacenamiento reservado donde el usuario no puede acceder, contiene información relacionada con la unidad y la partición. Sin esta información automáticamente quedaría inutilizable.
- Como los platos que contiene la unidad son magnéticos, la información se almacena mediante señales autosincronizantes.

Existe algunos términos a tener en cuenta relacionados con el presente capítulo como son:

- **Bit:** Término relacionado con el almacenamiento de valores booleanos, verdadero/falso, o simplemente valores de 0 y 1.
- **Byte:** Posee un conjunto de 8 bits, con lo cual representa 256 estados distintos.
- **Clúster:** Su función es agrupar varios sectores en una sola unidad lógica, todo archivos se almacena en estos clústeres.
- **Sector:** Es la subdivisión de una pista, posee la capacidad de almacenar parte de la información privada. Cuatro sectores representa un clúster, la mayoría de los discos duros los sectores son de 512 Bytes cada uno.

8.1.2 Unidades de Estado Sólido SSD

Figura 8.2: Unidad de estado sólido

A diferencia de un disco duro magnético, las unidades de estado solido son dispositivos electrónicos basado en memorias flash NAND no volátil, no poseen partes mecánicas ni presenta tiempos de latencia de rotación. Utiliza un controlador con el fin de realizar varias tareas de lectura y escritura al mismo tiempo, haciendo que el dispositivo sea más resistente a fallos y mucho mas rápido.[7]

Algunas de sus características que se diferencia a los discos duros tradicionales:[18] [7]

- Interfaz del controlador: Permite que el dispositivo sea reconocido por el sistema operativo host.
- Interfaz NAND flash: Referente al diseño en la configuración de la memoria.
- Bus Host: Interfaz de los dispositivos SSS (Solid State Storage).
- Factor forma: Indica el tamaño y la proporción disponibles, como tarjetas o módulos de estado sólido.
- Memoria no volátil: Conectado directamente al bus de memoria en el sistema.
- Test SSS: Compara los SSS en busca de características en común.
- Tiempo de escritura y lectura baja.
- Bajo consumo de energía y temperatura.
- Libre de ruido por ausencia de partes mecánicas.
- Resistentes a golpes, caídas y vibraciones.

Si embargo existen algunas desventajas a tener en cuenta:

- Capacidad de almacenamiento.
- Costo por gigabyte sigue siendo alto.
- Tiempo de vida es mas corto que un disco tradicional.

TRIM

El comando TRIM ayuda al sistema operativo con información relacionada con el espacio disponible para su limpieza y reutilización en la unidad de estado sólido. Es decir, si el usuario borra algún archivo, el sistema operativo con este comando indicara a la unidad que dicho espacio está apto para ser borrado.

El comando TRIM trabajo en conjunto con la tecnología de recolección de basura evitando que el rendimiento de la unidad no se reduzca. Esta tecnología copia los datos en uso en un nuevo bloque y posterior a eso los elimina junto con los antiguos. El comando TRIM reduce el número de operaciones que genera la recolección, es así como logra que la unidad no se desgaste innecesariamente. [19]

8.1.3 Recuperación de datos

Si no se toman las medidas de respaldo adecuadas, la pérdida de datos será un problema frecuente, donde las personas e incluso organizaciones enteras perderán muchos recursos. Por tal motivo la recuperación de datos reduce el impacto causado.

Definición

Se entiende como recuperación de datos al proceso de obtención de todo los datos borrados de la unidad de almacenamiento ya sea por problemas de fabrica o error humano, utilizando métodos de restauración especializados. Una vez ejecutada la recuperación, entra el tema de la extracción de datos, que es el proceso de operaciones específicas orientadas en dispositivos de almacenamiento a través de métodos y tecnologías especiales. [20]

Funcionalidad

Durante el proceso se debe asegurar que la información obtenida sea completa o al menos la mayor parte, utilizando en todo momento técnicas y/o métodos diseñados para el procedimiento.

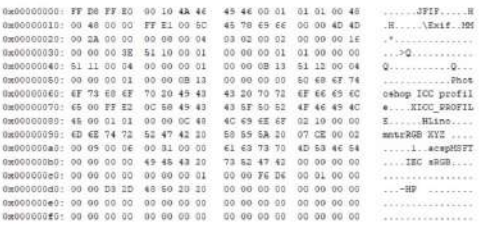
Algunos aspectos que influyen en la perdida de información son:[20]

- Motivación humana: Juega un papel determinante en el éxito del proceso de recuperación de datos, se convierte en evidencia forense con la posibilidad de argumentar mediante estas pruebas sobre un posible delito en la corte.
- Tipo de archivo: Cada archivo posee diferentes particularidades almacenados en un dispositivo con características específicas, por lo que si se usa un archivo de imagen como referencia, habrá etiquetas únicas que apunten al encabezado y pie del archivo.
- Tipo de fallo: Debido a una falla del sistema de archivos o sus componentes de hardware en un caso, el medio de almacenamiento puede sufrir daños lógicos y físicos.

Técnicas de recuperación de datos

- **Según el tipo de daño:** Todo daño o falla de los dispositivos de almacenamiento lleva a la necesidad de desarrollar algoritmos de recuperación, que a su vez producen tecnologías que eventualmente se convertirán en la base para el desarrollo de aplicaciones.
- **Según la fragmentación del archivo:** En la mayoría de los dispositivos de almacenamiento, los datos se almacenan de dos formas, guiando otros procesos como el acceso de lectura, modificación, eliminación y restauración.
  - Secuencial: Es decir, el cabeza de lectura y escritura busca un espacio disponible (clúster) y lo graba, pudiendo usar mas de un clúster dependiendo del tamaño de los datos.
  - Aleatorio: Similar al anterior punto, el cabezal buscar un clúster disponible y almacena los datos en ella. Si los datos no avanzan en este clúster, lo almacenará en otro, la diferencia es que no almacena de forma continua haciendo que los datos se fragmenten.
- **Según la integridad del sistema de archivos:** El sistema de archivos se encarga de la estructura de los datos en el dispositivo de almacenamiento, con ello el sistema operativo le resulta más fácil administrar la información independientemente del proceso que utiliza el archivo. La recuperación de datos sin un sistema de archivos o con con bajo rendimiento hará que este proceso sea difícil de realizar, para aliviar este problema la técnica File Carving se utiliza como uno de los recursos para respaldar el proceso de recuperación. [20]

8.2 File Carving



File Carving es una técnica forense utilizada en la recuperación de archivos, sin considerar ningún metadato en la estructura del sistema de archivos, toda técnica de Carving se utilizan en investigaciones forenses cuando se analiza el espacio no asignado de un sistema de archivos para extraer archivos. [21] En la actualidad, esta técnica genera copias de todo los archivos recuperados, haciendo que durante el proceso genere archivos basura. [22]

8.2.1 Clasificación

Esta técnica se clasifica de la siguiente manera: [18][20]

1. Basadas en las características del archivo.
   a) Header File
   Cuando exista la presencia de un identificador "Encabezado" ayuda a identificar el inicio de un archivo, lo restante se puede conocer haciendo un análisis de su estructura. Cabe mencionar que este identificador es único para cada archivo.
   b) Header-Footer File
   Cuando exista la presencia de un identificador "Encabezado" y "Pie/Fin", significa que el archivo posee un inicio y final, ese decir que, en dentro de este rango esta los bloques ocupados por el archivo a recuperar.

Extensión	Header	Footer / Tipo de Carving
jpg	FFD8	FFD9
gif	47494638	003B
png	89504E470D0A1A0A	49454E44
html	3C48544D4C3E	3C2F68746D6C3E
pdf	25504446	2525454F46
doc	D0CF11E0A1B11AE1	Estructura del archivo basado en Carving
ppt	-	-
xls	-	-
thumbs.db	-	-
zip	504B0304	-
bmp	424D	El tamaño del archivo se encuentra en el Header
avi	52494646	-
dat	-	-
mp4	66747670	Estructura del archivo basado en Carving
mov	-	-
3gp	-	-
wmv	3026B2758E66CF11	-

Cuadro 8.1: Header y Footer [23]

   c) File Structure and Block Content
   Se encarga en la restauración de archivos según su estructura y según su bloque de contenidos que disponga.
2. Basadas en la fragmentación del archivo.
   a) Fragmentation Issue
   Esta técnica va mas enfocado en archivos que se encuentren fragmentados, a diferencia de las técnicas previas, no posee identificadores que reconozcan los fragmentos.
   b) Predictive File
   Crea la metadata de todos los bloques obtenidos en la unidad de almacenamiento, utiliza de forma virtual un sistema de archivo para facilitar el acceso.
   c) Statistical Carving
   Reconstruye archivos en busca de similitudes.

8.2.2 Métricas de Carving

Durante el análisis de los archivos, se puede aplicar diversas métricas, estas a su vez ayudar con la evaluación y la calidad del resultado final. Las métricas son: [19] [18]

- Número de archivos recuperados
  Durante el proceso de extracción, el Carver genera un número definido de archivos.
- Número de archivos válidos
  Cantidad de archivos con contenido válido para el examinador, esto puede ser imágenes, documentos entre otros.
- Número de archivos recuperados de forma parcial
  Contiene todo archivo donde al menos tiene coherencia con el formato de archivo hasta donde la información esté dañada.
- Número de archivos no recuperados
  Todo archivos que durante el análisis no pudieron ser recuperados con la técnica de Carving.
- Número de falsos positivos
  De la cantidad de archivos analizados, cuantos presentan información no acorde al archivo, ya sea esto por falta de validación del mismo.
- Precisión de Carving
  Clasificación de todo los archivos recuperados, donde se especifica cuantos tienen información relevante o con información válida.

8.2.3 Herramientas

Una de las partes mas importantes para el análisis de archivos es conocer que herramientas resultan imprescindibles, en el mercado actual existen varias herramientas ya sean estas pagadas o gratuitas. Su enfoque van desde la recuperación de datos, análisis de memoria, recuperación de contraseñas, entre otras; cabe mencionar que la mayoría son multiplataforma, es decir, con soporte para Windows y/o Linux. [24] [25]

Algunas de estas herramientas son:

Nombre	Licencia	Plataforma	Enlace
HxD	Open Source	Windows	https://mh-nexus.de/en/hxd/
PhotoRec	Open Source	Multiplataforma	https://www.cgsecurity.org/wiki/PhotoRec
Scalpel	Open Source	Multiplataforma	https://sourceforge.net/projects/scalpel/
Autopsy	Open Source	Multiplataforma	https://www.autopsy.com/

Cuadro 8.2: Herramientas de recuperación de datos

8.2.4 Validación de archivos recuperados

Resulta importante saber como proceder con la tarea de evaluar los archivos recuperados mediante cualquier herramienta utilizada. Para ello es necesario conocer algunas observaciones con relación a este tema

Estas pueden ser: [21]

- Con un número limitado de archivos, existe la posibilidad de analizar uno a uno con algún programa adecuado. Sin embargo cuando exista un aumenta en el numero de archivos, resultará poco práctico aplicar este método.
- Existen casos donde la herramienta encargada de interpretar los archivos se vuelve inestable, esto sucede cuando encuentra un archivo corrupto haciendo que el análisis dure mas tiempo de lo normal o simplemente hace que la herramienta se cierre inesperadamente.

- Algunas herramientas poseen librerías que brindan soporte para una tarea en específico, a veces la información que otorga las herramientas con algunas librerías instaladas (con relación al estado de un archivo) no es clara, es decir, no especifica cual es el problema.
- La validación debe funcionar en archivos generados por un Carver, no debe presentarse excepciones o generar bucles.
- La validación brinda la facilidad de identificar posibles punto de fragmentación durante el análisis.
- Durante la validación se debería brindar las facilidades para identificar la estructura del archivo a analizar.

8.2.5 Niveles de validación

Los niveles de validación según Garfinkel son: [21]

- Header y Footer
  Se analiza si el procedimiento realizado por este método sea aplicado de forma correcta usando el formato adecuado.
- Por estructuras
  Se analiza la integridad y coherencia de los objetos, este nivel no procesa completamente la información.
- Por descompresión
  Mediante el uso de una herramientas se procede con la interpretación y procesamiento de datos, con el objetivo de verificar el cumplimiento del formato establecido con sus respectivas reglas.
- Por semántica
  Se analiza que la información tenga relación con el objeto, mediante el uso de analizadores semánticos.
- Humana
  Durante este nivel debe existir una persona encargada de evaluar los resultados y reconocer falsos positivos durante el proceso.

9. Documentación y reportes

Los examinadores deben informar de manera detallada y precisa cada hallazgo y los resultados que genere la revisión y el análisis de pruebas digitales, la documentación se lo debe realizar en todo el proceso del examen de manera continua. Es importante registrar con precisión los pasos dados durante el examen de la evidencia digital, además de poseer información comprensible, completo, precisos.

9.1 Apuntes del examinador

La documentación debe realizarse al mismo tiempo que el examen, todo reporte debe ser consistente con las políticas del departamento. Durante el proceso de documentación, se menciona algunas consideraciones que podría ayudar la examinador:

- Tome notas cuando consulte con el investigador y/o fiscal del caso.
- Las notas deben ser lo suficientemente detallada como para repetir la operación por completo.
- Conserve la solicitud inicial de ayuda con respecto al archivo del caso.
- Guarde una copia del documento que contenga la cadena de custodia.
- Registre el sistema operativo, las versiones de software importantes y los parches instalados actualmente.
- Registre cualquier novedad encontrada y detallar la medida tomada durante la inspección.
- Registre los cambios realizados en el sistema o la red, esto debe hacerlo la policía o el examinador.
- Incluya la fecha, hora, descripción y el resultado de las acciones tomadas en sus apuntes.
- Registre la información sobre la acceso remoto, ya sea este sobre el almacenamiento, el acceso de usuarios y la copia de seguridad externa recopilada en el sitio.
- Otro tipo de información puede incluir la topología de red, lista de usuarios autorizados y contraseña.

9.2 Reporte del examinador

Durante esta sección se mencionará algunas recomendaciones para la preparación de los informes que se enviarán a investigadores, fiscales, entre otros. Sin embargo, existen políticas departamentales que puedan otorgar detalles específicos sobre la redacción del informe, como el orden y el contenido del informe. La información del reporte puede incluir:

- La identidad de la organización informante.
- La identidad del remitente.
- Identificador de caso o número de registro.
- Fecha del reporte.
- Fecha de recepción.
- Caso a investigar.
- Id y firma del investigador.
- Generar una lista donde describa los artículos enviados a inspección, incluido el número de serie, la marca y el modelo.
- Describir los pasos tomados durante el examen, puede ser la búsqueda de cadenas, imágenes y la recuperación de archivos eliminados.
- Finalmente mencionar las conclusiones y recomendaciones.

X. Apéndice A. Glosario

analista forense Es un experto en informática forense con el conocimiento, las habilidades y la experiencia necesarios para ayudar en juicios y tribunales para resolver delitos cibernéticos.

Autopsy Conjunto de herramientas forenses dirigida al análisis y recuperación de información..

cadena de custodia Sistema de garantía basado en el principio de identidad y tiene como objetivo asegurar la autenticidad de las evidencias.

Data hiding Es un proceso que dificulta la búsqueda de datos y, al mismo tiempo, está disponible para su uso a futuro.

evidencia digital La evidencia digital es un registro de información almacenada o difundida a través de un sistema informático, que puede utilizarse como prueba en procedimientos judiciales.

file slack Es el espacio no utilizado entre el final del archivo y el final del último clúster asignado.

File Carving Es un proceso de extracción de un archivo de un dispositivo de almacenamiento, analizando su contenido de bloque, considerando las características específicas del formato de archivo e ignorando la estructura del sistema de archivos.

hash Es una función que utiliza algoritmos matemáticos para convertir un conjunto de datos en códigos alfanuméricos de longitud fija.

HPA Esta es un área del disco duro a la que los usuarios generalmente no pueden acceder. Su existencia no se informará al BIOS o al sistema operativo del host.

HxD Editor hexadecimal capaz de abrir archivos y leer sectores del disco duro..

PhotoRec Software de recuperación de datos utilizado en la recuperación de archivos perdidos en unidades de almacenamiento como discos duros, CD-ROM, pendrive..

Scalpel Software para recuperación de archivos utilizando File Carving, recupera y reconstruir archivos fragmentados después de formatear la unidad de almacenamiento, o si la información se encuentra corrompida o dañada..

sistemas embebidos Sistema electrónico que usa un procesador (similar a una computadora personal) para controlar un proceso específico.

SSS Siglas pertenecientes a Solid State Storage (Unidad de almacenamiento sólido).

timeframe Son planes de organización de la información en los que se considera parte del tiempo, que puede ser años, meses o días.

CADENA DE CUSTODIA

CADENA DE CUSTODIA DE EVIDENCIAS

N.º Caso:

Tipo de incidente:

Empresa afectada:

Dirección:

Teléfono:

Fecha y Hora: / / :

Investigador:

Observaciones:

LISTADO DE EVIDENCIAS

N.º Caso:

N.º. Página:

Cod. Evidencia	Cantidad	Descripción del articulo

EVIDENCIA DISCO DURO

EVIDENCIA DEL DISCO DURO

N.° Caso: _____

N.° Laboratorio: _____ N.° Control: _____

INFORMACIÓN DE LA UNIDAD			Sin información: ☐
Fabricante:		Cilindros:	
Modelo:		Cabezales:	
N.° Serie:		Sectores:	
Capacidad:		Ver. Controlador	
TIPO DE INTERFAZ			
IDE ☐	SATA ☐	USB ☐	Otro:

PARÁMETROS DE LA UNIDAD				
☐ Autopsy	☐ FTK Tools	☐ FDisk	☐ Testdisk	☐ Otros
Capacidad:		Sectores LBA:		
Sectores:		Capacidad con formato:		
Cilindros:		Etiqueta volumen:		
Cabezales:				

PARTICIONES				
NOMBRE	**UNIDAD DE ARRANQUE**	**INICIO**	**FIN**	**TIPO**
	☐			
	☐			
	☐			
	☐			
	☐			

ARCHIVO DE IMAGEN	
Método:	☐ Tar ☐ FTK Imager ☐ Alm. Directo Otros: _____ Comprimido ☐
Tipo de almacenamiento:	CD ☐ DVD ☐ HDD ☐
<<Papel de trabajo del archivo de imagen>>	

PLATAFORMA		
Sistema operativo:	☐ Windows ☐ Mac ☐ Unix Otros: _____ Versión: _____	
Software de análisis base:	☐ Autopsy ☐ Caine ☐ Herramientas DOS	
	Otros: _____ Versión: _____	
Copia de trabajo restaurada / imagen validada	☐ **Si**	☐ **No**

OTRAS HERRAMIENTAS UTILIDAZAS (Diferentes a las herramientas base)		
UTILIDAD	**VERSIÓN**	**FUNCIÓN**

ANÁLISIS DE EVENTOS		
ACTIVIDADES	**OBSERVACIONES**	**INICIALES**
Lista completa de archivos con metadatos		
Examinar sistema de archivos		
Recuperar y examinar el espacio libre / slack		
Examinar área de intercambio		
Eliminar / recuperar archivos eliminados		
Ejecutar programas según sea necesario		

EVIDENCIA EQUIPOS

EVIDENCIA DEL EQUIPO

N.° Caso: _____

N.° Laboratorio: _____ N.° Control: _____

INFORMACIÓN DEL EQUIPO					
Fabricante: _____	Tipo:	Desktop ☐	Portátil ☐	Otro: _____	
Modelo: _____	Estado:	Bueno ☐	Dañado ☐		
N.° Serie: _____	N.° HDD: _____				
Otros: _____		Lector CD/DVD ☐	Lector SD ☐	NIC ☐	
Apuntes del examinador: _____					

INFORMACIÓN CMOS				Automático ☐
Capacidad: _____		Cabezales: _____		
Cilindros: _____		Sectores: _____		
Modo:	LBA ☐	CHS ☐	Normal ☐	Auto ☐

OBSERVACIONES

XII. Apéndice D. Bibliografía

[1] Vázquez Juan Bernardo. «Arquitectura de computadoras I». En: *Red tercer milenio* (2012) (véanse páginas 8, 10).

[2] Dominick Rosato y Donald Rosato. «Computer-Aided Design». En: (2003) (véase página 9).

[3] Pérez Ana. «Las tarjetas inteligentes como herramienta innovadora en las ciudades». En: (2012) (véase página 10).

[4] Escobar Cortéz Medina. «Sistemas de seguridad basados en biometría». En: (2010) (véase página 10).

[5] Marín Antoni. «FOTOGRAFÍA DIGITAL: Manual de Uso y Recursos». En: (s.f) (véase página 11).

[6] Seth Misenar y Joshua Feldman Eric Conrad. «Chapter 8 - Domain 7: Telecommunications and network security». En: (2010) (véase página 11).

[7] Jorge Helí Espitia Ruiz y Wilmer Espitia Muñoz. «Análisis forense en discos duros magnéticos y de estado sólido». En: (2014) (véanse páginas 12, 36, 37).

[8] Dogan Ibrahim. «Enterprise Applications Administration. The Definitive Guide to Implementation and Operations». En: (2010) (véase página 13).

[9] Faircloth Jeremy. *SD Card Projects Using the PIC Microcontroller*. 2014 (véanse páginas 13, 14).

[10] Víctor Ortíz, Iridian Carrera, Jorge Gómez, Ruth Romero y María Hernández. «Servidor de Clonación y Restauración de particiones propuesta para la optimización del matenimiento de software de los laboratorios de informática de la UTFV». En: (2017) (véanse páginas 14, 15).

[11] Agustín Cernuda del Río y Daniel Gayo. «Informática General». En: (2006) (véase página 16).

[12] José Joskowicz. *Conceptos básicos de telefonía*. 2015 (véase página 17).

[13] Javier Luque. *Dispositivos y tecnologías wearables*. 2016 (véase página 17).

[14] Edison Llerena y Enrique Suárez. «Sistema de Navegación para Personas no Videntes, mediante el uso del Sistema de Posicionamiento Híbrido (GPS & GLONASS), para la Universidad de las Fuerzas Armadas ESPE». En: () (véase página 18).

[15] Asier Martínez. «Guía de toma de evidencias en entornos Windows». En: *INCIBE:Instituto Nacional de Ciberseguridad* (2014) (véase página 19).

[16] Ángel Amutio, Javier Candau y Otros. «Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información». En: (2012) (véase página 19).

[17] Eduardo Gómez-Luna, Diego Fernando-Navas, Guillermo Aponte-Mayor y Luis Andrés Betancourt-Buitrago. «Metodología para la revisión bibliográfica y la gestión de información de temas científicos, a través de su estructuración y sistematización». En: *Dyna* (2014) (véase página 21).

[18] G. Ninahualpa, C. Perez, S. G. Yoo, T. Guarda, J. Diaz y D. Piccirilli. «Restoring data in solid state devices damaged by crushing and falling, using file carving technique». En: (2018). DOI: 10.23919/CISTI.2018.8399344 (véanse páginas 37, 39, 40).

[19] Bruno Constanzo y Julian Waimann. «El estado actual de las Técnicas de File Carving y la necesidad de Nuevas Tecnologías que implementen Carving Inteligente». En: (2012) (véanse páginas 37, 40).

[20] Geovanni Ninahualpa Quina, Javier Díaz, Sang Guun Yoo Park y Darío Piccirilli. «Data restoration and file carving». En: (2017) (véanse páginas 37-39).

[21] Ana Haydée Di Iorio, Martín Alfredo Castellote, Bruno Constanzo, Hugo Curti, Julián Waimann, Sabrina Bibiana Lamperti, María Fernanda Giaccaglia, Pablo Adrián Cistoldi, Ariel Podestá, Juan Ignacio Iturriaga, Fernando Greco, Juan Ignacio Alberdi, Gonzalo M. Ruiz de Angeli, Santiago Trigo y Luciano Nuñez. «El rastro digital del delito: aspectos técnicos, legales y estratégicos de la Informática Forense». En: (2017) (véanse páginas 38, 40, 41).

[22] Golden Richard, Vassil Roussev y Lodovico Marziale. «In-place file carving». En: (2007) (véase página 38).

[23] Digambar Povar y VK Bhadran. «Forensic data carving». En: (2010) (véase página 39).

[24] Miguel López. «Análisis Forense Digital». En: (2007) (véase página 40).

[25] Jorge Helí Espitia Ruiz y Wilmer Espitia Muñoz. «Análisis forense en discos duros magnéticos y de estado sólido». En: (2014) (véase página 40).

ANEXO 2: ENCUESTA DE EVALUACIÓN

CUESTIONARIO DE EVALUACIÓN DE LA GUÍA DE RECUPERACIÓN DE DATOS EN ORDENADORES WINDOWS

El presente instrumento está diseñado para identificar la validez de la presente guía de recuperación de datos utilizando la técnica forense File Carving en ordenadores Windows, y la misma está dirigida a los peritos informáticos calificados por el Consejo de la Judicatura de Ecuador.

*Obligatorio

INSTRUCCIONES PARA COMPLETAR EL CUESTIONARIO

Se recomienda leer detenidamente cada pregunta antes de responder.

1) Se recomienda leer detenidamente cada pregunta antes de responder.
2) De un clic en la opción que corresponda.
3) Las preguntas tienen varias opciones de respuesta y le pedimos que señale la respuesta que considere que describe mejor su situación.
4) Para lograr un adecuado diagnóstico sobre la validez de la presente guía, es imprescindible que usted responda sinceramente.
5) Tenga presente que no existen respuestas correctas o incorrectas.
6) La aplicación total de la encuesta demora alrededor de 10 minutos.
7) Concéntrese mientras responda la encuesta, recuerde que lo que importa es su opinión respecto de los distintos temas.

Esta encuesta es parte de una investigación con fines académicos.

SECCIÓN GENERAL DATOS SOCIODEMOGRÁFICOS DE LOS PERITOS INFORMÁTICOS CALIFICADOS POR EL CONSEJO DE LA JUDICATURA DE ECUADOR

1. Fecha *

Ejemplo: 7 de enero del 2019

2. Antigüedad, años de experiencia dentro de la empresa o institución: * *Marca solo un óvalo.*

- Menos de 1 año
- De 1 a 5 años
- Más de 5 a 10 años
- Más de 10 a 15 años
- Más de 15 años

3. Antigüedad dentro del puesto o cargo actual: * *Marca solo un óvalo.*

- Menos de 1 año
- De 1 a 5 años
- Más de 5 a 10 años
- Más de 10 a 15 años
- Más de 15 años

SECCIÓN ESPECÍFICA DE VALIDEZ DE LA GUÍA

4. ¿La guía indica como preservar la autenticidad e integridad de los medios probatorios? * *Marca solo un óvalo.*

	1	2	3	
No cumple				Cumple totalmente

5. ¿Explica la guía la cadena de custodia que seguirán los medios para garantizar que no se han modificado durante la pericia? * *Marca solo un óvalo.*

	1	2	3	
No cumple				Cumple totalmente

6. ¿La guía indica los pasos a seguir durante el procedimiento pericial? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

7. ¿Enuncia la guía las técnicas forenses que se emplearán para el análisis, valoración, recuperación y preservación de la información digital almacenada en dispositivos o sistemas informáticos? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

8. ¿Indica la guía los pasos a seguir durante la recolección de datos en tiempo real con técnicas digitales forenses, de equipos tecnológicos que formen parte de la infraestructura crítica del sector público o privado y explica la cadena de custodia? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

9. ¿Indica la guía como preservar la integridad del contenido digital cuando este se encuentre almacenado en medios no volátiles? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

10. ¿Ayuda la guía a identificar e inventariar cada objeto individualmente durante una investigación, cumpliendo los requerimientos estipulados en el Art. 500 del COIP? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

11. ¿La guía menciona la importancia de la confidencialidad durante la obtención de la información? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

12. ¿La guía menciona la importancia de la integridad de la información obtenida y aclara quienes tienen derecho a cambiarla si es necesario? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

13. ¿Aclara la guía la importancia de la disponibilidad de la información obtenida durante un proceso pericial, para usuarios con acceso autorizado? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

ANEXO 3: ENCUESTA DE COMPROBACIÓN

CUESTIONARIO DE EVALUACIÓN DE LA GUÍA DE RECUPERACIÓN DE DATOS EN ORDENADORES WINDOWS

El presente instrumento está diseñado para identificar la validez de la presente guía de recuperación de datos utilizando la técnica forense File Carving en ordenadores Windows, y la misma está dirigida a los peritos informáticos calificados por el Consejo de la Judicatura de Ecuador.

*Obligatorio

INSTRUCCIONES PARA COMPLETAR EL CUESTIONARIO

Se recomienda leer detenidamente cada pregunta antes de responder.

1) Se recomienda leer detenidamente cada pregunta antes de responder.
2) De un clic en la opción que corresponda.
3) Las preguntas tienen varias opciones de respuesta y le pedimos que señale la respuesta que considere que describe mejor su situación.
4) Para lograr un adecuado diagnóstico sobre la validez de la presente guía, es imprescindible que usted responda sinceramente.
5) Tenga presente que no existen respuestas correctas o incorrectas.
6) La aplicación total de la encuesta demora alrededor de 10 minutos.
7) Concéntrese mientras responda la encuesta, recuerde que lo que importa es su opinión respecto de los distintos temas.

Esta encuesta es parte de una investigación con fines académicos.

SECCIÓN ESPECÍFICA DEL PORCENTAJE DE RECUPERACIÓN

Elige una sola respuesta para cada una de las siguientes preguntas. Responda todas las preguntas. Encierre alrededor del número correspondiente a su respuesta

1. ¿Considera que la guía menciona buenas prácticas a seguir con relación a la seguridad de la información? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

2. ¿Considera que esta guía menciona directrices a seguir durante la integridad de datos, necesarios para el caso de estudio? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

3. ¿Cree que esta guía influye de manera positiva en la recuperación de archivos de manera eficaz ayudando al caso de estudio? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

4. ¿Cree que esta guía menciona sobre la confiabilidad de la información y su aplicación para el caso de estudio? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

5. ¿Considera que la recuperación de datos aplicando técnicas forenses tiene un grado aceptable en la obtención de la información perdida? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

6. ¿Considera que la obtención de datos es de relevancia para una investigación y así tener un informe forense estructurado? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

7. ¿Considera que la guía tiene un grado de importancia durante de recuperación de datos? *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

SECCIÓN ESPECÍFICA DEL TIEMPO DE RECUPERACIÓN

Elige una sola respuesta para cada una de las siguientes preguntas. Responda todas las preguntas. Encierre alrededor del número correspondiente a su respuesta.

8. ¿Considera que el tiempo empleado durante la recuperación de la información en el caso de estudio se redujo utilizando la guía? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

9. ¿Considera que el proceso de documentación presentado en el caso de estudio reduce el tiempo de recolección de datos forenses con la utilización de la guía? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

10. ¿Considera que se redujo el tiempo empleado durante el proceso de análisis presentado en el caso de estudio con la ayuda de la guía? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

11. ¿Considera que se redujo el tiempo utilizado durante el proceso de transporte de la información aplicando la guía? * *Marca solo un óvalo.*

1	2	3

No cumple	◯	◯	◯	Cumple totalmente

12. ¿Considera que se redujo el tiempo utilizado en el análisis de evidencias de la información aplicando la guía? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

13. ¿Considera que se redujo el tiempo utilizado durante el reporte de datos aplicando la guía? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

CONSIDERACIONES GENERALES

Elige una sola respuesta para cada una de las siguientes preguntas. Responda todas las preguntas. Encierre alrededor del número correspondiente a su respuesta

14. ¿Considera que la guía utilizada es eficiente y eficaz dentro del área relacionada al peritaje en el país? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

15. ¿Considera que es viable la aplicación de esta guía dentro de la legislación ecuatoriana en comparación con otras guías que conozca? * *Marca solo un óvalo.*

	1	2	3	
No cumple	◯	◯	◯	Cumple totalmente

ANEXO 4: CASO DE ESTUDIO

CASO DE ESTUDIO: EJEMPLO PRÁCTICO

OBSERVACIÓN: El escenario planteado es solo para fines de instrucción y cualquier asociación con un caso real y un litigio es pura coincidencia. Cada nombre y ubicación presentado en este caso de estudio es ficticio y no tienen la intención de reflejar personas reales o lugares. La información y las declaraciones no se utilizarán con fines publicitarios.

RESUMEN BREVE DEL CASO

Un ciudadano preocupado se comunicó con el departamento de policía con respecto a un posible robo de propiedad. Le dijo a la policía que mientras buscaba en Internet, con la esperanza de encontrar un auto con buenas características, finalmente encontró uno que cumplía con sus expectativas. Este anuncio incluía un auto marca Chevrolet a bajo precio, por lo que se comunicó con el vendedor, al encontrarse con este, sospechó que dicho auto había sido robado. Después de escuchar esta información, la policía alertó a la Fiscalía especializada en Patrimonio Ciudadano. La Fiscalía en conjunto con la policía realizó una operación encubierta para comprar el auto. Los agentes encubiertos se reunieron con el sospechoso, quien, después de recibir el pago, les proporcionó el vehículo, un título de propiedad y una tarjeta de seguro. El sospechoso fue arrestado y el vehículo que conducía fue registrado en durante su arresto. Durante el registro, se incautó una computadora portátil. Aunque los documentos proporcionados por el sospechoso parecían auténticos, los examinadores de documentos determinaron que los documentos eran falsos. El investigador de robo de automóviles se comunicó con el laboratorio forense informático para obtener ayuda para examinar la computadora incautada. El investigador obtuvo una orden de allanamiento para analizar la computadora y buscar materiales usados en la elaboración de documentos falsificados y otras pruebas relacionadas con los cargos de robo de automóviles. La computadora portátil se envió al laboratorio forense informático para su análisis.

Objetivo: Determinar si el sospechoso usó la computadora portátil como instrumento de los delitos de robo de autos, fraude, falsificación, emisión de documentos falsos y posesión de títulos de vehículos falsificados y/o como depósito de datos relacionados con esos delitos.

Tipo de ordenador: Portátil Lenovo IdeaPad S340-IWL
Sistema Operativo: Microsoft® Windows 10
Cargos: Robo de auto, Fraude, Falsificación, Portar documentos falsos y Posesión de títulos de vehículos falsos.
Agente del caso: Investigador de la unidad de Patrimonio Ciudadano
Lugar de la examinación: Laboratorio de informática forense
Herramientas usadas: Guía de recuperación de datos en ordenadores Windows, PhotoRec, Autopsy.

Procedimiento

Evaluación

1. Se revisó la documentación proporcionada por el investigador.
    a. La autorización legal se estableció mediante una orden de registro obtenida específicamente para el examen de la computadora en un laboratorio.
    b. La cadena de custodia fue documentada apropiadamente utilizando el formato definido.
    c. La solicitud de servicio y resumen detallado fueron explicados durante la investigación, indicando palabras clave y la información del sospechoso, vehículo robado, documentos falsificados y la publicidad hecha por internet. De igual forma se incluyeron fotos de los documentos falsificados.
2. Se realizó una reunión entre el investigador forense y el agente del caso, se analizó vías de investigación posibles, pruebas que se busquen en la investigación.
3. Se completó con la recolección de pruebas.
    a. La evidencia fue marcada y fotografiada

b. Un archivo fue creado y la información del caso fue registrado en la base de datos del laboratorio.

c. La computadora se almacenó en la sala de propiedad del laboratorio.

4. El caso fue asignado al investigador forense

Recolección

1. La portátil fue examinada y fotografiada

   a. El hardware fue examinado y documentado.

   b. La portátil fue encendida y se accedió a la configuración de la BIOS, todo esto fue documentado, la hora del sistema fue comparado con una hora de una fuente de confianza y registrada. La secuencia de arranque fue revisada y documentada.

   c. La portátil se apagó sin hacer algún cambio en la BIOS.

2. Autopsy® fue usado para crear un archivo de evidencia que contenga la imagen del disco duro de la portátil.

   a. La portátil fue conectada en el laboratorio de computación a través de una conexión USB.

   b. Se inició la portátil con un disco de arranque y se empezó con la utilización de Autopsy®.

   c. La evidencia fue adquirida mediante dicha herramienta y almacenada en discos compactos.

   d. Una vez completado el proceso de imagen, se apagó la portátil.

      i. La portátil fue devuelta al laboratorio.

      ii. El disco compacto contiene la evidencia obtenida mediante Autopsy®, donde fue protegida contra escritura y presentado como prueba.

Análisis

1. Se preparó un laboratorio de cómputo con Windows® 10, Autopsy® para Windows y otros programas forenses.
2. Las evidencias obtenidas de Autopsy® en la portátil fueron copiadas al disco duro del laboratorio.
3. Un nuevo archivo de caso fue abierto en Autopsy®, los archivos de evidencias fueron analizados con esta herramienta.
    a. Se recuperaron archivos borrados mediante la herramienta mencionada
    b. Datos de archivos incluyendo nombres, fechas y horas, tamaño físico y lógico, y la ruta fueron recuperados.
    c. Los datos de archivos fueron abiertos y revisados; se localizaron archivos protegidos con contraseña y encriptados.
    d. Se buscó espacio no asignado y file slack.
    e. Los archivos de interés para la investigación se copiaron y/o eliminaron del archivo de pruebas de Autopsy® y se copiaron en un disco compacto.
4. Los clústeres no asignados se copiaron y/o eliminaron del archivo de evidencia de Autopsy® y enviado a un disco duro en blanco. Luego, se utilizó PhotoRec© para la obtención de imágenes por Carver de espacios no asignados. Las imágenes por Carver de PhotoRec©, se abrieron y se visualizaron. Se extrajeron un total de 8.476 imágenes.

Hallazgos

El análisis de la computadora portátil resultó en la recuperación de 176 archivos de valor probatorio o interés investigativo. Los archivos recuperados incluyen:

1. 59 documentos que contienen el nombre del sospechoso y su información personal; texto incluido en los documentos falsificados; cheques corporativos y certificados escaneados; texto describiendo artículos robados y del auto recuperado.
2. 38 imágenes de alta resolución que representan roles de pago corporativos y cheques certificados en moneda americana; títulos de vehículos, tarjetas de

registro y licencias de conducir; tarjetas de seguros de diversas empresas; y cheques falsificados dirigidos a una empresa de informática que oscilan entre $ 25 000 y $ 40 000 para la compra de ordenadores portátiles. Se escanearon la mayoría de los gráficos.

3. 63 archivos en HTML que incluyen el correo electrónico de Outlook® y Gmail®, anuncios clasificados del auto recuperado, otros vehículos y varias marcas de computadoras portátiles; texto de correo electrónico entre el sospechoso y el ciudadano con relación a la venta del auto recuperado; y correos electrónicos entre el sospechoso y una empresa de informática sobre la compra de ordenadores portátiles.
4. 14 gráficos obtenidos por Carver del espacio no asignado representado en diversos controles durante las etapas de finalización, incluye imágenes escaneadas de la moneda estadounidense.

Documentación

1. **Informe forense**: Todas las acciones, procesos y hallazgos se describieron en un informe forense detallado, que se mantiene en el expediente del laboratorio.
2. **Informe policial**: El agente del caso recibió un informe policial que describía las pruebas examinadas, las técnicas utilizadas y los hallazgos.
3. **Producto de trabajo**: Se usó un disco compacto que contiene archivos y datos de valor probatorio o de interés para la investigación. El original se guardó en el expediente del laboratorio. Se proporcionaron copias al agente del caso y al fiscal.

Resumen

Por medio de la información revelada durante el análisis informático, se abrieron varias nuevas vías de investigación.

- El contacto con la compañía de computadoras reveló que los cheques falsificados encontrados en la computadora del sospechoso habían sido aceptados para la compra de computadoras y enviado a esta persona, razón por la cual fueron objeto de la investigación en curso. Los números de serie y modelo proporcionados por la compañía de computadoras coincidían con varios de los anuncios clasificados de Outlook® y Gmail® que se encuentran en la computadora del sospechoso.

- La información obtenida sobre otros vehículos dio lugar a la recuperación de vehículos robados adicionales.

Conclusión

El sospechoso finalmente se declara culpable y ahora está encarcelado.

ANEXO 5: GUÍAS USADAS DURANTE LA INVESTIGACIÓN

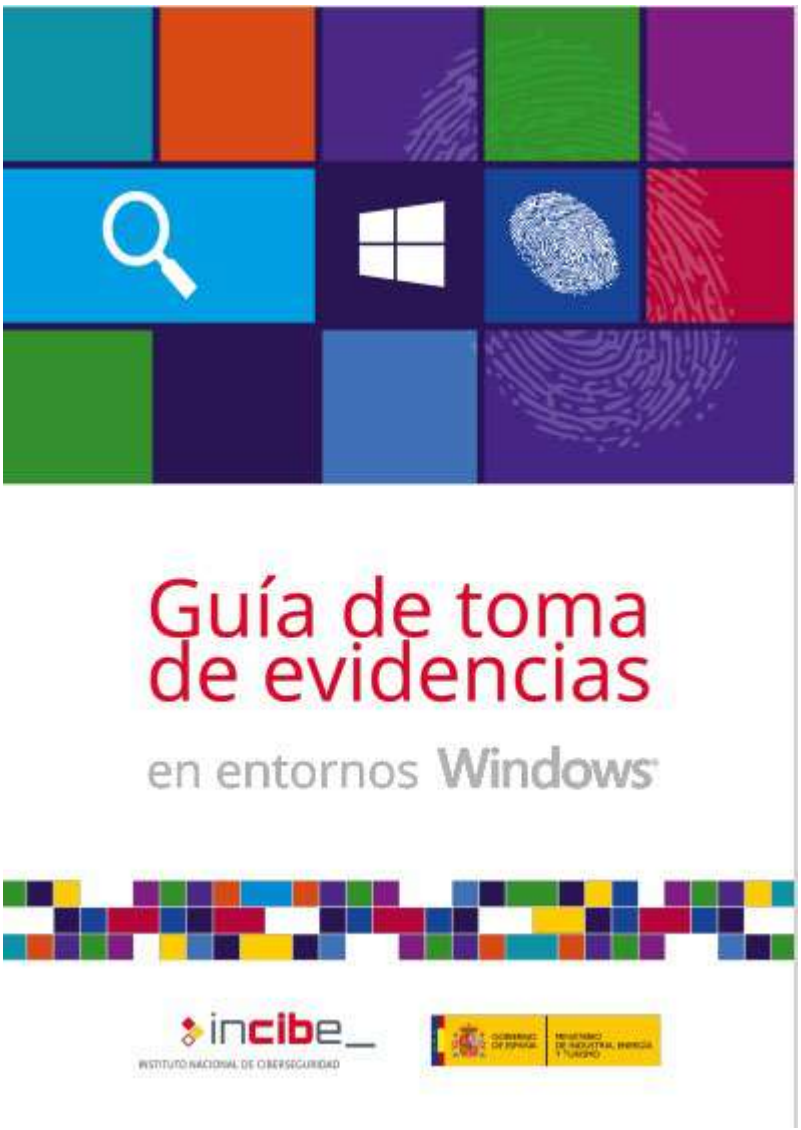


Figura 40: Guía 1
Fuente: Instituto Nacional de Ciberseguridad

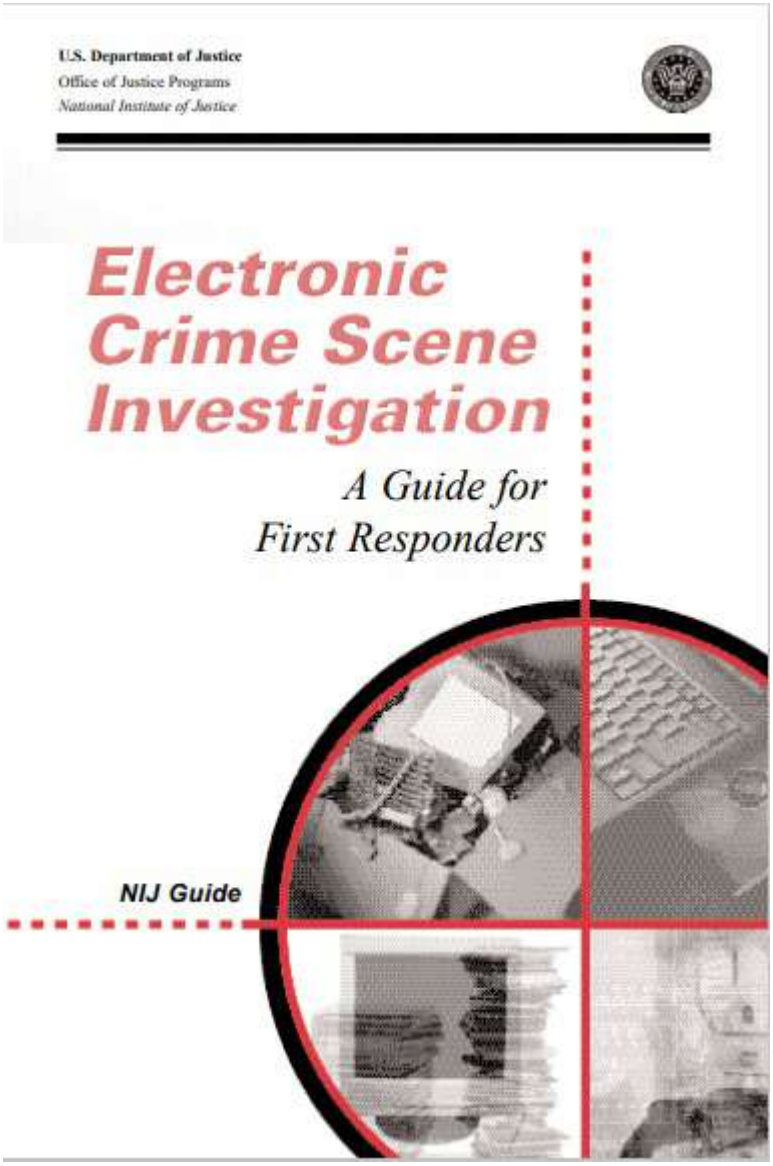


Figura 41: Guía 2
Fuente: Departamento de justicia de EE. UU

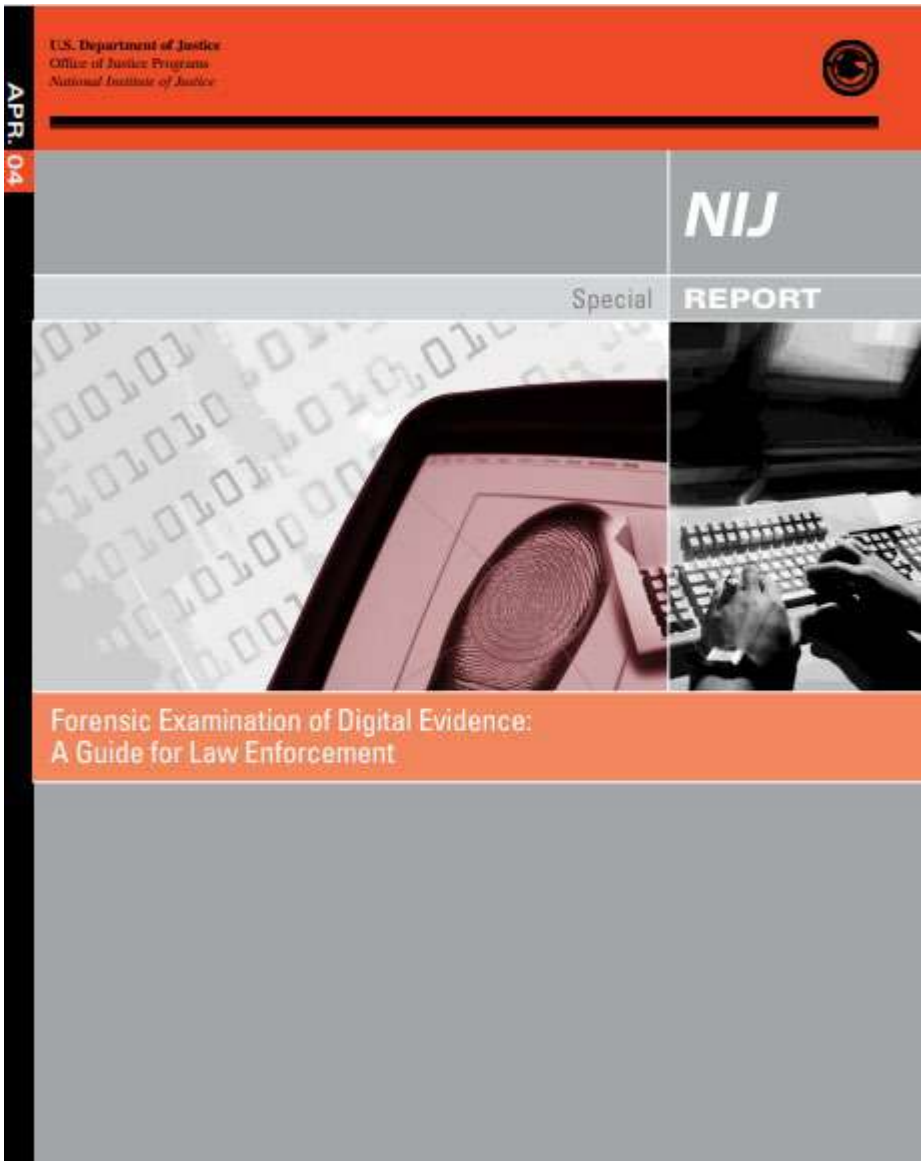


Figura 42: Guía 3
Fuente: Departamento de justicia de EE. UU