

Peritaje informático en casos prácticos conforme a las normas ISO/IEC 27037:2012 e ISO/IEC 27042:2015

Computer forensics in practical cases according to ISO/IEC 27037:2012 and ISO/IEC 27042:2015

ALVAREZ, Ivanna P.¹

LOJA, Nancy M.²

OCHOA, Heckler R.³

Resumen

Este artículo examina la aplicación del peritaje informático en casos reales, conforme a las normas ISO/IEC 27037:2012 y 27042:2015. Se describe un enfoque metodológico estructurado para la identificación, adquisición, preservación y análisis de evidencia digital. Los hallazgos incluyen la recuperación de archivos eliminados, el análisis de memoria RAM y la detección de un programa oculto tipo keylogger, lo que evidencia la efectividad de las herramientas forenses aplicadas en entornos de investigación digital.

Palabras clave: evidencia digital, peritaje informático, ISO/IEC 27037:2012, herramientas forenses

Abstract

This article examines the application of computer forensics in real cases, following the ISO/IEC 27037:2012 and 27042:2015 standards. It presents a structured methodological approach for identifying, acquiring, preserving, and analyzing digital evidence. Findings include the recovery of deleted files, RAM memory analysis, and the detection of a hidden keylogger program, demonstrating the effectiveness of forensic tools in digital investigation environments.

Key words: evidence digital, computer expertise, ISO/IEC 27037:2012, forensic tools

1. Introducción

En el entorno actual, marcado por la globalización de los datos y el acelerado avance tecnológico, se han desarrollado múltiples plataformas digitales que facilitan la comunicación, el almacenamiento y la gestión de información. No obstante, este mismo progreso ha propiciado un crecimiento paralelo de los delitos informáticos, como el fraude electrónico, la ciberextorsión y el acceso no autorizado a sistemas. En este contexto, la evidencia digital se ha convertido en un componente esencial dentro de los procesos de investigación forense. La naturaleza volátil de la evidencia digital, junto con su susceptibilidad a alteraciones, exige el uso de metodologías forenses estructuradas que aseguren su integridad, autenticidad y trazabilidad. En respuesta a esta necesidad, surge el peritaje informático, una disciplina que se encarga de la identificación, adquisición, preservación y análisis de información digital vinculada a actos ilícitos, garantizando su utilidad y admisibilidad en procesos judiciales (Cañarte Rodríguez y otros, 2022).

¹ Estudiante de Ingeniería en Tecnologías de la Información. Universidad Técnica de Machala. Machala, Ecuador. Correo electrónico: ivanna.alvarez@utmachala.edu

² Profesora de la Universidad Técnica de Machala. Machala, Ecuador. Correo electrónico: nmloja@utmachala.edu.ec

³ Perito informático. Independiente, Ecuador. Correo electrónico: heckler.rothwell@gmail.com

Para regular estas actividades, se han adoptado normativas internacionales como la ISO/IEC 27037:2012, que proporciona directrices específicas para la identificación, recolección, adquisición y preservación de la evidencia digital (International Organization for Standardization; International Electrotechnical Commission, 2012). Esta norma también define roles clave dentro del procedimiento, como el Digital Evidence First Responder (DEFR) y el Digital Evidence Specialist (DES), quienes intervienen según el entorno y tipo de incidente (Gómez, 2018). La correcta aplicación de estos lineamientos resulta fundamental para evitar manipulaciones indebidas y asegurar que la evidencia recolectada mantenga su validez jurídica.

No obstante, esta norma por sí sola no cubre la totalidad del proceso forense. Mientras la ISO/IEC 27037:2012 regula las fases iniciales de la gestión de la evidencia desde su identificación hasta su conservación, la norma ISO/IEC 27042:2015 amplía este marco al proporcionar directrices específicas para el análisis técnico y contextual de los datos recolectados. En este sentido, ambas normativas deben entenderse como complementarias dentro de un flujo metodológico integral: una garantiza que la información digital sea recolectada bajo criterios de fiabilidad técnica, y la otra que sea interpretada de manera rigurosa y forense. Como afirman Coronel Rojas et al., (2020), este enfoque dual resulta fundamental para asegurar la coherencia del proceso pericial, especialmente cuando la evidencia digital sirve de soporte para la formulación de hipótesis investigativas y decisiones judiciales.

Con el propósito de analizar la aplicabilidad del peritaje informático en escenarios reales, este estudio examina distintos casos prácticos relacionados con delitos informáticos, incluyendo la explotación de una computadora portátil y la intervención ante un incidente de seguridad en un entorno de red institucional. A través del análisis de estos casos se busca demostrar cómo la aplicación adecuada de metodologías forenses puede contribuir a la recolección técnica y legalmente válida de evidencia digital, incluso en contextos con limitaciones operativas.

Diversas investigaciones han respaldado la importancia de emplear protocolos formales en el tratamiento de evidencia digital, ya que estos mejoran su trazabilidad y admisibilidad en procesos judiciales (Proaño Escalante & Gavilanes-Molina, 2018). Sin embargo, en América Latina persisten limitaciones estructurales para su implementación, debido a la falta de infraestructura tecnológica adecuada y la escasez de personal capacitado (Banegas Crespo y Andrade Pesantez, 2024). En el caso de Ecuador, se han reportado cifras preocupantes: entre enero y septiembre de 2023, la Policía Nacional registró 5.930 denuncias por extorsión, de las cuales el 57% correspondieron a la modalidad de extorsión virtual, donde se emplearon medios digitales para chantajear a las víctimas (La Hora, 2023; Primicias, 2023).

Frente a este panorama, surgen interrogantes fundamentales: ¿cómo aplicar correctamente el peritaje informático en contextos reales para asegurar la validez de la evidencia digital recolectada?, y ¿qué criterios permiten seleccionar herramientas adecuadas para cada entorno técnico y judicial?

En este sentido, el propósito de este estudio es analizar la aplicación del peritaje informático en casos prácticos, evaluando su efectividad en la identificación, adquisición, preservación y análisis de evidencia digital. Se busca además sustentar técnicamente la selección de herramientas especializadas que permitan actuar con precisión ante diferentes incidentes relacionados con delitos informáticos, garantizando la trazabilidad y validez legal del proceso.

El documento se estructura en tres secciones centrales. En primer lugar, se detalla la metodología adoptada, fundamentada en las normas ISO/IEC 27037:2012 e ISO/IEC 27042:2015, explicando las herramientas y criterios empleados. Posteriormente, se describen los casos prácticos desarrollados, en los que se evidencia la aplicación de principios forenses y la eficacia de los procedimientos utilizados. Finalmente, se presentan las conclusiones generales y específicas del estudio, destacando los hallazgos más relevantes y su aporte a la consolidación de buenas prácticas en informática forense.

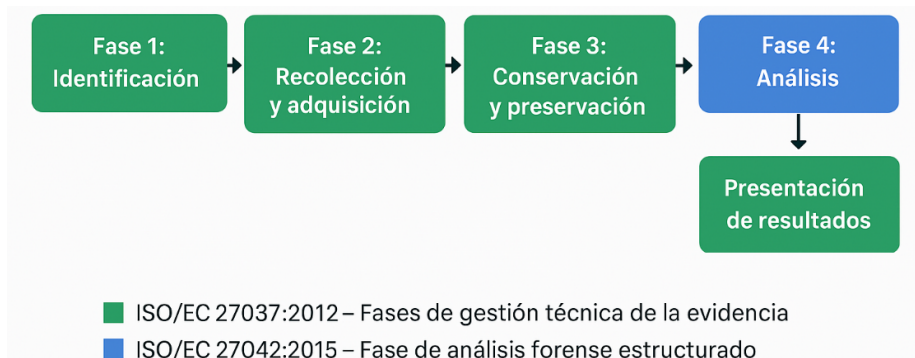
2. Metodología

El presente estudio se enmarca en la aplicación del peritaje informático en varios casos prácticos, desarrollados conforme a los lineamientos de las normas ISO/IEC 27037:2012 e ISO/IEC 27042:2015, las cuales establecen un marco integral para regular los procesos de identificación, adquisición, preservación y análisis de evidencia digital en contextos judiciales. La metodología utilizada tiene como objetivo asegurar la trazabilidad, integridad y validez de la información obtenida desde dispositivos electrónicos vinculados a presuntos actos ilícitos, permitiendo su uso como prueba en procesos legales.

Para visualizar el enfoque metodológico aplicado, en la Figura 1 se presenta un esquema secuencial que resume las fases del procedimiento pericial conforme a los estándares internacionales. Las actividades representadas en color verde corresponden a las fases cubiertas por la ISO/IEC 27037:2012, orientadas a la gestión técnica de la evidencia digital, incluyendo la identificación, adquisición y preservación. El componente en color azul representa el análisis de la evidencia, que puede abordarse de dos formas complementarias.

En primer lugar, la propia ISO/IEC 27037:2012, en su cláusula 7, permite realizar un análisis básico de la evidencia digital, siempre que este se desarrolle con herramientas forenses adecuadas y siguiendo principios que aseguren la trazabilidad y validez de los datos obtenidos. No obstante, cuando se requiere una evaluación más profunda o interpretativa de la información, se recurre a la ISO/IEC 27042:2015, la cual establece directrices específicas para el análisis estructurado y contextualizado en entornos forenses.

Figura 1
Esquema de actuación pericial bajo los estándares ISO/IEC 27037:2012 y 27042:2015



Fuente: Archivo de los autores

Según (Banegas Crespo y Andrade Pesantez, 2024), la norma ISO/IEC 27037:2012 presenta una cobertura más amplia y actualizada en comparación con otras normativas internacionales como NIST SP 800-86, ISO/IEC 27041, 27042, 27043, y los RFC 4998 y 6283. A diferencia de estas, que abordan aspectos parciales del proceso forense, la 27037 ofrece un marco metodológico que abarca de forma holística las fases críticas de tratamiento de evidencia digital, asegurando su correcta gestión técnica y legal a lo largo del proceso investigativo.

En concordancia con esta normativa, la ejecución del peritaje informático en este estudio fue dividida en cuatro fases principales, respaldadas por la literatura forense y las buenas prácticas internacionales, las cuales se describen a continuación.

2.1. Fase 1: Identificación de la evidencia digital

Esta etapa implica la localización, reconocimiento y documentación de los elementos de prueba digital en sus dos dimensiones: física (como discos duros o dispositivos USB) y lógica (como archivos del sistema, logs, configuraciones o registros en aplicaciones). De acuerdo con Proaño Escalante & Gavilanes-Molina, (2018), un proceso riguroso de identificación asegura la trazabilidad de la información y su vinculación con los hechos investigados. La ISO/IEC 27037:2012, en su cláusula 5.3, enfatiza que esta fase es crítica para garantizar la autenticidad de la evidencia y su validez posterior en entornos forenses. (Coronel Rojas et al., 2020)

2.2. Fase 2: Recolección y adquisición de la evidencia digital

Una vez identificada la evidencia, se procede a su adquisición utilizando herramientas forenses que aseguren la no alteración de los datos originales (Coronel Rojas y otros, 2020). Estas técnicas incluyen la clonación bit a bit, la extracción de memoria RAM y la verificación de integridad mediante funciones hash (MD5, SHA-256). Según la ISO/IEC 27037:2012, durante esta fase es esencial emplear métodos que minimicen cualquier riesgo de corrupción o pérdida de datos, permitiendo que la evidencia sea admisible en procedimientos judiciales (International Organization for Standardization; International Electrotechnical Commission, 2012).

2.3. Fase 3: Conservación y preservación de la evidencia digital

La preservación de la evidencia digital tiene como objetivo protegerla contra manipulaciones no autorizadas, fallos técnicos o accesos indebidos. Esta fase incluye el uso de dispositivos de almacenamiento seguros, bloqueadores de escritura, empaques antiestáticos y bitácoras que mantengan el control de la cadena de custodia. Además, toda la información recolectada debe estar debidamente documentada y etiquetada, conforme a lo dispuesto en la cláusula 6.5 de la norma 27037 (International Organization for Standardization; International Electrotechnical Commission, 2012).

2.4. Fase 4: Análisis de la evidencia digital (ISO/IEC 27042:2015)

Cuando la intervención del perito incluye la interpretación técnica de los datos recolectados, se aplica la norma ISO/IEC 27042:2015, que proporciona directrices para el análisis estructurado y contextual de evidencia digital. Esta fase abarca tareas como la reconstrucción de cronologías, el análisis de metadatos, la recuperación de archivos eliminados y la detección de patrones de uso, con el fin de sustentar hipótesis investigativas de manera técnica y coherente (Melán Angel, 2022). A diferencia de las fases previas, esta etapa no se aplica de forma general, sino únicamente cuando la autoridad competente solicita un análisis especializado que complemente la recolección técnica de datos con una valoración forense detallada.

Esta estructura metodológica no solo permite estandarizar las actuaciones periciales en distintos contextos digitales, sino que también sienta las bases técnicas para su aplicación flexible en escenarios reales. Para comprobar la aplicabilidad de la metodología propuesta, se desarrollaron casos prácticos reales en los que se aplicó el peritaje informático conforme a las normas ISO/IEC 27037:2012 e ISO/IEC 27042:2015. Cada caso corresponde a un escenario distinto vinculado a incidentes digitales y permite demostrar cómo se llevan a cabo los procesos de identificación, adquisición, preservación y análisis de evidencia digital, así como la selección fundamentada de herramientas forenses según las características técnicas y requerimientos específicos del entorno analizado.

2.5. Casos prácticos

2.5.1. Caso 1: Explotación de computadora portátil HP mediante peritaje informático

Este caso surge de un requerimiento judicial emitido por una unidad fiscal del sur del Ecuador, en el marco de una investigación por un presunto delito. El dispositivo analizado fue una computadora portátil marca HP, modelo 550, serie CNU8331K68X13-42879, considerada evidencia clave por contener posibles registros de comunicación, archivos recientes y actividad del usuario relevante para el proceso investigativo.

El peritaje tuvo como objetivo la extracción técnica de información desde el sistema operativo y aplicaciones como WhatsApp, Messenger y Facebook, así como la recuperación de documentos eliminados. Entre los archivos de interés se identificó un documento denominado DENUNCIA.docx, cuya recuperación parcial fue priorizada por su posible relación con los hechos denunciados.

El procedimiento se ejecutó conforme a los lineamientos establecidos en la norma ISO/IEC 27037:2012, y para el análisis de la evidencia recuperada se complementó con los criterios definidos por la ISO/IEC 27042:2015 (International Organization for Standardization; International Electrotechnical Commission, 2015), los cuales orientan la interpretación técnica y contextual de los datos digitales.

Para ello, se seleccionaron herramientas forenses específicas que respondieran a los requerimientos técnicos del caso, priorizando su compatibilidad, confiabilidad y validación en entornos judiciales. Como lo señalan (Hidalgo Cajo et al., 2018), la eficacia del peritaje informático depende no solo del rigor metodológico, sino también de la idoneidad de las herramientas utilizadas, ya que la calidad de la evidencia digital recolectada puede incidir directamente en su valor legal y en la agilidad para resolver un caso. Por ello, se evaluaron alternativas funcionales disponibles, descartando aquellas cuya complejidad, licencia comercial o limitaciones técnicas no se ajustaban al contexto operativo. La siguiente tabla resume los materiales utilizados y las herramientas comparadas, junto con sus funciones principales:

Cuadro 1

Comparación de herramientas para el análisis forense de equipo informático

Tipo de herramienta	Herramientas	Descripción	Sistema Operativo	Formato de salida	Licencia
Clonación/adquisición de disco	FTK Imager Lite 3.1.1	Creación de imágenes forenses bit a bit del disco con generación de hash.	Windows	E01, DD, AFF, RAW	Gratuita
	X-Ways Forensics	Clonación y análisis avanzado de discos, orientado a entornos profesionales.	Windows XP/2003/Vista/7/8/10/11	DD, RAW, otros	Comercial
	HDClone	Clonación rápida de discos con soporte RAID, sin funciones forenses integradas.	Windows XP/7/8/10/Server 2003–2016	IMG, RAW	Freemium
Captura de memoria	Magnet RAM Capture	Captura de memoria RAM sin alterar datos en ejecución.	Windows	RAW, BIN	Gratuita
	Belkasoft RAM Capturer	Alternativa para la extracción de memoria RAM en sistemas Windows.	Windows XP/Vista/7/8/10/Server 2003/2008	RAW, BIN	Gratuita
Análisis forense de disco	Autopsy 4.9.0	Análisis estructurado de discos, recuperación de archivos, cronología forense.	Windows, Linux, macOS	HTML, CSV, otros	Gratuita
	EnCase	Plataforma comercial robusta para análisis integral de evidencia digital.	Windows	E01	Comercial
	WinHex	Análisis hexadecimal y recuperación de datos a nivel bajo.	Windows	Varios formatos	Comercial
Análisis técnico del sistema	WinAudi 1.8	Captura de parámetros técnicos del sistema para documentación del entorno lógico.	Windows	TXT, CSV	Gratuita
	Belarc Advisor	Muestra detalles del hardware, software y configuraciones del sistema en un solo informe.	Windows	HTML	Gratuita
	Speccy	Ofrece un resumen técnico del sistema, incluyendo CPU, RAM, disco y otros componentes clave.	Windows	TXT, XML, otros	Gratuita

Fuentes: Exterro, (2024); X-Ways Software Technology AG, (2024); Miray Software, (2024); Magnet Forensics, (2024); Belkasoft, (2024); Sleuth Kit Labs, (2024); OpenText, (2024); X-Ways Software Technology AG, (2024); Parmavex Services, (2024); Belarc Inc., (2024); Piriform, (2024)

Cuadro 2

Descripción de fases, técnicas y normativas aplicadas en el peritaje digital

Fase	Actividad	Procedimiento	Recomendaciones técnicas	Cláusula ISO/IEC 27037:2012
Identificación de la evidencia digital	Identificación de componentes físicos y lógicos	Se inspeccionó el equipo utilizando WinAudi y Autopsy, documentando sistema operativo, cuentas de usuario y componentes internos.	Verificar estado del sistema sin alterarlo, registrar datos clave del hardware y software.	Cláusula 5.3 - Identificación
	Registro fotográfico del estado del equipo	Se realizaron fotografías forenses para registrar el estado físico del equipo antes de su manipulación.	Evitar manipulación previa al registro visual completo del equipo.	Cláusula 5.3
Recolección y adquisición de la evidencia digital	Extracción de memoria RAM	Se utilizó Magnet RAM Capture para obtener una imagen de la memoria RAM, preservando datos volátiles.	Capturar la memoria lo antes posible, usar herramientas certificadas para asegurar integridad.	Cláusula 6.3 - Evidencia volátil
	Clonación del disco duro	Se aplicó FTK Imager Lite para realizar una copia bit a bit del disco duro, con verificación de integridad mediante hash	Usar bloqueadores de escritura y generar hash antes y después del copiado.	Cláusula 7.2 - Evidencia no volátil
Conservación y preservación de la evidencia digital	Almacenamiento y resguardo seguro de la evidencia	Las imágenes forenses obtenidas y los archivos generados fueron almacenados en dispositivos externos seguros, con bloqueo de escritura y empaques antielectrostáticos. Se verificaron los valores hash antes y después de la transferencia.	Usar medios de almacenamiento certificados, asegurar integridad con hashes, mantener bitácoras y cadena de custodia.	Cláusula 7.4 - Preservación de la evidencia
Análisis de la evidencia digital (ISO/IEC 27042:2015)	Análisis de memoria RAM	Se empleó Autopsy para analizar los datos extraídos de la memoria RAM, identificando procesos y archivos en ejecución.	Preservar los datos analizados, documentar hallazgos con precisión.	Conforme al marco de análisis establecido en la norma ISO/IEC 27042:2015, aplicable a la interpretación técnica y contextual de evidencia digital.
	Análisis de disco y reconstrucción de línea de tiempo	Se reconstruyó una línea de tiempo con Autopsy desde el 28/03/2020 al 02/01/2021, revelando eventos clave.	Establecer cronología forense para comprender patrones de uso.	
	Recuperación del archivo 'DENUNCIA.docx'	Se localizó y recuperó parcialmente un archivo eliminado, analizando metadatos y contenido relevante.	Aplicar técnicas de recuperación válidas, preservar estructura y metadatos del archivo.	

Fuente: Archivo de los autores

Las herramientas seleccionadas para este procedimiento fueron FTK Imager Lite 3.1.1, Magnet RAM Capture, Autopsy 4.9.0 y WinAudi 1.8, por su efectividad comprobada en procesos de adquisición, análisis y documentación de evidencia

digital. Estas soluciones fueron escogidas no solo por su rendimiento técnico, sino también por ser gratuitas, ampliamente utilizadas en entornos forenses y por ofrecer compatibilidad con sistemas operativos estándar, facilitando su implementación sin comprometer la integridad de los datos. Además, su uso permitió cumplir con los lineamientos normativos sin incurrir en costos adicionales de licenciamiento, lo cual representa una ventaja significativa en contextos institucionales con recursos limitados. La comparación con alternativas funcionales permitió sustentar técnicamente su elección, asegurando que cada fase del procedimiento se ejecutara con medios adecuados al contexto del caso. La siguiente tabla resume las actividades ejecutadas en las etapas de identificación, adquisición y análisis de la evidencia digital, junto con sus recomendaciones técnicas y la cláusula normativa correspondiente.

2.5.2. Caso 2: Intervención forense en laboratorio institucional

Este caso se desarrolló en el laboratorio de cómputo de una institución de educación superior, a raíz de un incidente relacionado con la violación de seguridades lógicas. El personal técnico de la institución identificó comportamientos anómalos en uno de los equipos, lo que llevó a una revisión más detallada del sistema. Durante esta revisión, se detectó un proceso oculto bajo el nombre lsvc.exe, que funcionaba como un Keylogger, es decir, un programa diseñado para registrar todas las pulsaciones del teclado sin el conocimiento del usuario. Este hallazgo activó un procedimiento de respuesta técnica urgente para preservar la integridad de la información y evitar una posible filtración de datos sensibles de la institución (Proaño Escalante & Gavilanes-Molina, 2018).

Dado que los dispositivos aún se encontraban encendidos y en funcionamiento al momento de la intervención, se aplicaron procedimientos de adquisición en vivo conforme a la norma ISO/IEC 27037:2012, con el fin de preservar la evidencia digital sin alterar su estado original. Se realizaron capturas del disco y memoria del equipo comprometido, aplicando funciones hash (SHA256 y SHA1) para garantizar la integridad de la información recolectada. La siguiente tabla agrupa las herramientas utilizadas y comparadas, clasificadas por tipo y funcionalidad.

Cuadro 3
Comparación de herramientas para el
análisis forense en red institucional

Tipo de herramienta	Herramientas	Descripción	Sistema Operativo	Formato de salida	Licencia
Clonación/adquisición de disco	FTK Imager Lite 3.1.1	Creación de imágenes forenses bit a bit del disco con generación de hash.	Windows	E01, DD, AFF, RAW	Gratuita
	OSFClone	Utilidad gratuita que permite clonar discos de forma segura, diseñada para entornos forenses.	Independiente del sistema operativo	DD, AFF, EWF	Gratuita
	Guymager	Clonación forense alternativa para entornos Linux con GUI.	Linux	DD, EWF, AFF	Gratuita
Verificación de integridad	QuickHash	Verificación de archivos mediante SHA256 y SHA1.	Windows, Linux, macOS	TXT, CSV	Gratuita
	HashCalc	Generación de hashes básicos para archivos individuales.	Windows	TXT	Gratuita
	MD5Summer	Comparación de sumas MD5 de archivos.	Windows	TXT	Gratuita
Análisis de red	Wireshark	Captura de tráfico de red en tiempo real.	Windows, Linux, macOS	PCAP, TXT, XML	Gratuita
	NetworkMiner	Análisis pasivo de paquetes desde archivos PCAP.	Windows	HTML, CSV	Gratuita
	SmartSniff	Visualización en tiempo real de paquetes TCP/IP capturados.	Windows	TXT, CSV	Gratuita

Fuentes: (Exterro, 2024); (Guymager Project, 2024); (OSForensics, 2024); (QuickHash GUI, 2024); (SlavaSoft, 2024); (Krylack Software, 2024); (Wireshark Foundation, 2024); (Netresec, 2024); (NirSoft, 2024).

Las herramientas seleccionadas fueron FTK Imager Lite 3.1.1, QuickHash y Wireshark, por su comprobada eficacia en entornos forenses, su compatibilidad con los sistemas analizados y su capacidad para asegurar la integridad de la evidencia. Estas soluciones permitieron ejecutar la clonación del disco, verificar los archivos extraídos y analizar el tráfico de red en tiempo real, todo sin comprometer el estado original de los datos. Las alternativas como Guymager, OSFClone, HashCalc, MD5Summer, NetworkMiner y SmartSniff fueron consideradas, pero no utilizadas debido a restricciones operativas, licencias o menor adecuación al escenario.

Las herramientas seleccionadas permitieron aplicar un procedimiento estructurado que abarcó desde la identificación del entorno hasta el análisis de los hallazgos, en cumplimiento con la norma ISO/IEC 27037:2012 y complementado

por la ISO/IEC 27042:2015 para la fase interpretativa. La siguiente tabla resume las actividades desarrolladas en cada fase, las recomendaciones técnicas aplicadas y su correspondencia normativa.

Cuadro 4
Descripción de fases, técnicas y normativas aplicadas
en el análisis forense del incidente de red institucional

Fase	Actividad	Procedimiento	Recomendaciones técnicas	Cláusula ISO/IEC 27037:2012
Identificación de la evidencia digital	Inspección del entorno físico y digital	Se inspeccionaron equipos encendidos y conectados a red, documentando su estado sin apagarlos.	Evitar alteraciones al entorno antes de su documentación completa.	Cláusula 5.3 - Identificación
	Registro de elementos asociados al incidente	Se identificaron elementos como USBs, contraseñas visibles, y CD de respaldo presentes en el área.	Asegurar la recolección de todos los objetos físicos y digitales asociados al incidente.	Cláusula 5.3 - Identificación
Recolección y adquisición de la evidencia digital	Clonación forense del disco	Se aplicó FTK Imager para realizar una imagen forense bit a bit del disco duro.	Generar hash de los discos antes y después del clonado, y usar bloqueadores de escritura.	Cláusula 7.2 - Evidencia no volátil
	Captura de tráfico de red	Se utilizó Wireshark para capturar tráfico de red activo durante el uso del sistema.	Capturar la mayor cantidad de tráfico posible durante la intervención, manteniendo estabilidad.	Cláusula 6.3 - Evidencia
Conservación y preservación de la evidencia digital	Almacenamiento y resguardo de evidencia	La evidencia fue almacenada en medios externos con medidas de seguridad y verificación hash.	Verificar hashes, etiquetar soportes y mantener registro de cadena de custodia.	Cláusula 7.4 - Preservación
Análisis de la evidencia digital (ISO/IEC 27042:2015)	Análisis de tráfico de red capturado	Se analizaron los paquetes capturados para detectar conexiones sospechosas y tráfico anómalo.	Correlacionar eventos en los paquetes con posibles actividades maliciosas.	Conforme al marco de análisis establecido en la norma ISO/IEC 27042:2015, aplicable a la interpretación técnica y contextual de evidencia digital.
	Verificación de integridad con QuickHash	Se aplicó QuickHash para validar la integridad de los archivos adquiridos mediante SHA256.	Comparar hashes con los originales para garantizar integridad.	
	Identificación de software malicioso (keylogger)	Se detectó un proceso oculto (lscv.exe) que almacenaba pulsaciones de teclado en un archivo plano.	Documentar hallazgos, preservar evidencias recuperadas y su contexto técnico.	

Fuente: Archivo de los autores

3. Resultados y discusión

3.1. Caso 1: Explotación de computadora portátil HP mediante peritaje informático

Finalizadas las fases de identificación, adquisición, preservación y análisis, el peritaje informático permitió recuperar y examinar información clave contenida en el equipo analizado, asegurando la integridad, autenticidad y trazabilidad de la evidencia digital conforme a los lineamientos de la ISO/IEC 27037:2012.

Figura 2
Resultados de búsqueda por palabra clave “denuncia” en Autopsy 4.9.0

Name	Location	Modified Time	Change Time	Access
[0d3377d4-9711-4b87-bfee-26aeeb112f7e].final-slack	img_DISCO.001\vol_v02\	02 18:26:51 COT	2020-04-02 18:26:51 COT	2020
es.pak	img_DISCO.001\vol_v02\	01 18:26:04 COT	2020-04-02 17:26:21 COT	2020
8-DICEMBRIS 2018.pdf	img_DISCO.001\vol_v02\	-15 15:38:19 COT	2020-04-10 12:58:14 COT	2019
A1CE89F741346C62A84324D5E4E714E88A	img_DISCO.001\vol_v02\	-09 12:25:26 COT	2020-04-09 12:25:26 COT	2020
[20F560E8-4F30-431A-4724-03D67E8B381].msi	img_DISCO.001\vol_v02\	-01 14:36:55 COT	2017-09-01 14:36:55 COT	2017
R113016	img_DISCO.001\vol_v02\	-00 00:00:00	0000-00-00 00:00:00	0000
P200408	img_DISCO.001\vol_v02\	-00 00:00:00	0000-00-00 00:00:00	0000
[edc27b88-1189-4bd7-a211-38115ee21a36].final	img_DISCO.001\vol_v02\	-02 18:26:40 COT	2020-04-02 18:26:40 COT	2020
WdContextLog.es.002-slack	img_DISCO.001\vol_v02\	-22 15:46:55 COT	2020-07-22 15:46:55 COT	2020
eframe.dll.msi	img_DISCO.001\vol_v02\	-14 03:49:12 COT	2017-09-01 03:27:15 COT	2009
[edc27b88-1189-4bd7-a211-38115ee21a36].final-slack	img_DISCO.001\vol_v02\	-02 18:26:40 COT	2020-04-02 18:26:40 COT	2020
F1971584	img_DISCO.001\vol_v02\	-00 00:00:00	0000-00-00 00:00:00	0000
R758704.xlsx	img_DISCO.001\vol_v02\	-00 00:00:00	0000-00-00 00:00:00	0000
D444C9544763F2095AD898C5428C3D709735AC	img_DISCO.001\vol_v02\	-07 15:46:48 COT	2020-04-07 15:46:48 COT	2020
NbrPDFHistory.dat	img_DISCO.001\vol_v02\	-13 08:57:12 COT	2020-04-13 08:57:12 COT	2017
R544344	img_DISCO.001\vol_v02\	-00 00:00:00	0000-00-00 00:00:00	0000
Web History Artifact	img_DISCO.001\vol_v02\	-22 15:13:58 COT	2020-07-22 15:13:58 COT	2017
[2d405ca2-78f2-11ea-bf95-54a7da5b180c].[200807b-c176-4e40-b7ae-0404ee	img_DISCO.001\vol_v02\	-22 15:48:44 COT	2020-07-22 15:48:44 COT	2020

Matches on page: 1 of 3 Match Page: 1 of 1 Page

Text Source: Search Results

[[0d3377d4-9711-4b87-bfee-26aeeb112f7e].final-slack, e sufrido denuncia tras denuncia en redes sociales por parte del usuario que manifiesta su inconformidad y si se denuncia

Fuente: Archivo de los autores

Durante el análisis de la memoria RAM, se identificaron archivos recientemente abiertos, entre ellos documentos en formato PDF y Word vinculados directamente con los hechos investigados. Esta información, alojada en la memoria volátil, fue extraída antes de que pudiera perderse por el apagado del sistema.

En el disco duro, se reconstruyó una línea de tiempo de eventos que abarcó desde marzo hasta abril de 2020. Este análisis permitió evidenciar la creación, modificación y eliminación de archivos relevantes durante ese período. Uno de los hallazgos más significativos fue la localización de un documento de interés denominado DENUNCIA.docx, el cual había sido eliminado del sistema. Mediante técnicas de recuperación forense, se logró recuperar parcialmente su contenido y analizar los metadatos, revelando fechas clave asociadas al caso.

La figura 2 muestra una captura del entorno de análisis en la herramienta Autopsy, donde se visualiza el resultado de la búsqueda por palabra clave “denuncia”. En ella se observa la identificación del archivo recuperado, junto con fragmentos de su contenido donde se evidencian referencias directas al término, reforzando su relevancia dentro de la investigación digital.

Toda la evidencia extraída fue preservada en medios de almacenamiento externos con medidas de seguridad apropiadas, incluyendo el uso de bloqueadores de escritura, empaques antiestáticos y generación de valores hash, lo que garantiza su validez como prueba digital en el proceso legal correspondiente.

3.2. Caso 2: Intervención forense en laboratorio institucional

El análisis permitió confirmar que el proceso llsv.exe estaba activo en segundo plano y capturaba discretamente las pulsaciones del teclado, almacenándolas en un archivo oculto dentro del sistema. Se identificó la ruta exacta del archivo de registro generado por el keylogger, así como fragmentos de texto con datos digitados por usuarios recientes, entre los cuales se encontraron cadenas de texto asociadas a contraseñas, términos de búsqueda y formularios de acceso.

Si bien no se detectaron conexiones de salida en tiempo real durante el monitoreo con Wireshark, la presencia del software malicioso constituía una amenaza directa a la privacidad de los estudiantes y del personal que utilizaban el equipo intervenido. Para validar la autenticidad de los archivos adquiridos durante la intervención, se aplicaron funciones hash utilizando la herramienta QuickHash. Este proceso permitió verificar que los archivos analizados no presentaran alteraciones, lo cual refuerza la confiabilidad de los hallazgos presentados. El cuadro 5 resume los valores hash generados y el estado de integridad de cada archivo inspeccionado.

Cuadro 5
Verificación de integridad

Nombre del archivo	Hash SHA256	Estado
acceso_remoto.exe	2f3c4b65d8a8c3fa12d1e9c1a3c75f12345678abcdef1234567890abcdefabcd	Archivo no documentado
index.html	83b7f927eb2e7c456a75f6aa987ced45678a9b3cde8911ab23456789abcdef01	No alterado
launcher_portable.bat	9c7b2da334dc55f998877aa99bbccddeeff00112233445566778899aabbccdde	Uso no autorizado detectado
informe.docx	a3b2c17d9ef26fd01a47c20db7f8349029e8a5f5e61e1234567890abcdef1234	No alterado

Fuente: Archivo de los autores

La correcta ejecución de las fases forenses, el uso de herramientas adecuadas y la preservación rigurosa de la evidencia permitieron establecer con claridad la existencia de una amenaza activa en el entorno institucional. El análisis técnico sirvió no solo para documentar un incidente de seguridad real, sino también para sentar las bases de una respuesta más robusta ante futuros eventos. Este caso evidencia la importancia de contar con protocolos definidos, personal capacitado y metodologías alineadas con los estándares internacionales para garantizar intervenciones efectivas en escenarios de riesgo digital.

4. Conclusiones

El desarrollo de este estudio evidenció que la aplicación del peritaje informático bajo un enfoque estructurado, conforme a las normas ISO/IEC 27037:2012 e ISO/IEC 27042:2015, garantiza la integridad, autenticidad y trazabilidad de la evidencia digital recolectada. Estas normas proporcionan una base metodológica sólida que permite intervenir técnicamente sobre dispositivos electrónicos y contextos digitales diversos, asegurando que la información obtenida sea válida y utilizable en entornos judiciales y administrativos.

Organizar el proceso a partir de fases claramente definidas como la identificación, la adquisición, la preservación y el análisis no solo facilita una ejecución ordenada y reproducible, sino que también permite adaptar los procedimientos al tipo de evidencia, al estado del dispositivo y a las condiciones específicas del incidente. En este contexto, la selección de herramientas forenses desempeña un rol crucial. No basta con que estas sean funcionales: deben ser compatibles con el entorno técnico, validadas en el ámbito pericial y capaces de generar resultados verificables, tanto técnica como jurídicamente.

Los casos analizados permitieron comprobar la efectividad de este enfoque. En el primer escenario, orientado al análisis de una computadora portátil, se logró recuperar parcialmente un archivo eliminado, reconstruir una línea de tiempo de eventos relevantes y extraer información crítica desde la memoria RAM. Esto fue posible gracias al uso combinado de herramientas como FTK Imager, Autopsy y Magnet RAM Capture, seleccionadas por su estabilidad, compatibilidad y aceptación en la práctica forense.

Por su parte, el segundo caso abordó un incidente de seguridad informática en un laboratorio institucional, donde los equipos se encontraban encendidos y en red. En este entorno activo, se aplicaron técnicas que permitieron capturar tráfico de red en tiempo real, detectar la presencia de un keylogger oculto y verificar la integridad de los archivos adquiridos mediante QuickHash. La intervención demostró que, incluso en escenarios complejos y operativamente limitados, es posible preservar la evidencia sin comprometer su valor legal, siempre que se sigan estándares y protocolos establecidos.

A lo largo del estudio, se realizó además una comparación técnica entre herramientas utilizadas y descartadas, lo cual permitió sustentar de forma justificada cada decisión tomada. Esta evaluación reforzó la importancia de contar con criterios de selección claros que consideren no solo el rendimiento de la herramienta, sino también su adecuación al contexto, facilidad de implementación y licencia de uso.

En conjunto, los resultados confirman que la combinación de una metodología forense estandarizada con un criterio técnico riguroso permite actuar eficazmente ante distintos tipos de incidentes digitales. Tanto en dispositivos individuales como en entornos de red, el uso de buenas prácticas garantiza que la evidencia digital sea recolectada, analizada y preservada de forma confiable, transparente y legalmente admisible.

4.1. Perspectivas futuras

A partir de los resultados obtenidos, se considera pertinente continuar con investigaciones que integren el análisis forense automatizado mediante inteligencia artificial, así como la incorporación de herramientas que permitan acelerar la detección de amenazas en tiempo real. Asimismo, se plantea como línea futura la creación de protocolos de respuesta adaptados a distintos entornos (educativos, corporativos y gubernamentales), que utilicen marcos normativos como la ISO/IEC 27037:2012 y la ISO/IEC 27042:2015 como base metodológica estandarizada.

Referencias bibliográficas

- International Organization for Standardization; International Electrotechnical Commission. (2015). ISO/IEC 27042:2015. Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence. Geneva: ISO/IEC.
- Banegas Crespo, D. A., y Andrade Pesantez, D. J. (2024). Análisis Forense en Dispositivos Móviles Android para Casos de Ciberextorsión, Revisión Sistemática de Literatura. MQRInvestigar, 8(3), 22.
<https://doi.org/https://doi.org/10.56048/MQR20225.8.3.2024.4076-4097%20%20%20%20>
- Belarc Inc. (10 de Febrero de 2024). Belarc Advisor. Belarc: <https://www.belarc.com/products/belarc-advisor>
- Belkasoft. (05 de Febrero de 2024). Belkasoft RAM Capturer. Belkasoft: <https://belkasoft.com/es/ram-capturer>
- Cañarte Rodríguez, T., Idrovo Flores, P., Pinargote Vásquez, A., & Ponce Toala, F. (14 de 09 de 2022). PERITAJE DIGITAL Y DELITO INFORMÁTICO. Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS, 4(5), 22-30.
<https://editorialalema.org/index.php/pentaciencias/article/view/271>
- Coronel Rojas, L. A., Areniz Arévalo, Y., Cuesta Quintero, F., & Rico Bautista, D. (2020). Definición de una metodología de adquisición. Revista Ibérica de Sistemas e Tecnologías de Informação, 266–282.
<https://www.proquest.com/openview/0f5c06f94949d96044de8ebf92986bed/1?cbl=1006393&pq-origsite=gscholar>
- Cruz Vela, E. M. (2015). Modelo para el Análisis y Gestión de Riesgos en. REVISTA PGI.
<http://repositorio.umsa.bo/xmlui/handle/123456789/8754>
- Exterro. (18 de Marzo de 2024). FTK Imager. FTK Imager: <https://www.exterro.com/digital-forensics-software/ftk-imager>
- Gómez, L. S. (2018). Evidencia digital en la investigación penal.
https://www.researchgate.net/publication/323613054_Evidencia_digital_en_la_investigacion_penal

- Guymager Project. (21 de Febrero de 2024). Guymager – A fast forensic imager. Guymager Project: <https://guymager.sourceforge.io/>
- Hidalgo Cajo, I. M., Pucuna, S. Y., Hidalgo Cajo, G. B., Cevallos Paredes, A. K., Hidalgo Cajo, P. D., & Oquendo Coronado, M. V. (31 de 12 de 2018). Análisis Comparativo De Herramientas Forenses Informáticas Para La Realización De Peritajes En Medios Digitales. *European Scientific Journal*, 14(34). <https://doi.org/https://doi.org/10.19044/esj.2018.v14n34p80>
- International Organization for Standardization; International Electrotechnical Commission. (2012). ISO/IEC 27037:2012. Geneva: ISO/IEC.
- Krylack Software. (12 de Enero de 2024). MD5Summer – Check file hashes. Krylack Software: <https://www.md5summer.org/download.html>
- La Hora. (25 de Septiembre de 2023). Las extorsiones han crecido un 85% este 2023 en Ecuador. La Hora Ecuador: <https://www.lahora.com.ec/pais/las-extorsiones-han-crecido-un-85-este-2023-en-ecuador/>
- Magnet Forensics. (10 de Marzo de 2024). Magnet RAM Capture. Magnet Forensics: <https://www.magnetforensics.com/resources/magnet-ram-capture/>
- Melián Angel, J. (23 de Octubre de 2022). Análisis forense de la huella digital de un usuario en sistemas informáticos. Análisis forense de la huella digital de un usuario en sistemas informáticos. Valencia. <https://riunet.upv.es/entities/publication/5389ffab-b389-4a42-a2b7-55f2653df181>
- Miray Software. (01 de Enero de 2024). HDClone. Miray Software: <https://www.miray.de/products/sat.hdclone.html>
- Netresec. (05 de Febrero de 2024). NetworkMiner – Network forensic analysis tool. Netresec: URL: <https://www.netresec.com/?page=NetworkMiner>
- NirSoft. (08 de Marzo de 2024). SmartSniff – Packet sniffer tool. NirSoft: <https://www.nirsoft.net/utls/smsniff.html>
- OpenText. (08 de Marzo de 2024). EnCase Forensic. OpenText: <https://www.opentext.com/es-es/productos/forensic>
- OSForensics. (10 de Marzo de 2024). OSFClone – Disk Cloning Tool. OSForensics: <https://www.osforensics.com/tools/create-disk-images.html>
- Parmavex Services. (15 de Enero de 2024). WinAudit. Parmavex Services: <http://parmavex.co.uk/winaudit.html>
- Piriform. (12 de Enero de 2024). Speccy. CCleaner: <https://www.ccleaner.com/es-es/speccy/download?srltid=AfmBOpuahFL4Eu8TF9ckDqvTxduEXxetZRI3s6IRiG2Lh98yrP1Xrb4>
- Primicias . (27 de Junio de 2023). Primicias El periodismo comprometido. Ecuador: cada vez hay más víctimas de extorsiones 'clásicas' y virtuales: <https://www.primicias.ec/noticias/en-exclusiva/ecuador-extorsiones-denuncias-virtual-siciliana/>
- Proaño Escalante, R. A., & Gavilanes-Molina, A. F. (2018). Estrategia para responder a incidentes de inseguridad informática ambientado en la legalidad ecuatoriana. *Enfoque UTE*, 9(1), 90-101. <https://doi.org/https://doi.org/10.29019/enfoqueute.v9n1.229>
- QuickHash GUI. (15 de Enero de 2024). QuickHash GUI – Data hashing tool. QuickHash: <https://www.quickhash-gui.org/>
- SlavaSoft. (10 de Febrero de 2024). HashCalc – Free Hash Calculator. SlavaSoft: <https://hashcalc.software.informer.com/download/>
- Sleuth Kit Labs. (12 de Enero de 2024). Autopsy. Autopsy: <https://www.autopsy.com/>
- Wireshark Foundation. (01 de Abril de 2024). Wireshark – Network protocol analyzer. Wireshark: <https://www.wireshark.org/>
- X-Ways Software Technology AG. (10 de Febrero de 2024). WinHex: Computer Forensics & Data Recovery Software. X-Ways: <https://x-ways.net/winhex/>
- X-Ways Software Technology AG. (21 de Febrero de 2024). X-Ways Forensics: Integrated Computer Forensics Software. X-Ways: <https://www.x-ways.net/forensics/>

5. Anexos

Anexo A. Evidencia documental del caso de análisis forense aplicado a equipo portátil HP

Cuadro 6

Listado de archivos que contienen la imagen del disco duro de la computadora portátil objeto del examen pericial

No.	Nombre del archivo	MD5	SHA1	Fecha Creación	Tamaño (byte)
01	DISCOC.001	a5d94b6799da560f68e7676800932ea3	b7b55a17fb282382945e12efe6676671daf934a0	22/07/2020 19:01	1,572,864,000
02	DISCOC.001.txt	ca942a8d832241364ab5b7b7f0bc01f1	2e054d6f1fd28599180dffa75245c4fb03bb64c3	22/07/2020 20:16	2,959
03	DISCOC.002	df3cf3f65f5c70e8f94451ee217c88db	4b062f67c76c183afed57a81cc4c71c2a3cc4c3e	22/07/2020 19:03	1,572,864,000
04	DISCOC.003	883a9524fb4a988d26af5e79b585405c	65fd4fd4933073fd68e999136542d8518e93f5bc	22/07/2020 19:04	1,572,864,000
05	DISCOC.004	4d29d9ec1a06eb5d282460f39d82a49d	fd3c963b32af73dfc775008f9378047fafb309df	22/07/2020 19:05	1,572,864,000
06	DISCOC.005	eeba7b4ee6de684b86e346a3c11d4d5	6b88401616531a34691ff457d6c347fb07be5fc8	22/07/2020 19:06	1,572,864,000
07	DISCOC.006	e593ecfd886b3d72cbf568b51f611143	0a2014e90c0d1edc044885181e65cee644d49a48	22/07/2020 19:08	1,572,864,000
08	DISCOC.007	3f73135fb79478f680a7b03fe5352d9e	8c16273274a80e9f502d67733c44cad3ee63c376	22/07/2020 19:09	1,572,864,000
09	DISCOC.008	1f72cd1b3228fcee4c115b7ecf1ad9e4	c8fbf253aa0815bb3aa3adc94f3cb6b16e8bf9fb	22/07/2020 19:11	1,572,864,000
10	DISCOC.009	e5b07803ee364a81fac2ec96dc26af8c	75c75dc9a83d590dc3cb1d71231327130eeef8	22/07/2020 19:12	1,572,864,000
11	DISCOC.010	75358171b8843b9e87fc9763123e1e2c	d2da19eab4d29c92374757742eb01265f7956922	22/07/2020 19:13	1,572,864,000
12	DISCOC.011	4363346b4650de7b6efd4aebf7087907	cbe28fa40431e5939496101b91c5f06f63ffc597	22/07/2020 19:15	1,572,864,000
13	DISCOC.012	6be13021b2be7e8a4cde2473097ecbb6	4b7028b7492c9b5c1b6570da4be9da114498baf1	22/07/2020 19:16	1,572,864,000
14	DISCOC.013	22ac016fc45ab569998dc53364c8ddc4	25b92d38d0316346f6ade0f04bbdb6fb5bfff7e98e	22/07/2020 19:18	1,572,864,000
15	DISCOC.014	31d112d0c7d747ac51e9fc2551397877	943413cd7598d5d22bd27f8171d8f6bac9a9feaa	22/07/2020 19:19	1,572,864,000
16	DISCOC.015	d749b8ada6527bd9d7e139ec2c694b72	95b4b759b4e79cf5b3651ed0c609b8e960eee14b	22/07/2020 19:20	1,572,864,000
17	DISCOC.016	b63412691d1eead8730725a8651de88	723e5acaa2ad4d66850a4b0241891b7d95938721d	22/07/2020 19:22	1,572,864,000
18	DISCOC.017	3585f298cf89c8284bc6f57843a885f3	9955c1e9e3455b0fe99d4e4adf9518601c320a55	22/07/2020 19:23	1,572,864,000
19	DISCOC.018	1ba65d1c9d27975616bb1bb4083ff176b	cc0f7bfe2075b2e61ab59c14cef2a5ebfbae4cae	22/07/2020 19:25	1,572,864,000
20	DISCOC.019	5bdbdf326fa871e8e154fd92b8169d2f	d6298e0c2f6978f78f3e246b776436b430ded8a	22/07/2020 19:26	1,572,864,000
21	DISCOC.020	6a07cd0cc167be0cb8013120a1262ddf	cb3b31a9853af4e6768c8c39ad217e6dbc1a0567	22/07/2020 19:28	1,572,864,000
22	DISCOC.021	52431423389b0b05edc0040c441a7dc3	5696e4be47f934793b987ef3c1d0f09a848d6d3f	22/07/2020 19:29	1,572,864,000
23	DISCOC.022	d72166a1190ec23c57b8a02e9ae74c13	916b0c1c2029487edccc40f03947603cd86bab46	22/07/2020 19:30	1,572,864,000
24	DISCOC.023	d25a30705fad0cd23ba51465f4dd9a1e	14acedf3e680905809c7d322e60d4367ee295892	22/07/2020 19:32	1,572,864,000
25	DISCOC.024	07b675a3011bc8c56344d60c25b5281a	d801eb809f4cf86eba39176d0754a16b20cbe666	22/07/2020 19:33	1,572,864,000
26	DISCOC.025	ff2c1bea977f900e8e0a305b73ab53e7	fdc8cefdccae00946ff4a3833a546d5b51279bb	22/07/2020 19:35	1,572,864,000
27	DISCOC.026	b42eb925a24d4cdec193f3d1e39fe4	a3040d527402be436392524309861a82d37571cc	22/07/2020 19:36	1,572,864,000
28	DISCOC.027	03e814afb16e56d2848a0f7128de74f5	0139e725c8e5dfcc37959d7934a831a862e00fb8	22/07/2020 19:38	1,572,864,000
29	DISCOC.028	afe8ea5cc287869a30b1a8f9030f90e6	f611f8fb53678ab7d9803216eab6492c6ea2e0ec	22/07/2020 19:39	1,572,864,000
30	DISCOC.029	0328fac56e2e36482ab8625b78955e8	bebf8ce9fde765180c5011217f5b5ae6ddaebac4	22/07/2020 19:40	1,572,864,000
31	DISCOC.030	f0c2c64bb25fea4ed13849cacee1d195	a45e958e7ba97096fe94d84bc08df109461c9217	22/07/2020 19:42	1,572,864,000
32	DISCOC.031	1638f3f19882d5f89945c38af4b29b7d	2c8de71109a7c11b646536bd8ab4a71aabc12cf1	22/07/2020 19:43	1,572,864,000
33	DISCOC.032	97eae9b0745f3f03a2f69952fa690caa	db366d7f2f516d6e73a2a0bf5618098fcd53d2d	22/07/2020 19:45	1,572,864,000
34	DISCOC.033	5ec00608e59c4dc61f68b9f9a073992d	2e0636fdd8b718483ec137a2355aba226f8561c8e	22/07/2020 19:46	1,572,864,000
35	DISCOC.034	7fce3810b2c477de0118c8a2e6aaeb89	d831e3a9eb95b00342bad5a268bd8c6a57376a62	22/07/2020 19:48	1,572,864,000
36	DISCOC.035	4b883290b64ff40bbbd8871e287b254d	466c5c8bb703c4d3697e20dae3267c75da6bdd48	22/07/2020 19:49	1,572,864,000
37	DISCOC.036	8a9def8c732e14a69f2bb9277540b6c6	d520c6cd4a865687585e22b19d84b3c1e20d6cdf	22/07/2020 19:50	1,572,864,000
38	DISCOC.037	012cecd0f045972cbf4d3bc6e1de0e75	57eb4b3fb9d10e32a9becb40370b794d0b2a2387	22/07/2020 19:52	1,572,864,000
39	DISCOC.038	eeba7b4ee6de684b86e346a3c11d4d5	6b88401616531a34691ff457d6c347fb07be5fc8	22/07/2020 19:53	1,572,864,000
40	DISCOC.039	7388cef642707da7f7107c42a2974c08	0aadab7ba55463b44a76f59283ebfe0fe6b05d8b	22/07/2020 19:55	1,572,864,000
41	DISCOC.040	440ea56b4409f75e1e6c6ae977d978ca	d84914452473123b7b575ea1ea3b1377057d19ed	22/07/2020 19:56	1,572,864,000
42	DISCOC.041	d5d46035b60da6966089976af5e772e4	f8b94e17ff51a85e74005c9c12fb29580338bba	22/07/2020 19:58	1,572,864,000
43	DISCOC.042	3385a1ccce3e45680d4c4f4d3959fb57	45d24a623d19f3d22c360b846f6a9c0506ad3a73	22/07/2020 19:59	1,572,864,000
44	DISCOC.043	eeba7b4ee6de684b86e346a3c11d4d5	6b88401616531a34691ff457d6c347fb07be5fc8	22/07/2020 20:00	1,572,864,000
45	DISCOC.044	7397d874d1e57a83261e31b4b72019b8	f7a71569d514e696da7a4523b6f36e0af226c675	22/07/2020 20:02	1,572,864,000
46	DISCOC.045	5800b786d88944bfb22cb0df0030e09	64afcb7a70e6c97e57ff7b73fda30ae1a7f8fbb9	22/07/2020 20:03	1,572,864,000
47	DISCOC.046	9e327c9285c94769144942816a7f21cf	1406ff82e8a6296f27d48c759618a39a52317b65	22/07/2020 20:05	1,572,864,000
48	DISCOC.047	c34c834871d9fbb48f781aa502d0c631	f8312eb63bb99c2dd304c965caa5805ed1648f3c	22/07/2020 20:06	1,572,864,000
49	DISCOC.048	d5d46035b60da6966089976af5e772e4	f8b94e17ff51a85e74005c9c12fb29580338bba	22/07/2020 20:07	1,572,864,000
50	DISCOC.049	00e3446f6dbce5b6ed840d766e139f1	a29e0663f8ca56bef3e27d286adfa7a19cf556c9	22/07/2020 20:09	1,572,864,000
51	DISCOC.050	8bc0b6d69c4fe07e4c0a6cf0502ad11e	b2b68a07bb5752df1e3c70f8224d664e5a9ec49f	22/07/2020 20:10	1,572,864,000
52	DISCOC.051	fb985dbf4ff8674e42be5d74291f4203	3f16ffa2e26bab940959560a4cb86e57a9e414a9	22/07/2020 20:12	1,572,864,000
53	DISCOC.052	e8b328422f436df44be7fd8ad044a597	3f1deddb6c7fe5a3c3400f3cb13e346ec0cd76db	22/07/2020 20:13	1,572,864,000
54	DISCOC.053	a145d2e37f76ef108b92eea46124022b	09ed0c8622b59d6ff34632fbfb658dda44a8345d	22/07/2020 20:14	1,572,864,000
55	DISCOC.054	a5dac9bcb15a87644e5d9210d4c6f6e3	896c5896195bf0b8d61fdf68b27b1fb37df7a78	22/07/2020 20:15	535,822,336

Fuente: Archivo de los autores



Esta obra está bajo una Licencia Creative Commons
Atribución-NoComercial 4.0 Internacional