No. orden de compra y/o servicios:	OSG-0035-JNCI-2025
Valor de la orden:	14.235.000,00
Fecha de expedición de la orden:	11/11/2025
Fecha de vencimiento:	11/12/2025
Objeto de la orden:	Contratar los servicios de auditoría en informática forense y representación legal en derecho digital para la identificación, recolección, aseguramiento y análisis de evidencia digital en tres (3) equipos de cómputo de la Junta Nacional de Calificación de Invalidez
Fecha de prestación del servicio o entrega del bien:	10/02/2026
Supervisor de la orden:	Ana Belly Meneses Rosales
Cargo:	Profesional Contractual
Dependencia:	Unidad de Gestión Contractual
Proveedor o prestador de servicio:	ARCONT GROUP SAS
Nit o cédula de ciudadanía:	901.138.375-9

BALANCE FINANCIERO DE LA ORDEN No. OSG-0035-JNCI-2025

Valor de la orden:	14.235.000,00
Valor pagado:	7.117.500,00
Valor pendiente pago:	7.117.500,00

INFORME DE LA PRESTACIÓN DE SERVICIOS O ENTREGA DE BIENES:

ITEM	SI	NO	JUSTIFIQUE	N/A
¿El bien o servicio cumplió con las especificaciones técnicas mínimas solicitadas?	X		Se recibió informe de laboratorio Misión de trabajo N°20250101011 de fecha 10 de febrero de 2026, por parte de Arcont Group SAS.	
¿El contratista cumplió con los tiempos pactados			El contratista entregó	

para la entrega del bien o la prestación del servicio?			el informe final el día 10 de febrero de 2026.	
¿Se llevó a cabo la instalación o puesta en funcionamiento de los bienes a entera satisfacción?				X
¿Se llevaron a cabo los mantenimientos preventivos o correctivos solicitados a entera satisfacción?				X
¿Se recibió el bien o la prestación del servicio a entera satisfacción?	X		Se recibió el informe de auditoría requerido por la Entidad.	

En mi calidad de supervisor designado de la Orden de Prestación de Servicios No. OSG-0035-JNCI-2025, certifico que cumplí con las funciones de verificación, vigilancia y control respecto del adecuado desarrollo y ejecución del objeto contractual, de conformidad con las obligaciones asignadas.

Así mismo, se suscribe la presente Acta de Recibo a Satisfacción y Entrega de Supervisión, dejando constancia de que, a la fecha, se adelantaron las siguientes gestiones:

1. El contratista Arcont Group entregó el día 10 de febrero de 2026 el informe final en informática forense.

2. El 27 de febrero de 2026, se recibió acta de entrega de supervisión por parte de Estephany Cruz Suarez donde se relaciona que se encontraban pendientes las siguientes actuaciones:

   a. Requerir formalmente al contratista para que emita pronunciamiento respecto del cargador correspondiente al equipo marca Lenovo, identificado con el número de activo EPD00300.
   b. Solicitar al contratista la verificación de la factura que se encuentra pendiente, en atención a que no fue posible realizar el descifrado del computador MacBook, modelo A223B, circunstancia que impidió culminar la validación técnica requerida.

   Teniendo en cuenta lo anterior, se relacionaron las siguientes gestiones por la supervisora actual de la orden de servicios:

3. El día 09 de marzo de 2026, la profesional contractual remitió requerimiento formal al contratista solicitando la entrega del cable, conforme se evidencia en el documento adjunto.

4. El día 19 de marzo de 2026, el contratista realizó la entrega del cable a la JNCI, de conformidad con el Acta de Recepción adjunta.

5. El día 09 de marzo de 2026, se realizó reunión entre la supervisión de la orden de servicios OSG-0035-JNCI-2025 y el contratista Arcont Group SAS, donde se solicitó aclaración sobre el computador MacBook Modelo A223B, ante lo cual el contratista Arcont Group SAS manifiesta que enviará un informe por escrito donde se relacione los procedimientos realizados en el computador MacBook Modelo A223B.

6. El día 20 de abril de 2026, Arcont Group SAS remite un informe ejecutivo donde se detalla lo siguiente:

   a. Procedimientos realizados en el computador MacBook Modelo A223B

En relación con el MacBook A223B, es preciso señalar que la actuación pericial se desarrolló dentro del máximo alcance técnicamente viable, con observancia de los principios de integridad, preservación y no alteración de la evidencia digital. Durante la intervención se realizó la fijación fotográfica, la inspección técnica del equipo, la verificación de su arquitectura de almacenamiento y la evaluación del método de adquisición forense procedente. De esta valoración se estableció que el equipo cuenta con una unidad SSD soldada directamente a la placa lógica y con chip de seguridad Apple T2, condiciones que impiden la aplicación de métodos tradicionales de extracción física del medio de almacenamiento, como sí ocurrió en los demás equipos examinados. En consecuencia, la ruta técnicamente procedente para este dispositivo depende de técnicas de adquisición lógica o adquisición en vivo, condicionadas por el acceso legítimo al volumen cifrado mediante una clave válida de FileVault.

Sobre este equipo se adelantaron labores periciales concretas y especializadas, entre ellas: documentación e inspección técnico-fotográfica, identificación de su configuración de seguridad, determinación de la imposibilidad de extracción física del medio, evaluación de técnicas forenses compatibles con macOS, validación de la clave suministrada y ejecución de intentos controlados de restablecimiento de FileVault. Tales actividades constituyen trabajo pericial material y metodológicamente sustentado, orientado a preservar la evidencia y a agotar el alcance técnico seguro de intervención sobre el dispositivo.

Asimismo, desde el punto de vista forense, no resultaba procedente insistir en nuevos intentos no soportados por una credencial válida, toda vez que ello podía comprometer la integridad del sistema, alterar el estado lógico del dispositivo, afectar artefactos potencialmente relevantes para el análisis o activar restricciones adicionales de seguridad, en contravía de los principios de preservación de la evidencia digital. Por tal razón, la intervención se mantuvo dentro de parámetros técnicamente seguros, trazables y compatibles con las buenas prácticas periciales, privilegiando la conservación del valor probatorio de la información sobre maniobras invasivas o potencialmente disruptivas.

   b. Cumplimiento del objeto contractual de la orden OSG-0035-JNCI-2025

En el equipo DELL W21B se halló el archivo "ALEGATOS ACCION POPULAR.pdf" en rutas del sistema bajo la estructura GUSTAVO\CONTESTACIONES DDA\ACCION POPULAR, así como una versión en formato .docx, ambas con metadatos de creación, acceso, modificación, autoría y último guardado. Adicionalmente, se identificaron rastros de descarga y gestión a través del navegador, vinculados al perfil gustavo.zarate y al aplicativo Ciclo de Firma. En el equipo Lenovo, por su parte, la búsqueda exhaustiva dentro del universo indexado no evidenció coincidencias recuperables del archivo objeto de análisis. Bajo ese contexto, la incidencia técnica presentada con el MacBook no alteró el sentido de los resultados obtenidos ni modificó los hallazgos consolidados a partir de la evidencia forense válidamente adquirida y analizada en los demás equipos.

7. El día 12 de marzo de 2026, el contratista remitió la declaración juramentada de pago de aportes al Sistema de Seguridad Social Integral y parafiscales donde se evidencia que cumplió con sus obligaciones durante la ejecución de la orden OSG-0035-JNCI-2025

Por consiguiente, de acuerdo con la revisión y el análisis realizado por la supervisión del contrato se evidencia el cumplimiento del objeto contractual, toda vez que se prestaron los servicios de auditoria informática forense y se logró la identificación, recolección, aseguramiento y análisis de evidencia de los equipos.

En consecuencia, una vez efectuadas y verificadas las gestiones anteriormente descritas, se deja constancia de que el contratista cumplió a satisfacción con el objeto contractual, por lo cual la Entidad puede proceder con el trámite de pago hasta por la suma de SIETE MILLONES CIENTO DIECISIETE MIL QUINIENTOS PESOS M/CTE ($7.117.500,00).

Para constancia, se firma en Bogotá D.C., a los cuatro (04) días del mes de mayo de 2026.

Ana Meneses.
Ana Belly Meneses Rosales
Profesional Contractual

NÚMERO ÚNICO DE CASO: N/A	
SOLICITANTE: JUNTA NACIONAL	**MISIÓN DE TRABAJO:** 20250101011
UNIDAD ASIGNADA: LABORATORIO DE INFORMÁTICA FORENSE	**ABOGADO:** ALEJANDRO MEJÍA ORTIZ
CIUDAD, FECHA Y HORA: BOGOTÁ D.C., 10 DE FEBRERO DE 2026, 17:00 HORAS	

Señores
JUNTA NACIONAL DE CALIFICACIÓN DE INVALIDEZ
Bogotá. D.C.

Conforme a lo establecido en los artículos 210, 255, 257, 261,275 y artículos 218, nos permitimos rendir el siguiente dictamen pericial:

ESTUDIO SOLICITADO:

De acuerdo con lo solicitado por la JUNTA NACIONAL DE CALIFICACIÓN DE INVALIDEZ y siguiendo los protocolos y estándares internacionales, así como la norma ISO 27037, se requiere realizar lo siguiente:

1. Realizar imagen forense a los equipos que se relacionan a continuación:
   - Un (1) computador marca **DELL**, modelo **W21B**, tipo todo en uno, con el número de activo EPD00300.
   - Un (1) computador portátil marca **Lenovo ThinkPad**, identificado con el número de activo EPD00402.
   - Un (1) computador portátil marca MacBook, modelo A223B y número de activo EPD00354.
2. Una vez realizadas las imágenes forenses, efectuar la identificación del archivo titulado **"Alegatos Acción Popular"**, el cual fue enviado por correo electrónico el **24 de octubre de 2025** a las direcciones: cristian.collazos@juntanacional.com, directoradministrativo@juntanacional.com, Adicionalmente, se tiene como objetivo verificar si otras personas, distintas a los usuarios principales de cada equipo, tuvieron acceso al archivo o a la información relacionada contenida en los equipos, incluyendo las direcciones de correo electrónico.

DESCRIPCIÓN DE LOS ELEMENTOS MATERIALES PROBATORIOS Y EVIDENCIA FÍSICA RECIBIDOS PARA ESTUDIO:

El día 24 de noviembre del año 2025 en la carrera 19 No. 102 – 53 oficinas de la Junta Nacional de Calificación de Invalidez, se recibe por parte del área de sistemas, tres equipos de computador: Un (1) computador marca **DELL**, modelo **W21B**, tipo todo en uno. Un (1) computador portátil marca **Lenovo ThinkPad**, identificado con el número **EPD00402** y un (1) computador portátil marca MacBook, modelo A223B y número de activo EPD00354. Por parte del área de tecnología se suscribe el acta de acceso a medios electrónicos, dejando constancia de la autorización para el acceso y la obtención de copias mediante imágenes forenses. Posteriormente, se procede a la fijación fotográfica de los equipos de cómputo (ver imágenes 1, 2, 3, 4, 5, 6, 7, 8 y 9).




IMÁGENES 1 Y 2. Fotografía de primer plano, donde se observa parte anverso y reverso del equipo de cómputo.

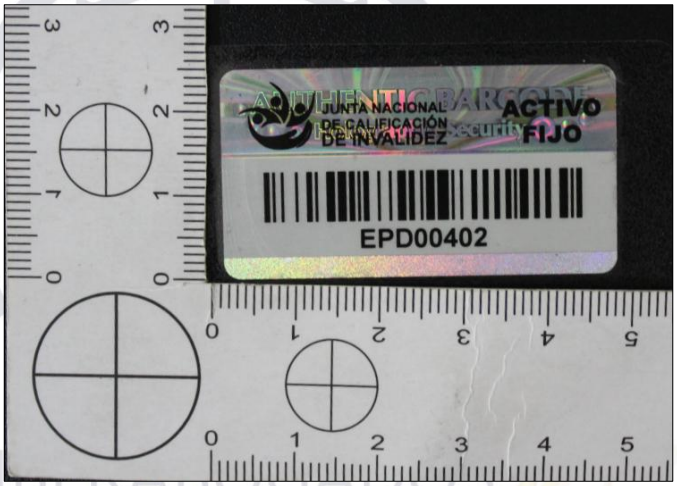


IMAGEN 3. Fotografía de primer plano, donde se observa las características del equipo de cómputo objeto de estudio identificado como la evidencia No. 1




IMÁGENES 4 Y 5. Fotografia de primer plano, donde se observa parte anverso y reverso del equipo de computo objeto de estudio e identificado con evidencia No. 2.



IMAGEN 6. Fotografía de primer plano, donde se observa las características del equipo de cómputo objeto de estudio identificado como la evidencia No. 2





IMÁGENES 7 Y 8. Fotografia de primer plano, donde se observa parte anverso y reverso del equipo de computo objeto de estudio e identificado con evidencia No. 3.



IMAGEN 9. Fotografía de primer plano, donde se observa las características del equipo de cómputo objeto de estudio identificado como la evidencia No. 3

DESCRIPCIÓN Y EXPLICACIÓN DE LOS PRINCIPIOS, MÉTODOS Y PROCEDIMIENTOS TÉCNICOS UTILIZADOS.

Para asegurar los elementos materiales probatorios a nivel digital se tiene en cuenta los procedimientos de informática forense avalados internacionalmente, las buenas prácticas y estándares internacionales como el establecido en la norma ISO 27037, 27042, 27043 y 27050, custodiando las imágenes forenses obtenidas y los equipos más importantes, teniendo en cuenta los principios básicos de PRINCIPIO DE DISPONIBILIDAD: Cuando la información es accesible a los usuarios autorizados en el momento de requerirla. PRINCIPIO DE NO REPUDIACIÓN: Cuando la información involucrada en un evento corresponde a quien participa en el mismo, quien no podrá desconocer su intervención en dicho evento. PRINCIPIO DE INTEGRIDAD: Cuando se garantiza que la información es exacta y completa no se modifica desde el momento de su creación y se almacena en un formato que asegura la exactitud de la información original. PRINCIPIO DE CONFIDENCIALIDAD: garantiza que la información solo estará accesible para las personas autorizadas OBSERVANCIA: Cuando se lleva el registro de los eventos importantes, todo esto usando el software adecuado para obtener una imagen forense y custodiarla.

ACEPTACIÓN DE LOS PRINCIPIOS, MÉTODOS O PROCEDIMIENTOS POR LA COMUNIDAD TÉCNICO CIENTÍFICA

La informática forense, computación forense, análisis forense digital o examinación forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos, para los análisis forenses se disponen de 4 pasos esenciales que son la identificación, preservación, análisis y presentación, reconocidos internacionalmente, de igual forma la preservación de la evidencia se debe alinear a la norma ISO 27037.

La herramienta FTK, es un software forense que se utiliza para crear archivos de imagen de disco o montar imágenes de disco o dispositivos de almacenamientos y luego podemos realizar análisis de la estructura del disco, recuperar datos, etc. Este software permite localizar archivos perdidos o buscar datos escaneando la imagen de disco mediante palabras claves. Una de las ventajas es que, al finalizar la Impresión de la imagen, el software calcula y genera un clave hash MD5 que será utilizada para confirmar la integridad de los datos y que la imagen que se crea no ha sido alterada. FTK Imager es muy utilizado por peritos informáticos forenses ya que permite Impresión datos de un dispositivo, crear una imagen con los datos y luego evaluar la evidencia digital para determinar si se justifica un análisis más detallado, el cual ha sido probado y avalado por el Instituto Nacional de Justicia del Departamento de Justicia de los Estados Unidos (NIJ - DOJ).

Una imagen es una copia de todo o parte del dispositivo de almacenamiento para prevenir que se modifiquen accidental o intencional los datos que existen en el dispositivo de almacenamiento. FTK Imager realizar una imagen copiando bit a bit, la imagen resultante en un archivo es idéntica a la estructura original del dispositivo, incluyendo espacio, configuración la unidad y cualquier

archivo que contenga la unidad incluso si fuera temporal. Esto permite almacenar estos datos en un lugar seguro para luego realizar una investigación utilizando la imagen del dispositivo.

EQUIPOS E INSTRUMENTOS EMPLEADOS Y SU ESTADO DE MANTENIMIENTO

Se utilizó una estación forense identificada como L4BOR4TORIO-INFORM4TIC4-1, equipada con procesador Intel® Core™ i9-12900KF de 12.ª generación, sistema operativo Windows 11 Profesional y suite ofimática Microsoft 365. Para la fijación fotográfica se empleó una cámara digital Nikon Coolpix P520, serie 30145018, lente 42X Wide Optical Zoom ED VR (4.3–180 mm, 1:3–5.9, 42X HD). Como herramientas forenses se utilizaron FTK Imager y FTK Toolkit versión 8.2, así como un duplicador y bloqueador de escritura Tableau TD3 Imager.

GLOSARIO DE TÉRMINOS

Bloqueadores: Dispositivo contra escritura que sirve para leer datos de dispositivos de almacenamiento masivo sin temor a que esos datos sean modificados durante el proceso de adquisición.
Carpetas: mecanismo virtual que permiten gestionar los datos que se guardan en la computadora.
Chipset o System On a Chip (SOC): es un conjunto de componentes electrónicos que están integrados en el procesador de un dispositivo electrónico. Su función es controlar el flujo de datos entre el procesador, la memoria y los diferentes periféricos que haya en un ordenador
Dispositivo Móvil: Dispositivo de reducido tamaño con algunas capacidades de procesamiento, conexión permanente o intermitente a una red, con memoria limitada, diseñados específicamente para una función, pero que pueden llevar a cabo otras más generales.
Dispositivos o Medios de Almacenamiento de Información Digital: Es un medio o elemento que permite almacenar información en formato digital tal como diskettes, discos duros, memorias, CDs, DVDs entre otros.
Estación Forense: Computador de gran capacidad tanto en hardware y software para resolver los requisitos terminantes de conducir una adquisición y un análisis forenses apropiados.
Evidencia Digital: También conocida como evidencia computacional única y conocida como: registros o archivos generados y/o almacenados por computador u otro medio equivalente.
Fecha de Creación de un archivo: Es la fecha en que se crea o se genera un archivo por primera vez en un computador o medio de almacenamiento determinado. O la fecha en que se copia por primera vez un archivo hecho en otro ordenador o medio de almacenamiento a otro. En conclusión, es la fecha de la primera vez que “aparece” un archivo en un computador y/o medio de almacenamiento con el nombre designado.
Fecha de ultimo acceso: Es la fecha que registra el sistema en la cual se abrió o accedió un archivo desde el ordenador por última vez, incluso esto puede ser realizado por procesos automáticos de revisión de archivos como un antivirus, el acceso a un archivo no necesariamente implica modificación al mismo.
Fecha de última modificación o ultima escritura: es la fecha registrada por el sistema cuando se graba o guarda un archivo por última vez, ya sea por realizar algún tipo de cambio al contenido del archivo o se almacena seleccionando la opción “guardar como”.
FTK: Software forense utilizado para procesar la imagen forense para lograr la recuperación, localización, búsqueda, análisis y clasificación de evidencias digitales (archivos).
FTK Imager: Software forense utilizado en el área de peritazgo para realizar imágenes forenses.

HASH: Es un valor alfanumérico calculado a través de algoritmos especializados a partir del contenido de un archivo lo que permite garantizar su integridad. Hace para los archivos las veces de Huella Digital. Cualquier modificación a un archivo, por pequeña que sea, hace que este valor cambie.

Imagen Forense: Es una copia idéntica de un dispositivo de almacenamiento, tanto del área ocupada como del área libre, realizada a través de software y/o equipos especializados que realizan automáticamente rutinas de comprobación y verificación de la imagen lo que garantiza su exactitud.

IMEI: Acrónimo de International Mobile Equipment Identity (identidad internacional del equipo móvil) identifica a un número individual y exclusivo de un teléfono móvil en particular. Es decir que este número IMEI es la Identidad del Equipo Móvil Internacional que puede utilizarse para identificarlo. Este código identifica al aparato unívocamente a nivel mundial, y es transmitido por el aparato a la red cuando se conecta a la misma.

IMSI: Acrónimo de International Mobile Subscriber Identity (Identidad Internacional del Abonado de un Móvil). Es un identificador único por cada teléfono móvil en sistemas GSM. El IMSI se guarda en la SIM (Subscriber Identity Module), que es la tarjeta chip que se inserta en el teléfono móvil para asignarle el número de abonado.

Inhibidor de señal: es un Dispositivo electrónico que impide o dificulta las transmisiones radioeléctricas en un determinado rango de frecuencias componiéndose básicamente de un generador de señal y un transmisor. El primero genera una señal que es enviada a través del segundo con una potencia determinada según la necesidad. Esta señal carece de información útil, únicamente es una señal generada por un oscilador o generador de onda. Esta, al emitirse con mayor potencia que los sistemas de transmisión a interferir, las suprime, evitando que emisor y receptor establezcan la comunicación.

MD5: En criptografía, MD5 (acrónimo de Message-Digest Algorithm 5, Algoritmo de Resumen de Mensaje 5) es un algoritmo de reducción criptográfico HASH de 128 bits ampliamente usado, representado en 32 caracteres hexadecimales, comúnmente conocido como huella digital de un archivo, dato o medio de almacenamiento de información, que identifica que un archivo o mensaje de datos.

Mensajes MMS: Sistema de Mensajería Multimedia es un estándar de mensajería que le permite a los teléfonos móviles enviar y recibir contenidos multimedia, incorporando sonido, video, fotos o cualquier otro contenido disponible en el futuro. La mensajería multimedia nos permite el envío de estos contenidos además a cuentas de correo electrónico.

Mensajes SMS: Es un servicio disponible en los teléfonos móviles que permite el envío de mensajes cortos (también conocidos como mensajes de texto, o más coloquialmente, textos) entre teléfonos móviles.

MobilEdit: Software forense dedicado a la extracción de dispositivos móviles, nube y Smartwacth

Partición: Es cada da una de las divisiones presentes en una unidad física de almacenamiento de datos, la cual se puede formatear con un sistema de archivos e identificar con una letra del alfabeto.

Software Forense: Herramientas o programas de software especializado en estudio de dispositivos de almacenamiento magnético desde el punto de vista forense, entre ellos se encuentran el FTK IMAGER, FTK, ENCASE, entre otros.

SPN: Acrónimo de Service Provider Name - Nombre del Proveedor de Servicio.

SHA1: (acrónimo Secure Hash Algorithm 1, Algoritmo Hash Seguro 1) es un algoritmo de reducción criptográfico HASH 160 bits, representado en 40 caracteres hexadecimales, el cual también es

utilizado como huella digital de un archivo, dato o medio de almacenamiento de información, que identifica que un archivo o mensaje de datos.

SSID: Es la identificación asociada a una red de área local inalámbrica (Wi-Fi) para que un cliente pueda diferenciarse de los demás en la misma ubicación. Por lo tanto, siempre que alguien quiera conectarse a una red inalámbrica, debe conocer el SSID y la contraseña que normalmente se asigna para el acceso.

Tarjeta SIM: Acrónimo de Subscriber Identity Module, en español módulo de identificación de suscriptor, es una tarjeta inteligente desmontable usada en teléfonos móviles, tablet y módems USB. Las tarjetas SIM almacenan de forma segura la clave de servicio del suscriptor usada para identificarse ante la red, de forma que sea posible cambiar la línea de un terminal a otro simplemente cambiando la tarjeta.

Tarjeta Micro SIM: Actualmente es el estándar de tarjeta SIM más extendido. Tiene un tamaño reducido (15 x 12 milímetros), de forma que se aprovecha mejor el espacio interno del teléfono para hacerlo más potente, y que tenga mayor capacidad de almacenamiento (desde 32KB hasta 128KB), lo que permite guardar más ajustes y aplicaciones, tener más seguridad y archivar un mayor número de contactos en la agenda.

Tarjeta Nano SIM: Es la tarjeta SIM más pequeña que existe en la actualidad (12,3 x 8,8 milímetros) y en ella se ha eliminado el plástico de alrededor, dejando únicamente el chip de almacenamiento. Es la tarjeta SIM con mayor capacidad de almacenamiento (128KB).

UFED: Herramienta forense que permite la extracción física y lógica de datos de dispositivos móviles.

RESULTADOS

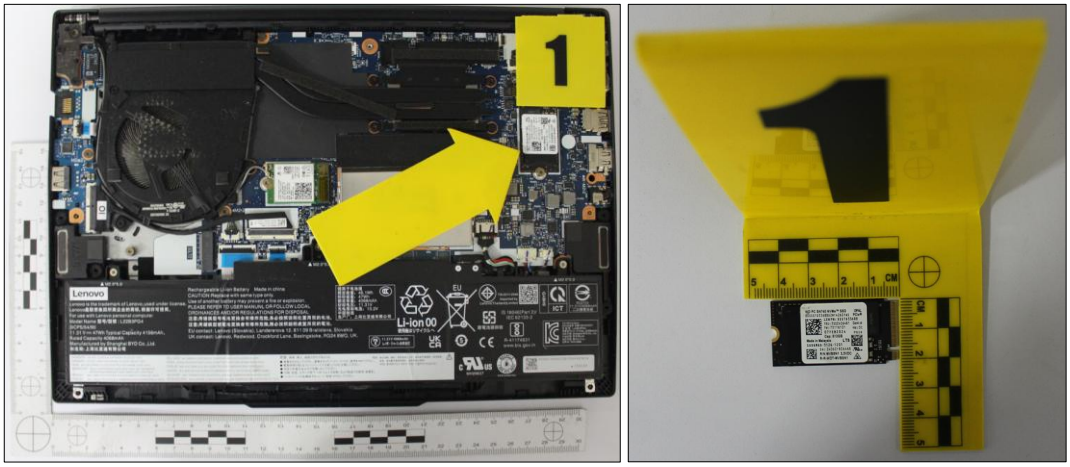
En atención a lo solicitado se realizó el procedimiento de extracción forense (aseguramiento de evidencia digital en equipos de cómputo). De la siguiente manera:

1. **Obtención de imágenes forenses**

Se procede a documentar la obtención de imágenes forenses de los equipos de cómputo objeto de estudio:

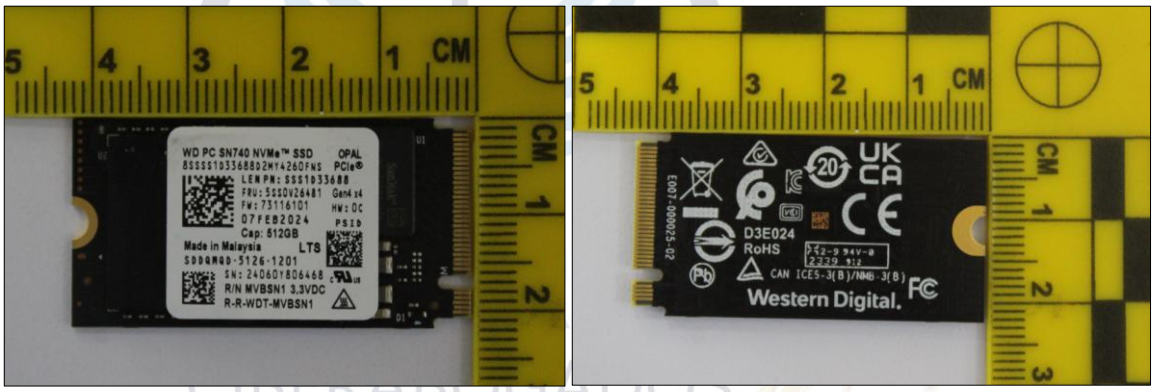
1.1. Computador portátil marca **Lenovo ThinkPad**, identificado con el número de activo **EPD00402**.

Se procede a destapar el equipo de cómputo de forma segura y controlada, ubicando e identificando el disco duro, el cual es rotulado con el numeral 1.



IMÁGENES 10 Y 11. Fotografías de primer plano donde se observa la identificación del disco duro

Una vez identificado el disco duro, se procede a su extracción de manera controlada. Dicho disco corresponde a una unidad de estado sólido (SSD), marca Western Digital, con una capacidad de 512 GB, identificado con el número de serie 24060Y806468.



IMÁGENES 12 Y 13. Fotografías de primerísimo plano donde se observa la identificación del disco duro

Una vez identificado el disco duro, se procede a conectarlo a una carcasa externa USB para SSD M.2, con el fin de que sea reconocido por la herramienta forense Tableau TD3 Forensic Imager. Esta herramienta permite la adquisición de una imagen forense del disco, garantizando la autenticidad e integridad de la información mediante la obtención de valores hash. El disco es conectado a través del bloqueador de escritura, con el propósito de impedir cualquier modificación sobre la información original contenida en el medio de almacenamiento.



IMAGEN 14. Fotografía de primer plano, donde se observa el disco duro de estado sólido (SSD), conectado al Tableau TD3 Forensic Imager.

Una vez finalizada la adquisición de la imagen forense, se obtiene el registro (log) de ejecución, en el cual consta el resultado exitoso del procedimiento, así como los datos técnicos asociados al proceso de adquisición.

```
----------Start of TD3 Log Entry----------

Task: Disk Image
Status: Ok
Created: Fri Nov 21 10:14:34 2025
Started: Fri Nov 21 10:14:34 2025
Closed: Fri Nov 21 15:45:40 2025
Elapsed: 5 hours 31 min
User: YEFRIN GARAVITO Y ANDRES DIAZ
Case ID:
 001
Case Notes:
 CASO JUNTA NACIONAL DE CALIFICACIÓN DE INVALIDEZ

Imager App: TD3
Imager Ver: 1.6.0
TD3 S/N: 000ecc01d3b086

----------Source Disk----------

Interface: USB
Model: Realtek RTL9210B-CG
```

Firmware revision: 1.00
Serial number: 0000000000000000
USB Serial number: 012345679250
Capacity in bytes: 512,110,190,592 (512.1 GB)
Block Size: 512 bytes
Block Count: 1,000,215,216

----------Destination Disk----------

Interface: USB
Model: TOSHIBA EXTERNAL_USB
Firmware revision: 5438
Serial number: 20250115009532F
USB Serial number: 20250115009532F
Capacity in bytes: 1,000,204,883,968 (1.0 TB)
Block Size: 512 bytes
Block Count: 1,953,525,164

----------Disk Imaging Results----------

Output file format: E01 - EnCase format
Chunk size in bytes: 2,147,483,648 (2.1 GB)
Chunks written: 95
Filename of first chunk: 1. IMAGUEN FORENSE PC PORTATIL LENOVO/2025-11-21_10-14-33/2025-11-21_10-14-33.E01
Total errors: 0
Acquisition MD5: c2e218393127845243e62a669c8df711
Acquisition SHA-1: 7e15c6f1542d73dba7e6cffc322d9d8a8c1ef612

----------Readback Verification Results----------

Verification MD5: c2e218393127845243e62a669c8df711
Verification SHA-1: 7e15c6f1542d73dba7e6cffc322d9d8a8c1ef612
Status: Verified

----------End of TD3 Log Entry----------

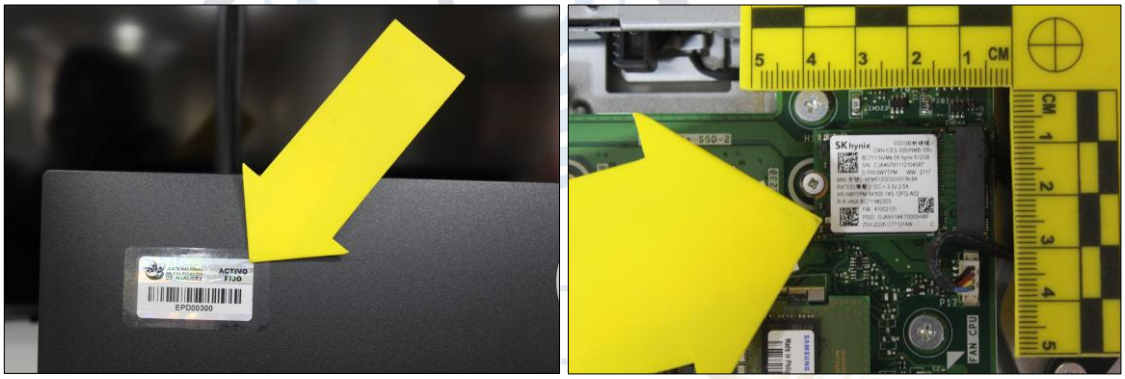
TABLA 1. En esta tabla se observa el log de la imagen forense

1.2. Computador marca **DELL**, modelo **W21B**, tipo todo en uno, con el número de activo **EPD00300**.

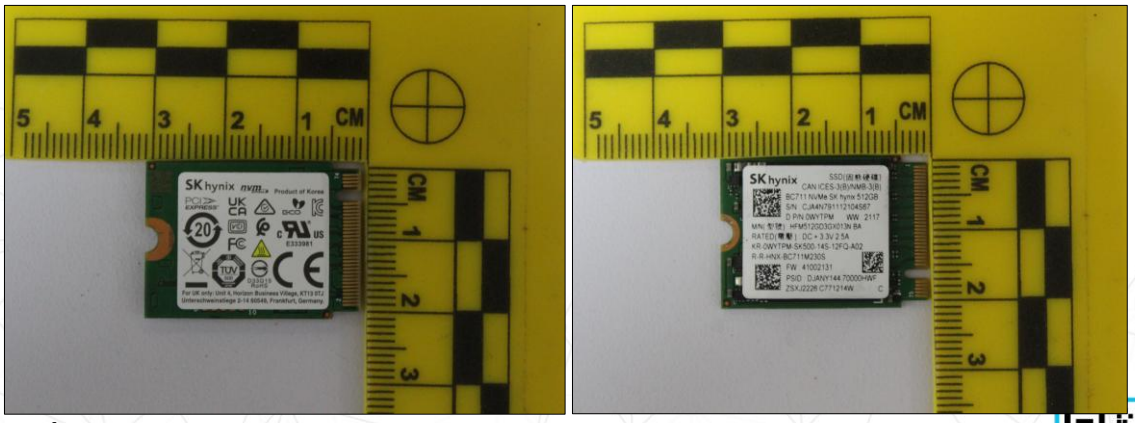
De igual forma, se procede a destapar el equipo de cómputo marca DELL, modelo **W21B**, con el propósito de identificar el disco duro y dar inicio al procedimiento de copiado forense.



IMÁGENES 15 Y 16. Fotografías de primer plano, donde se observa parte anverso del equipo de cómputo.



IMÁGENES 17 Y 18. Fotografías de primer plano, donde se identifica y se observa el número de activo EPD00300 y el disco duro parte anverso .



IMÁGENES 19 Y 20. Fotografías de primer plano, donde se observa parte anverso del disco duro y conectado a una carcasa externa USB para SSD M.2.

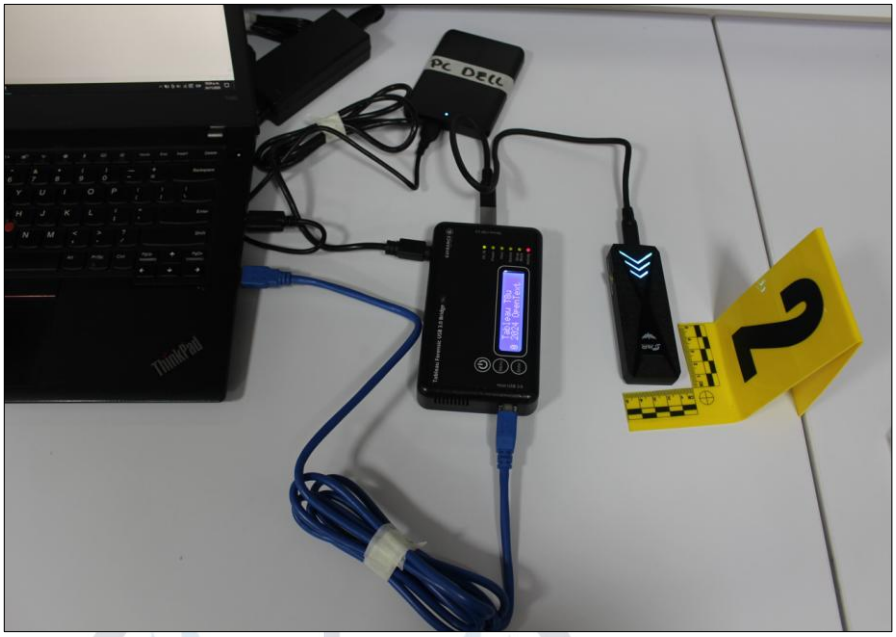


IMAGEN 21. Fotografías de primer plano, donde se observa el disco duro conectado a una carcasa externa USB para SSD M.2.

De igual forma, al equipo identificado como PC 2 se le aplica el mismo procedimiento técnico-forense realizado con el PC identificado como evidencia No. 1. Una vez identificado el disco duro, se procede a conectarlo a una carcasa externa USB para SSD M.2, con el fin de que sea reconocido por la herramienta forense Tableau TD3 Forensic Imager. Dicha herramienta permite la adquisición de una imagen forense del disco, garantizando la autenticidad e integridad de la información mediante la obtención de valores hash. El disco es conectado a través de un bloqueador de escritura, con el propósito de impedir cualquier modificación sobre la información original contenida en el medio de almacenamiento (ver imagen 18)

Una vez finalizada la adquisición de la imagen forense, se obtiene el registro (log) de ejecución, en el cual consta el resultado exitoso del procedimiento, así como los datos técnicos asociados al proceso de adquisición.

Created By Exterro® FTK® Imager 4.7.3.81

Case Information:
Acquired using: ADI4.7.3.81
Case Number: 001
Evidence Number: Evidencia No. 2
Unique description: Imagen forense fisica
Examiner: Yefrin Garavito y Andrés Díaz
Notes: Imagen forense PC DELL

Information for D:\1. Imagen Forense PC DELL\Imagen forense fisica:

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 62,260
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 1,000,215,216
[Physical Drive Information]
Drive Model: Realtek RTL9210B-CG USB Device
Drive Serial Number: 0000000000000000
Drive Interface Type: USB
Removable drive: False
Source data size: 488386 MB
Sector count: 1000215216
[Computed Hashes]
MD5 checksum: 3f788401466bfa1ad8a623b919752621
SHA1 checksum: d6e0156b02c262b2b4cdf9006873c09e7eab7e62

Image Information:
Acquisition started: Mon Nov 24 10:23:20 2025
Acquisition finished: Mon Nov 24 13:40:12 2025
Segment list:
D:\1. Imagen Forense PC DELL\Imagen forense fisica.001
D:\1. Imagen Forense PC DELL\Imagen forense fisica.002
D:\1. Imagen Forense PC DELL\Imagen forense fisica.003
D:\1. Imagen Forense PC DELL\Imagen forense fisica.004
D:\1. Imagen Forense PC DELL\Imagen forense fisica.005
D:\1. Imagen Forense PC DELL\Imagen forense fisica.006
D:\1. Imagen Forense PC DELL\Imagen forense fisica.007
D:\1. Imagen Forense PC DELL\Imagen forense fisica.008
D:\1. Imagen Forense PC DELL\Imagen forense fisica.009
D:\1. Imagen Forense PC DELL\Imagen forense fisica.010
D:\1. Imagen Forense PC DELL\Imagen forense fisica.011
D:\1. Imagen Forense PC DELL\Imagen forense fisica.012
D:\1. Imagen Forense PC DELL\Imagen forense fisica.013
D:\1. Imagen Forense PC DELL\Imagen forense fisica.014
D:\1. Imagen Forense PC DELL\Imagen forense fisica.015
D:\1. Imagen Forense PC DELL\Imagen forense fisica.016
D:\1. Imagen Forense PC DELL\Imagen forense fisica.017
D:\1. Imagen Forense PC DELL\Imagen forense fisica.018
D:\1. Imagen Forense PC DELL\Imagen forense fisica.019
D:\1. Imagen Forense PC DELL\Imagen forense fisica.020
D:\1. Imagen Forense PC DELL\Imagen forense fisica.021
D:\1. Imagen Forense PC DELL\Imagen forense fisica.022
D:\1. Imagen Forense PC DELL\Imagen forense fisica.023
D:\1. Imagen Forense PC DELL\Imagen forense fisica.024
D:\1. Imagen Forense PC DELL\Imagen forense fisica.025
D:\1. Imagen Forense PC DELL\Imagen forense fisica.026
D:\1. Imagen Forense PC DELL\Imagen forense fisica.027
D:\1. Imagen Forense PC DELL\Imagen forense fisica.028

D:\1. Imagen Forense PC DELL\Imagen forense fisica.029
D:\1. Imagen Forense PC DELL\Imagen forense fisica.030
D:\1. Imagen Forense PC DELL\Imagen forense fisica.031
D:\1. Imagen Forense PC DELL\Imagen forense fisica.032
D:\1. Imagen Forense PC DELL\Imagen forense fisica.033
D:\1. Imagen Forense PC DELL\Imagen forense fisica.034
D:\1. Imagen Forense PC DELL\Imagen forense fisica.035
D:\1. Imagen Forense PC DELL\Imagen forense fisica.036
D:\1. Imagen Forense PC DELL\Imagen forense fisica.037
D:\1. Imagen Forense PC DELL\Imagen forense fisica.038
D:\1. Imagen Forense PC DELL\Imagen forense fisica.039
D:\1. Imagen Forense PC DELL\Imagen forense fisica.040
D:\1. Imagen Forense PC DELL\Imagen forense fisica.041
D:\1. Imagen Forense PC DELL\Imagen forense fisica.042
D:\1. Imagen Forense PC DELL\Imagen forense fisica.043
D:\1. Imagen Forense PC DELL\Imagen forense fisica.044
D:\1. Imagen Forense PC DELL\Imagen forense fisica.045
D:\1. Imagen Forense PC DELL\Imagen forense fisica.046
D:\1. Imagen Forense PC DELL\Imagen forense fisica.047
D:\1. Imagen Forense PC DELL\Imagen forense fisica.048
D:\1. Imagen Forense PC DELL\Imagen forense fisica.049
D:\1. Imagen Forense PC DELL\Imagen forense fisica.050
D:\1. Imagen Forense PC DELL\Imagen forense fisica.051
D:\1. Imagen Forense PC DELL\Imagen forense fisica.052
D:\1. Imagen Forense PC DELL\Imagen forense fisica.053
D:\1. Imagen Forense PC DELL\Imagen forense fisica.054
D:\1. Imagen Forense PC DELL\Imagen forense fisica.055
D:\1. Imagen Forense PC DELL\Imagen forense fisica.056
D:\1. Imagen Forense PC DELL\Imagen forense fisica.057
D:\1. Imagen Forense PC DELL\Imagen forense fisica.058
D:\1. Imagen Forense PC DELL\Imagen forense fisica.059
D:\1. Imagen Forense PC DELL\Imagen forense fisica.060
D:\1. Imagen Forense PC DELL\Imagen forense fisica.061
D:\1. Imagen Forense PC DELL\Imagen forense fisica.062
D:\1. Imagen Forense PC DELL\Imagen forense fisica.063
D:\1. Imagen Forense PC DELL\Imagen forense fisica.064
D:\1. Imagen Forense PC DELL\Imagen forense fisica.065
D:\1. Imagen Forense PC DELL\Imagen forense fisica.066
D:\1. Imagen Forense PC DELL\Imagen forense fisica.067
D:\1. Imagen Forense PC DELL\Imagen forense fisica.068
D:\1. Imagen Forense PC DELL\Imagen forense fisica.069
D:\1. Imagen Forense PC DELL\Imagen forense fisica.070
D:\1. Imagen Forense PC DELL\Imagen forense fisica.071
D:\1. Imagen Forense PC DELL\Imagen forense fisica.072
D:\1. Imagen Forense PC DELL\Imagen forense fisica.073
D:\1. Imagen Forense PC DELL\Imagen forense fisica.074
D:\1. Imagen Forense PC DELL\Imagen forense fisica.075
D:\1. Imagen Forense PC DELL\Imagen forense fisica.076
D:\1. Imagen Forense PC DELL\Imagen forense fisica.077
D:\1. Imagen Forense PC DELL\Imagen forense fisica.078
D:\1. Imagen Forense PC DELL\Imagen forense fisica.079
D:\1. Imagen Forense PC DELL\Imagen forense fisica.080

D:\1. Imagen Forense PC DELL\Imagen forense fisica.081
D:\1. Imagen Forense PC DELL\Imagen forense fisica.082
D:\1. Imagen Forense PC DELL\Imagen forense fisica.083
D:\1. Imagen Forense PC DELL\Imagen forense fisica.084
D:\1. Imagen Forense PC DELL\Imagen forense fisica.085
D:\1. Imagen Forense PC DELL\Imagen forense fisica.086
D:\1. Imagen Forense PC DELL\Imagen forense fisica.087
D:\1. Imagen Forense PC DELL\Imagen forense fisica.088
D:\1. Imagen Forense PC DELL\Imagen forense fisica.089
D:\1. Imagen Forense PC DELL\Imagen forense fisica.090
D:\1. Imagen Forense PC DELL\Imagen forense fisica.091
D:\1. Imagen Forense PC DELL\Imagen forense fisica.092
D:\1. Imagen Forense PC DELL\Imagen forense fisica.093
D:\1. Imagen Forense PC DELL\Imagen forense fisica.094
D:\1. Imagen Forense PC DELL\Imagen forense fisica.095
D:\1. Imagen Forense PC DELL\Imagen forense fisica.096
D:\1. Imagen Forense PC DELL\Imagen forense fisica.097
D:\1. Imagen Forense PC DELL\Imagen forense fisica.098
D:\1. Imagen Forense PC DELL\Imagen forense fisica.099
D:\1. Imagen Forense PC DELL\Imagen forense fisica.100
D:\1. Imagen Forense PC DELL\Imagen forense fisica.101
D:\1. Imagen Forense PC DELL\Imagen forense fisica.102
D:\1. Imagen Forense PC DELL\Imagen forense fisica.103
D:\1. Imagen Forense PC DELL\Imagen forense fisica.104
D:\1. Imagen Forense PC DELL\Imagen forense fisica.105
D:\1. Imagen Forense PC DELL\Imagen forense fisica.106
D:\1. Imagen Forense PC DELL\Imagen forense fisica.107
D:\1. Imagen Forense PC DELL\Imagen forense fisica.108
D:\1. Imagen Forense PC DELL\Imagen forense fisica.109
D:\1. Imagen Forense PC DELL\Imagen forense fisica.110
D:\1. Imagen Forense PC DELL\Imagen forense fisica.111
D:\1. Imagen Forense PC DELL\Imagen forense fisica.112
D:\1. Imagen Forense PC DELL\Imagen forense fisica.113
D:\1. Imagen Forense PC DELL\Imagen forense fisica.114
D:\1. Imagen Forense PC DELL\Imagen forense fisica.115
D:\1. Imagen Forense PC DELL\Imagen forense fisica.116
D:\1. Imagen Forense PC DELL\Imagen forense fisica.117
D:\1. Imagen Forense PC DELL\Imagen forense fisica.118
D:\1. Imagen Forense PC DELL\Imagen forense fisica.119
D:\1. Imagen Forense PC DELL\Imagen forense fisica.120
D:\1. Imagen Forense PC DELL\Imagen forense fisica.121
D:\1. Imagen Forense PC DELL\Imagen forense fisica.122
D:\1. Imagen Forense PC DELL\Imagen forense fisica.123
D:\1. Imagen Forense PC DELL\Imagen forense fisica.124
D:\1. Imagen Forense PC DELL\Imagen forense fisica.125
D:\1. Imagen Forense PC DELL\Imagen forense fisica.126
D:\1. Imagen Forense PC DELL\Imagen forense fisica.127
D:\1. Imagen Forense PC DELL\Imagen forense fisica.128
D:\1. Imagen Forense PC DELL\Imagen forense fisica.129
D:\1. Imagen Forense PC DELL\Imagen forense fisica.130
D:\1. Imagen Forense PC DELL\Imagen forense fisica.131
D:\1. Imagen Forense PC DELL\Imagen forense fisica.132

D:\1. Imagen Forense PC DELL\Imagen forense fisica.133
D:\1. Imagen Forense PC DELL\Imagen forense fisica.134
D:\1. Imagen Forense PC DELL\Imagen forense fisica.135
D:\1. Imagen Forense PC DELL\Imagen forense fisica.136
D:\1. Imagen Forense PC DELL\Imagen forense fisica.137
D:\1. Imagen Forense PC DELL\Imagen forense fisica.138
D:\1. Imagen Forense PC DELL\Imagen forense fisica.139
D:\1. Imagen Forense PC DELL\Imagen forense fisica.140
D:\1. Imagen Forense PC DELL\Imagen forense fisica.141
D:\1. Imagen Forense PC DELL\Imagen forense fisica.142
D:\1. Imagen Forense PC DELL\Imagen forense fisica.143
D:\1. Imagen Forense PC DELL\Imagen forense fisica.144
D:\1. Imagen Forense PC DELL\Imagen forense fisica.145
D:\1. Imagen Forense PC DELL\Imagen forense fisica.146
D:\1. Imagen Forense PC DELL\Imagen forense fisica.147
D:\1. Imagen Forense PC DELL\Imagen forense fisica.148
D:\1. Imagen Forense PC DELL\Imagen forense fisica.149
D:\1. Imagen Forense PC DELL\Imagen forense fisica.150
D:\1. Imagen Forense PC DELL\Imagen forense fisica.151
D:\1. Imagen Forense PC DELL\Imagen forense fisica.152
D:\1. Imagen Forense PC DELL\Imagen forense fisica.153
D:\1. Imagen Forense PC DELL\Imagen forense fisica.154
D:\1. Imagen Forense PC DELL\Imagen forense fisica.155
D:\1. Imagen Forense PC DELL\Imagen forense fisica.156
D:\1. Imagen Forense PC DELL\Imagen forense fisica.157
D:\1. Imagen Forense PC DELL\Imagen forense fisica.158
D:\1. Imagen Forense PC DELL\Imagen forense fisica.159
D:\1. Imagen Forense PC DELL\Imagen forense fisica.160
D:\1. Imagen Forense PC DELL\Imagen forense fisica.161
D:\1. Imagen Forense PC DELL\Imagen forense fisica.162
D:\1. Imagen Forense PC DELL\Imagen forense fisica.163
D:\1. Imagen Forense PC DELL\Imagen forense fisica.164
D:\1. Imagen Forense PC DELL\Imagen forense fisica.165
D:\1. Imagen Forense PC DELL\Imagen forense fisica.166
D:\1. Imagen Forense PC DELL\Imagen forense fisica.167
D:\1. Imagen Forense PC DELL\Imagen forense fisica.168
D:\1. Imagen Forense PC DELL\Imagen forense fisica.169
D:\1. Imagen Forense PC DELL\Imagen forense fisica.170
D:\1. Imagen Forense PC DELL\Imagen forense fisica.171
D:\1. Imagen Forense PC DELL\Imagen forense fisica.172
D:\1. Imagen Forense PC DELL\Imagen forense fisica.173
D:\1. Imagen Forense PC DELL\Imagen forense fisica.174
D:\1. Imagen Forense PC DELL\Imagen forense fisica.175
D:\1. Imagen Forense PC DELL\Imagen forense fisica.176
D:\1. Imagen Forense PC DELL\Imagen forense fisica.177
D:\1. Imagen Forense PC DELL\Imagen forense fisica.178
D:\1. Imagen Forense PC DELL\Imagen forense fisica.179
D:\1. Imagen Forense PC DELL\Imagen forense fisica.180
D:\1. Imagen Forense PC DELL\Imagen forense fisica.181
D:\1. Imagen Forense PC DELL\Imagen forense fisica.182
D:\1. Imagen Forense PC DELL\Imagen forense fisica.183
D:\1. Imagen Forense PC DELL\Imagen forense fisica.184

D:\1. Imagen Forense PC DELL\Imagen forense fisica.185
D:\1. Imagen Forense PC DELL\Imagen forense fisica.186
D:\1. Imagen Forense PC DELL\Imagen forense fisica.187
D:\1. Imagen Forense PC DELL\Imagen forense fisica.188
D:\1. Imagen Forense PC DELL\Imagen forense fisica.189
D:\1. Imagen Forense PC DELL\Imagen forense fisica.190
D:\1. Imagen Forense PC DELL\Imagen forense fisica.191
D:\1. Imagen Forense PC DELL\Imagen forense fisica.192
D:\1. Imagen Forense PC DELL\Imagen forense fisica.193
D:\1. Imagen Forense PC DELL\Imagen forense fisica.194
D:\1. Imagen Forense PC DELL\Imagen forense fisica.195
D:\1. Imagen Forense PC DELL\Imagen forense fisica.196
D:\1. Imagen Forense PC DELL\Imagen forense fisica.197
D:\1. Imagen Forense PC DELL\Imagen forense fisica.198
D:\1. Imagen Forense PC DELL\Imagen forense fisica.199
D:\1. Imagen Forense PC DELL\Imagen forense fisica.200
D:\1. Imagen Forense PC DELL\Imagen forense fisica.201
D:\1. Imagen Forense PC DELL\Imagen forense fisica.202
D:\1. Imagen Forense PC DELL\Imagen forense fisica.203
D:\1. Imagen Forense PC DELL\Imagen forense fisica.204
D:\1. Imagen Forense PC DELL\Imagen forense fisica.205
D:\1. Imagen Forense PC DELL\Imagen forense fisica.206
D:\1. Imagen Forense PC DELL\Imagen forense fisica.207
D:\1. Imagen Forense PC DELL\Imagen forense fisica.208
D:\1. Imagen Forense PC DELL\Imagen forense fisica.209
D:\1. Imagen Forense PC DELL\Imagen forense fisica.210
D:\1. Imagen Forense PC DELL\Imagen forense fisica.211
D:\1. Imagen Forense PC DELL\Imagen forense fisica.212
D:\1. Imagen Forense PC DELL\Imagen forense fisica.213
D:\1. Imagen Forense PC DELL\Imagen forense fisica.214
D:\1. Imagen Forense PC DELL\Imagen forense fisica.215
D:\1. Imagen Forense PC DELL\Imagen forense fisica.216
D:\1. Imagen Forense PC DELL\Imagen forense fisica.217
D:\1. Imagen Forense PC DELL\Imagen forense fisica.218
D:\1. Imagen Forense PC DELL\Imagen forense fisica.219
D:\1. Imagen Forense PC DELL\Imagen forense fisica.220
D:\1. Imagen Forense PC DELL\Imagen forense fisica.221
D:\1. Imagen Forense PC DELL\Imagen forense fisica.222
D:\1. Imagen Forense PC DELL\Imagen forense fisica.223
D:\1. Imagen Forense PC DELL\Imagen forense fisica.224
D:\1. Imagen Forense PC DELL\Imagen forense fisica.225
D:\1. Imagen Forense PC DELL\Imagen forense fisica.226
D:\1. Imagen Forense PC DELL\Imagen forense fisica.227
D:\1. Imagen Forense PC DELL\Imagen forense fisica.228
D:\1. Imagen Forense PC DELL\Imagen forense fisica.229
D:\1. Imagen Forense PC DELL\Imagen forense fisica.230
D:\1. Imagen Forense PC DELL\Imagen forense fisica.231
D:\1. Imagen Forense PC DELL\Imagen forense fisica.232
D:\1. Imagen Forense PC DELL\Imagen forense fisica.233
D:\1. Imagen Forense PC DELL\Imagen forense fisica.234
D:\1. Imagen Forense PC DELL\Imagen forense fisica.235
D:\1. Imagen Forense PC DELL\Imagen forense fisica.236

D:\1. Imagen Forense PC DELL\Imagen forense fisica.237
D:\1. Imagen Forense PC DELL\Imagen forense fisica.238
D:\1. Imagen Forense PC DELL\Imagen forense fisica.239
D:\1. Imagen Forense PC DELL\Imagen forense fisica.240
D:\1. Imagen Forense PC DELL\Imagen forense fisica.241
D:\1. Imagen Forense PC DELL\Imagen forense fisica.242
D:\1. Imagen Forense PC DELL\Imagen forense fisica.243
D:\1. Imagen Forense PC DELL\Imagen forense fisica.244
D:\1. Imagen Forense PC DELL\Imagen forense fisica.245
D:\1. Imagen Forense PC DELL\Imagen forense fisica.246
D:\1. Imagen Forense PC DELL\Imagen forense fisica.247
D:\1. Imagen Forense PC DELL\Imagen forense fisica.248
D:\1. Imagen Forense PC DELL\Imagen forense fisica.249
D:\1. Imagen Forense PC DELL\Imagen forense fisica.250
D:\1. Imagen Forense PC DELL\Imagen forense fisica.251
D:\1. Imagen Forense PC DELL\Imagen forense fisica.252
D:\1. Imagen Forense PC DELL\Imagen forense fisica.253
D:\1. Imagen Forense PC DELL\Imagen forense fisica.254
D:\1. Imagen Forense PC DELL\Imagen forense fisica.255
D:\1. Imagen Forense PC DELL\Imagen forense fisica.256
D:\1. Imagen Forense PC DELL\Imagen forense fisica.257
D:\1. Imagen Forense PC DELL\Imagen forense fisica.258
D:\1. Imagen Forense PC DELL\Imagen forense fisica.259
D:\1. Imagen Forense PC DELL\Imagen forense fisica.260
D:\1. Imagen Forense PC DELL\Imagen forense fisica.261
D:\1. Imagen Forense PC DELL\Imagen forense fisica.262
D:\1. Imagen Forense PC DELL\Imagen forense fisica.263
D:\1. Imagen Forense PC DELL\Imagen forense fisica.264
D:\1. Imagen Forense PC DELL\Imagen forense fisica.265
D:\1. Imagen Forense PC DELL\Imagen forense fisica.266
D:\1. Imagen Forense PC DELL\Imagen forense fisica.267
D:\1. Imagen Forense PC DELL\Imagen forense fisica.268
D:\1. Imagen Forense PC DELL\Imagen forense fisica.269
D:\1. Imagen Forense PC DELL\Imagen forense fisica.270
D:\1. Imagen Forense PC DELL\Imagen forense fisica.271
D:\1. Imagen Forense PC DELL\Imagen forense fisica.272
D:\1. Imagen Forense PC DELL\Imagen forense fisica.273
D:\1. Imagen Forense PC DELL\Imagen forense fisica.274
D:\1. Imagen Forense PC DELL\Imagen forense fisica.275
D:\1. Imagen Forense PC DELL\Imagen forense fisica.276
D:\1. Imagen Forense PC DELL\Imagen forense fisica.277
D:\1. Imagen Forense PC DELL\Imagen forense fisica.278
D:\1. Imagen Forense PC DELL\Imagen forense fisica.279
D:\1. Imagen Forense PC DELL\Imagen forense fisica.280
D:\1. Imagen Forense PC DELL\Imagen forense fisica.281
D:\1. Imagen Forense PC DELL\Imagen forense fisica.282
D:\1. Imagen Forense PC DELL\Imagen forense fisica.283
D:\1. Imagen Forense PC DELL\Imagen forense fisica.284
D:\1. Imagen Forense PC DELL\Imagen forense fisica.285
D:\1. Imagen Forense PC DELL\Imagen forense fisica.286
D:\1. Imagen Forense PC DELL\Imagen forense fisica.287
D:\1. Imagen Forense PC DELL\Imagen forense fisica.288

D:\1. Imagen Forense PC DELL\Imagen forense fisica.289
D:\1. Imagen Forense PC DELL\Imagen forense fisica.290
D:\1. Imagen Forense PC DELL\Imagen forense fisica.291
D:\1. Imagen Forense PC DELL\Imagen forense fisica.292
D:\1. Imagen Forense PC DELL\Imagen forense fisica.293
D:\1. Imagen Forense PC DELL\Imagen forense fisica.294
D:\1. Imagen Forense PC DELL\Imagen forense fisica.295
D:\1. Imagen Forense PC DELL\Imagen forense fisica.296
D:\1. Imagen Forense PC DELL\Imagen forense fisica.297
D:\1. Imagen Forense PC DELL\Imagen forense fisica.298
D:\1. Imagen Forense PC DELL\Imagen forense fisica.299
D:\1. Imagen Forense PC DELL\Imagen forense fisica.300
D:\1. Imagen Forense PC DELL\Imagen forense fisica.301
D:\1. Imagen Forense PC DELL\Imagen forense fisica.302
D:\1. Imagen Forense PC DELL\Imagen forense fisica.303
D:\1. Imagen Forense PC DELL\Imagen forense fisica.304
D:\1. Imagen Forense PC DELL\Imagen forense fisica.305
D:\1. Imagen Forense PC DELL\Imagen forense fisica.306
D:\1. Imagen Forense PC DELL\Imagen forense fisica.307
D:\1. Imagen Forense PC DELL\Imagen forense fisica.308
D:\1. Imagen Forense PC DELL\Imagen forense fisica.309
D:\1. Imagen Forense PC DELL\Imagen forense fisica.310
D:\1. Imagen Forense PC DELL\Imagen forense fisica.311
D:\1. Imagen Forense PC DELL\Imagen forense fisica.312
D:\1. Imagen Forense PC DELL\Imagen forense fisica.313
D:\1. Imagen Forense PC DELL\Imagen forense fisica.314
D:\1. Imagen Forense PC DELL\Imagen forense fisica.315
D:\1. Imagen Forense PC DELL\Imagen forense fisica.316
D:\1. Imagen Forense PC DELL\Imagen forense fisica.317
D:\1. Imagen Forense PC DELL\Imagen forense fisica.318
D:\1. Imagen Forense PC DELL\Imagen forense fisica.319
D:\1. Imagen Forense PC DELL\Imagen forense fisica.320
D:\1. Imagen Forense PC DELL\Imagen forense fisica.321
D:\1. Imagen Forense PC DELL\Imagen forense fisica.322
D:\1. Imagen Forense PC DELL\Imagen forense fisica.323
D:\1. Imagen Forense PC DELL\Imagen forense fisica.324
D:\1. Imagen Forense PC DELL\Imagen forense fisica.325
D:\1. Imagen Forense PC DELL\Imagen forense fisica.326
COMPUTED HASH : 3f788401466bfa1ad8a623b919752621
COMPUTED HASH : d6e0156b02c262b2b4cdf9006873c09e7eab7e62

Image Verification Results:
Verification started: Mon Nov 24 13:40:12 2025
Verification finished: Mon Nov 24 14:44:50 2025
MD5 checksum: 3f788401466bfa1ad8a623b919752621 : verified
SHA1 checksum: d6e0156b02c262b2b4cdf9006873c09e7eab7e62 : verified

TABLA 2. En esta tabla se observa el log de la imagen forense

1.3. Computador portátil marca MacBook, modelo A223B y número de activo EPD00354.

Al verificar el modelo MacBook A223B, se evidencia que este equipo incorpora una unidad de estado sólido (SSD) soldada directamente a la placa lógica, lo cual impide su extracción física. Adicionalmente, este modelo cuenta con un chip de seguridad de alta protección (Apple T2 Security Chip), encargado de la gestión del cifrado del almacenamiento, el arranque seguro y la protección de la información. En consecuencia, no es posible aplicar el mismo procedimiento forense utilizado en equipos anteriores, toda vez que no se puede separar el dispositivo de almacenamiento del equipo para realizar una copia forense mediante métodos tradicionales. Por lo anterior, la adquisición de la información debe efectuarse mediante técnicas de adquisición lógica o adquisición en vivo, utilizando herramientas forenses compatibles con el sistema operativo macOS, y considerando las restricciones impuestas por el cifrado nativo del fabricante (FileVault). Para dicho procedimiento, es indispensable contar con la clave de cifrado FileVault, la cual permite el descifrado del disco y la posterior obtención de la copia forense. En este contexto, la señora Estephany Cruz Suárez, en calidad de gestora contractual de la Junta Nacional, suministró una clave de FileVault; sin embargo, al realizar las pruebas correspondientes, dicha clave no permitió el acceso ni la ejecución del procedimiento de copia de la información.



IMÁGENES 22 Y 23. fotografías de primer plano, donde se observa el procedimiento de intento de restablecimiento de la clave FileVault




IMÁGENES 24 Y 25. fotografías de primer plano, donde se observa el procedimiento de intento de restablecimiento de la clave FileVault





IMÁGENES 26 Y 27. fotografías de primer plano, donde se observa el procedimiento de intento de restablecimiento de la clave FileVault

2. Indexación de imágenes forenses.

Una vez obtenidas las imágenes forenses, se procedió a indexar cada una de ellas mediante la herramienta FTK Toolkit versión 8.2, con el fin de que la aplicación realizara el procesamiento e indexación integral de la información contenida en las imágenes forenses, permitiendo la correcta

identificación, búsqueda, análisis y recuperación de los datos obtenidos durante el proceso de adquisición.

2.1. Computador portátil marca **Lenovo ThinkPad**, identificado con el número de activo **EPD00402.**

Se procedió a abrir la imagen forense mediante la herramienta FTK Toolkit; sin embargo, al verificar su contenido, se evidenció que el equipo presentaba el disco cifrado con la tecnología BitLocker. En razón a lo anterior, se solicitó al grupo de la Junta Nacional el suministro de la clave de descifrado correspondiente. Posteriormente, la señora Estephany Cruz Suárez, en calidad de gestora contractual de la Junta Nacional, suministró la clave BitLocker de los dos equipos con sistema operativo Windows, con el fin de permitir el acceso y análisis de la información contenida en las imágenes forenses.

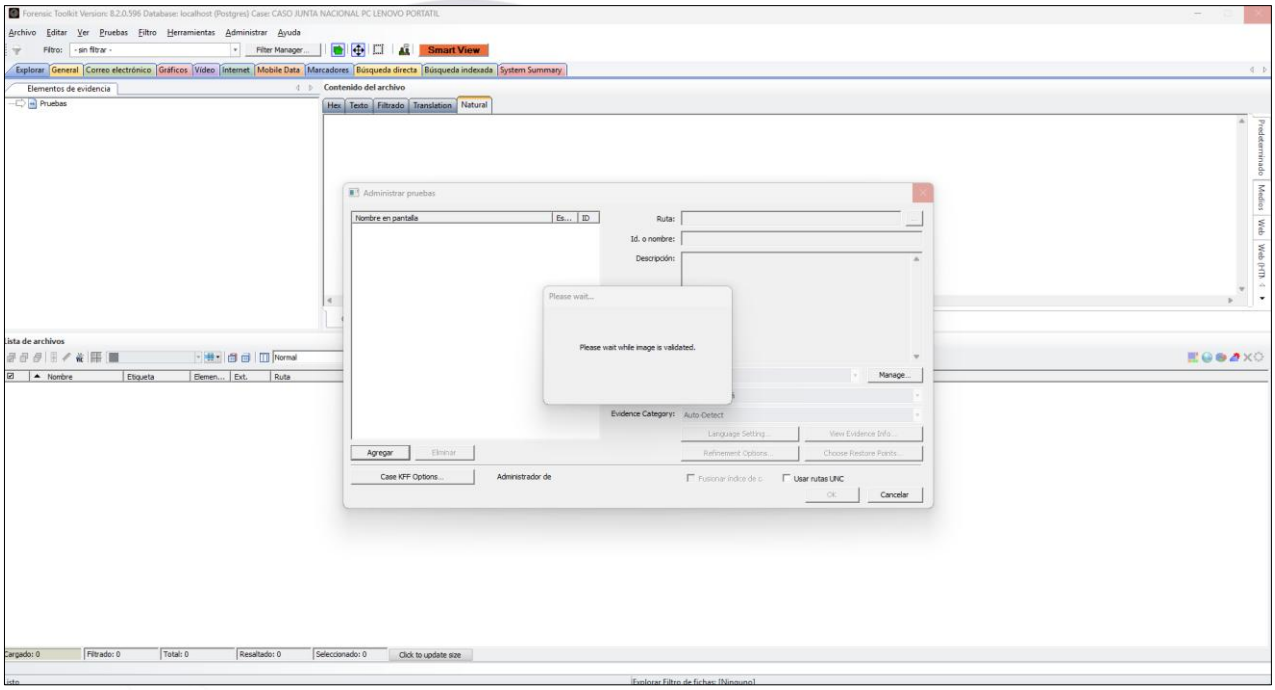


IMAGEN 28. Captura de pantalla, donde se observa la indexación de la imagen forense correspondiente al equipo **Lenovo ThinkPad**, identificado con el número de activo **EPD00402.**

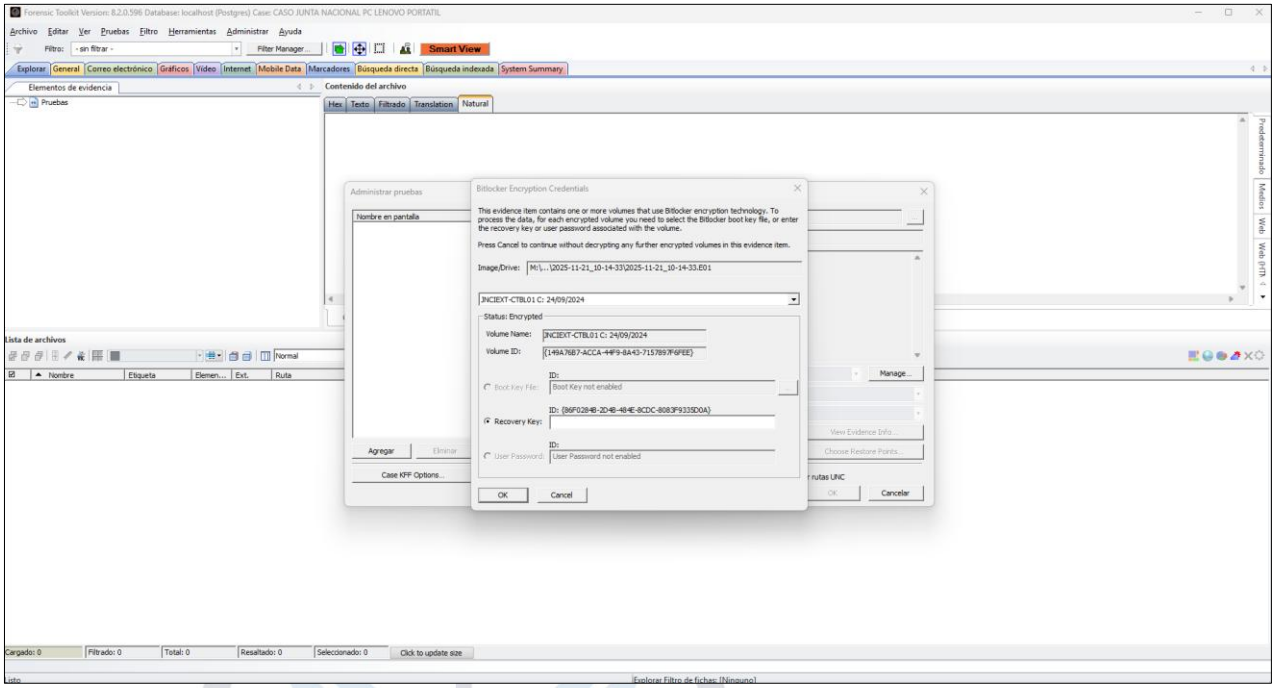


IMAGEN 29. Captura de pantalla, donde se observa la indexación de la imagen forense correspondiente al equipo **Lenovo ThinkPad**, identificado con el número de activo **EPD00402**

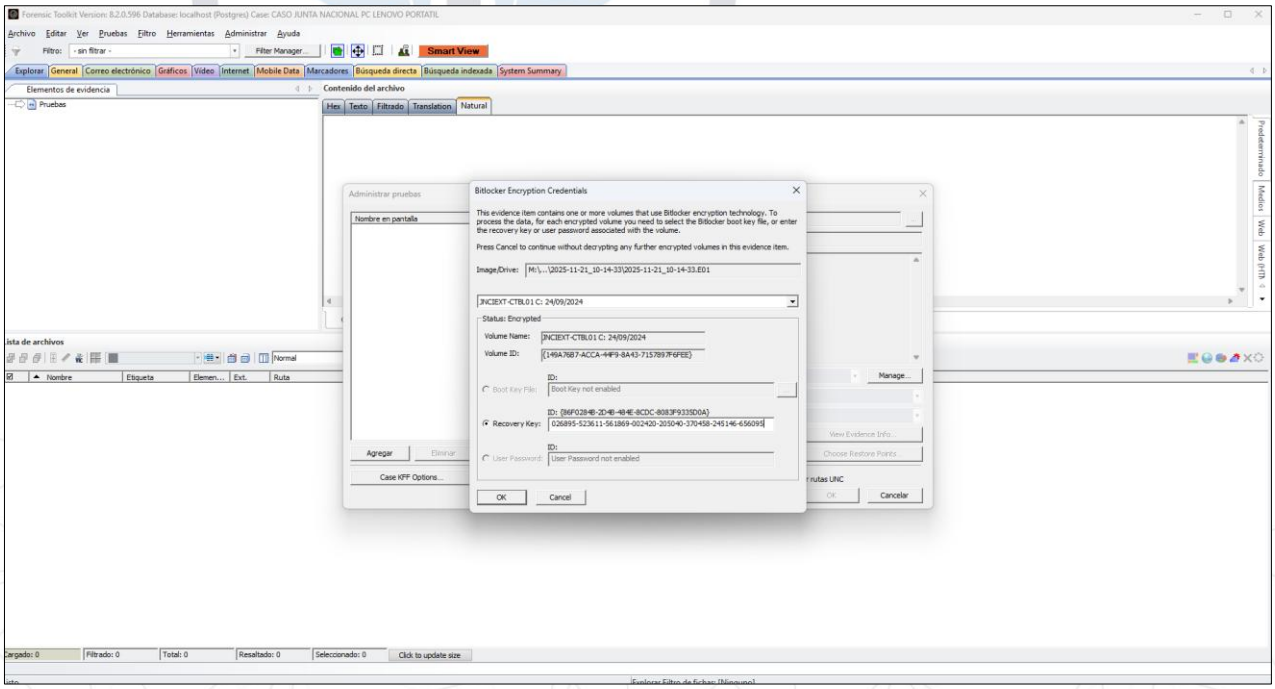


IMAGEN 30. Captura de pantalla, donde se observa la indexación de la imagen forense correspondiente al equipo **Lenovo ThinkPad**, identificado con el número de activo **EPD00402**

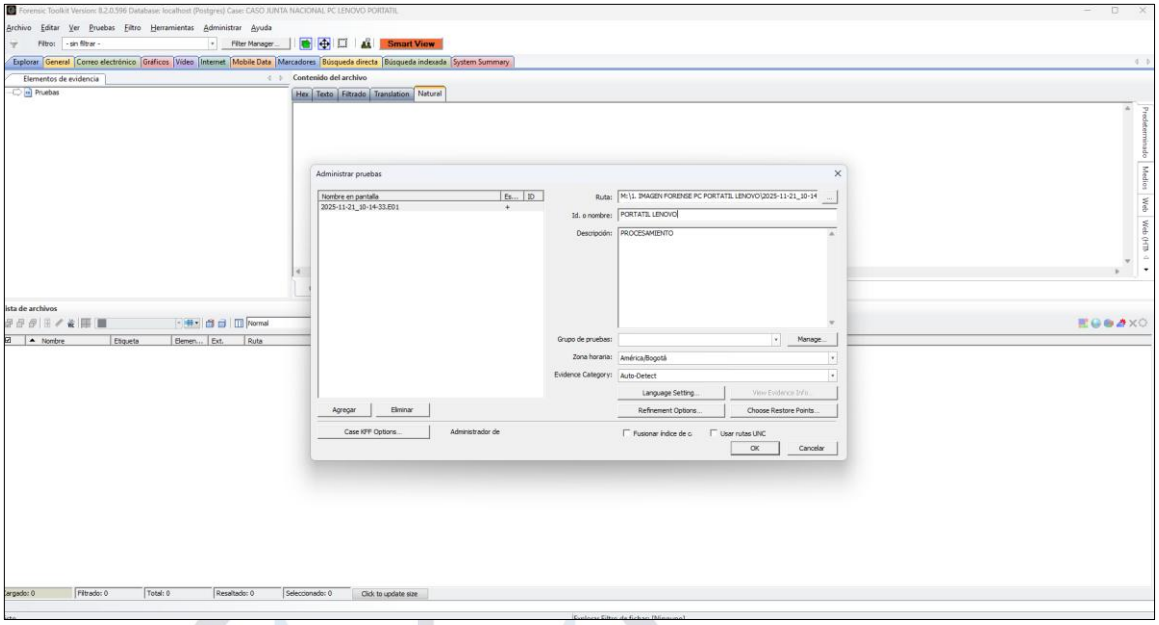


IMAGEN 31. Captura de pantalla, donde se observa la indexación de la imagen forense correspondiente al equipo **Lenovo ThinkPad**, identificado con el número de activo **EPD00402**

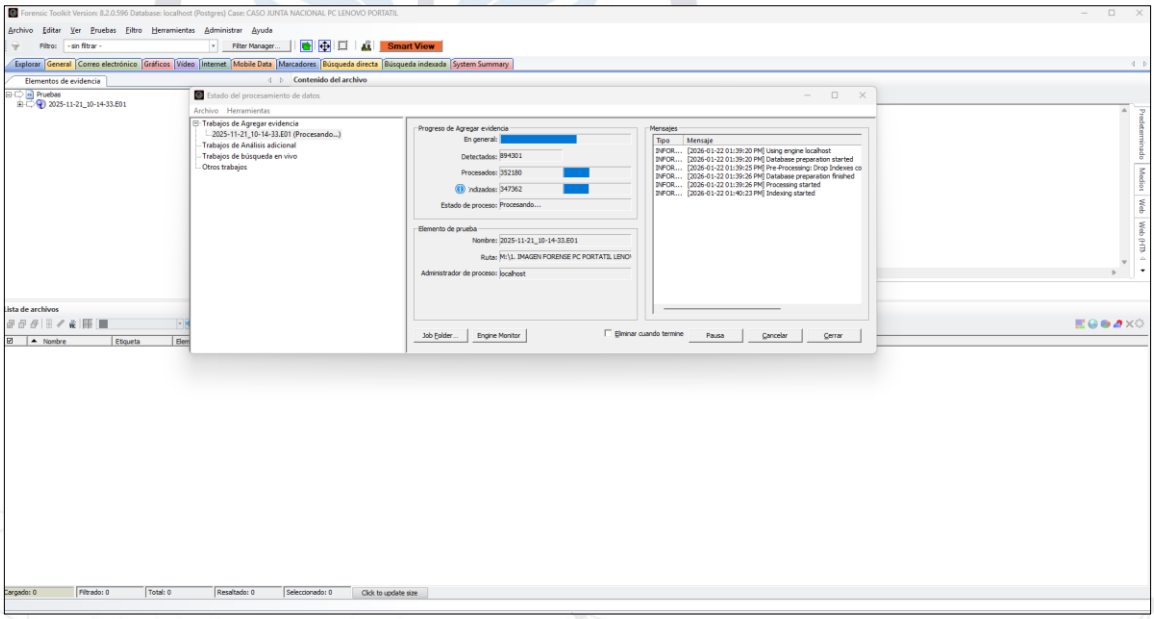


IMAGEN 32. Captura de pantalla, donde se observa la indexación de la imagen forense correspondiente al equipo **Lenovo ThinkPad**, identificado con el número de activo **EPD00402.**

Al finalizar el proceso de **indexación de la imagen forense**, se obtuvieron los siguientes resultados: la herramienta **FTK Toolkit** identificó un total aproximado de **1.119.507 archivos**, clasificados en diversas categorías, entre las que se destacan **documentos (257.066 archivos)**, **archivos gráficos (397.424)**, **archivos multimedia (1.434)**, **archivos de correo electrónico (151.392)**, **bases de datos (778)**, **ejecutables (111.351)**, **presentaciones (248)** y **hojas de cálculo (19.334)**. Así mismo, se

identificaron **86.157 carpetas** y **78.773 elementos correspondientes al sistema operativo o sistema de archivos**.

Adicionalmente, se evidenció la existencia de **179.539 archivos eliminados**, **468.988 archivos adjuntos de correo electrónico**, **625.393 elementos relacionados con correos electrónicos**, así como **419.659 archivos clasificados como tipos desconocidos** y **4.604 archivos asociados a otros métodos de cifrado**.

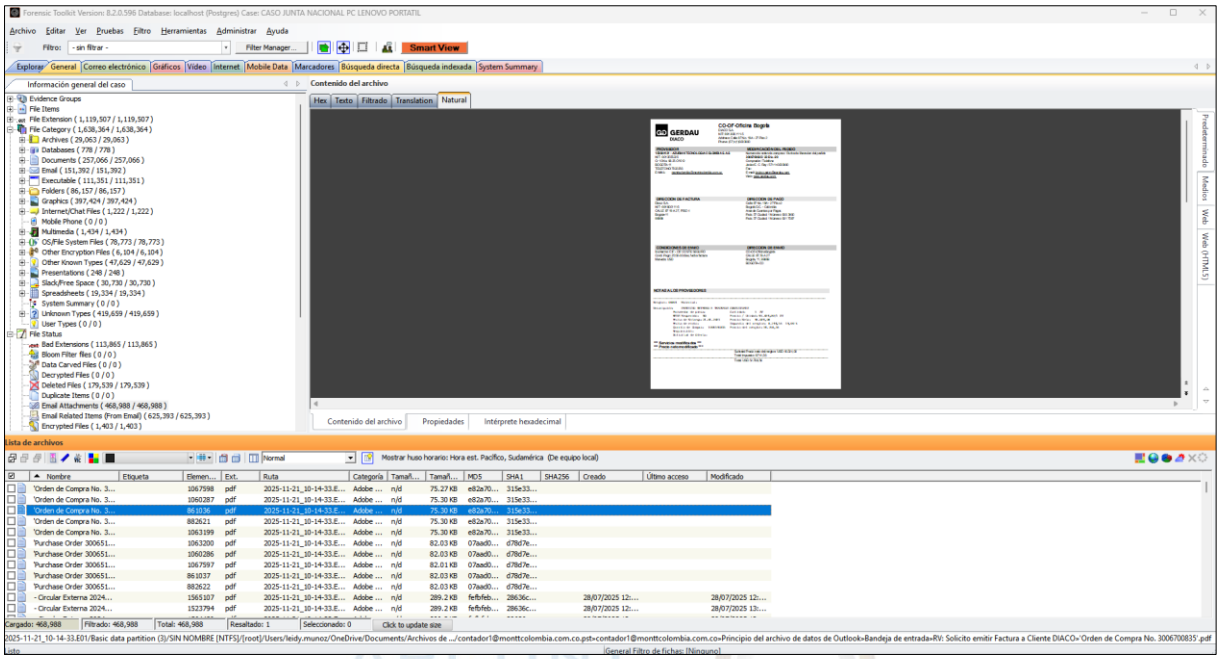


IMAGEN 33. Captura de pantalla, donde se observa los resultados de la indexación de la imagen forense correspondiente al equipo **Lenovo ThinkPad**, identificado con el número de activo **EPD00402.**

ESPACIO INTENCIONALMENTE DEJADO EN BLANCO

2.2. Computador portátil marca **DELL**, modelo **W21B**, tipo todo en uno, con el número de activo **EPD00300.**

De esta misma forma se procedió a indexar la imagen forense de este equipo:

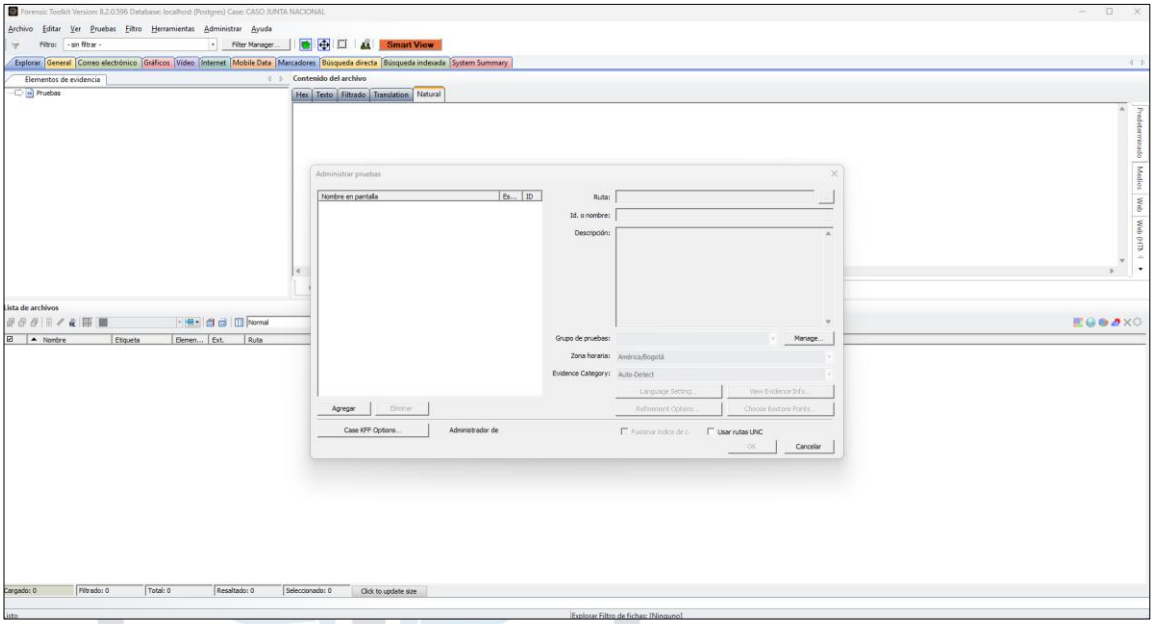


IMAGEN 34. Captura de pantalla, donde se observa la indexación de la imagen forense correspondiente al equipo **DELL W21B**, identificado con el número de activo **EPD00300.**

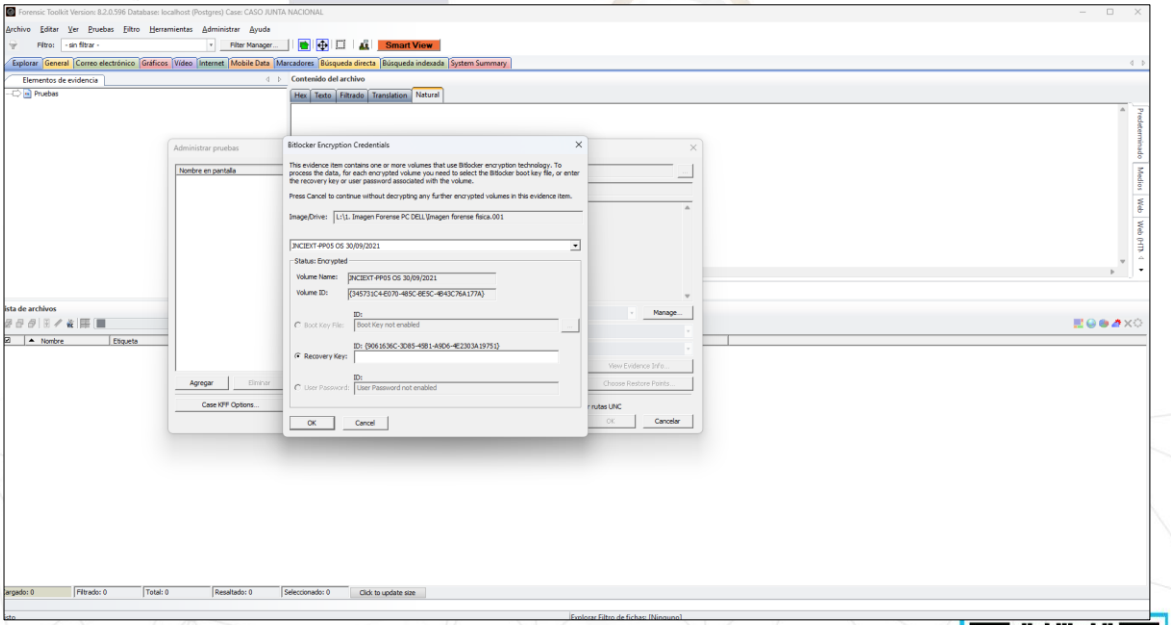


IMAGEN 35. Captura de pantalla, donde se observa la indexación de la imagen forense correspondiente al equipo **DELL W21B**, identificado con el número de activo **EPD00300.**

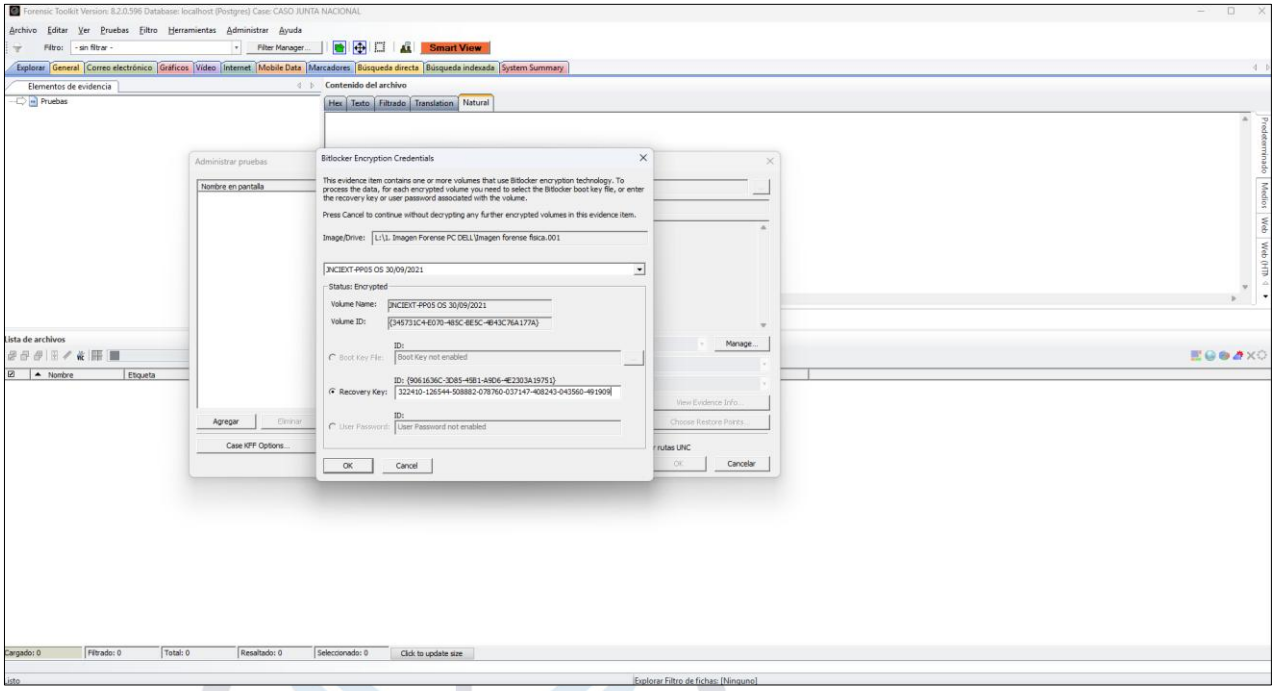


IMAGEN 36. Captura de pantalla, donde se observa la indexación de la imagen forense correspondiente al equipo **DELL W21B**, identificado con el número de activo **EPD00300.**

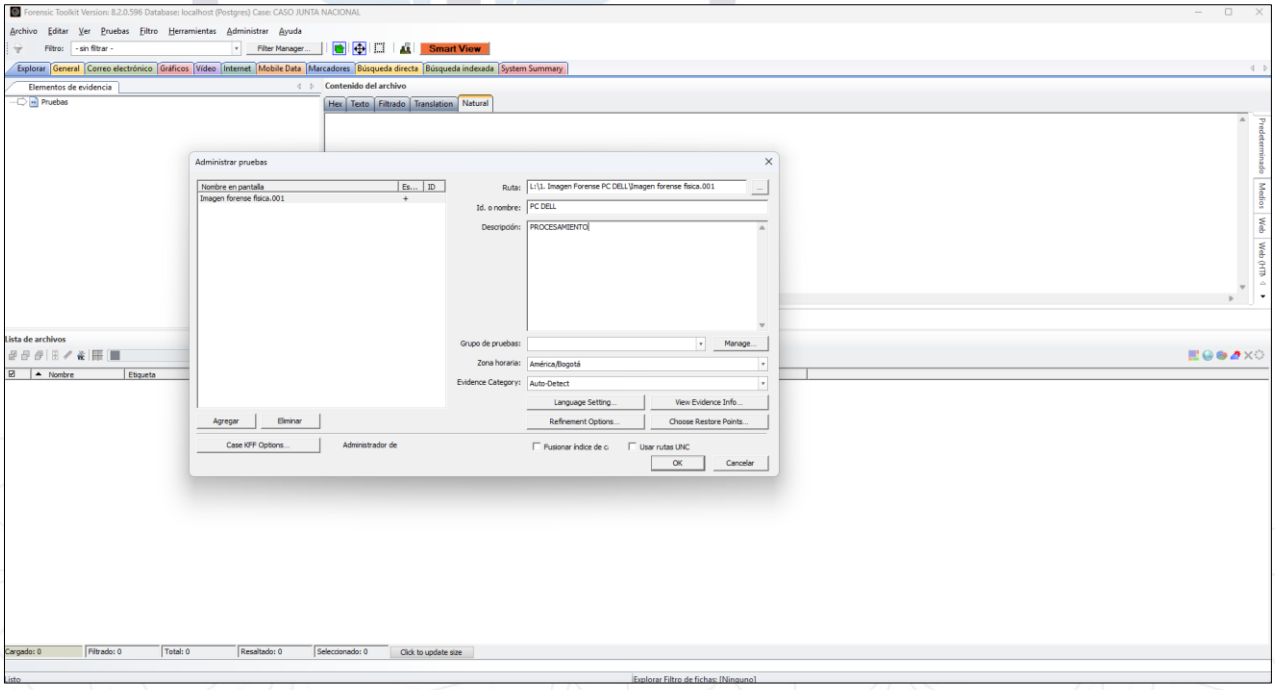


IMAGEN 37. Captura de pantalla, donde se observa la indexación de la imagen forense correspondiente al equipo **DELL W21B**, identificado con el número de activo **EPD00300.**

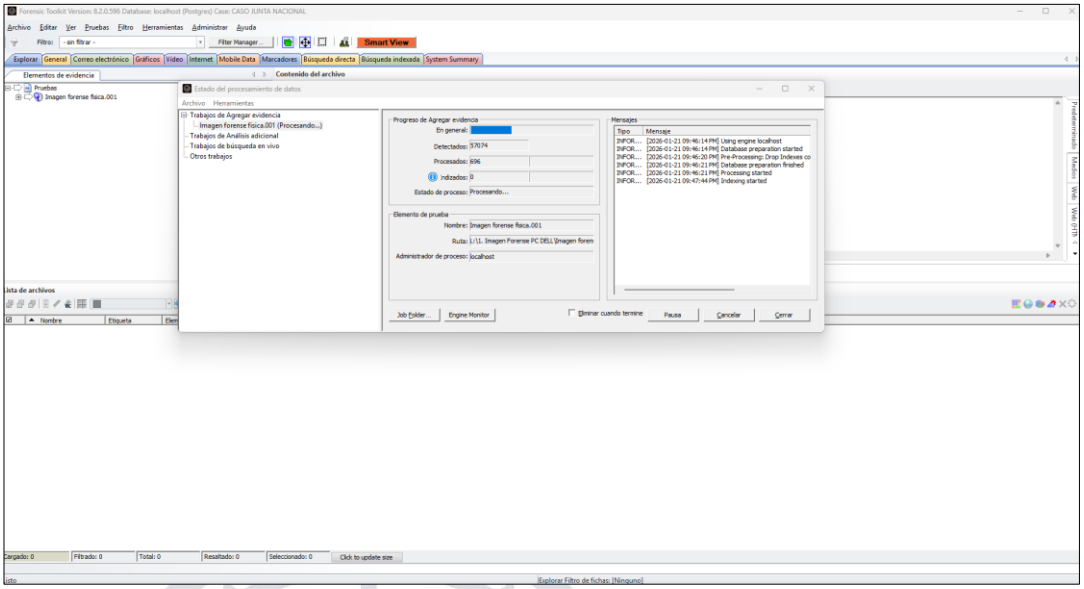


IMAGEN 38. Captura de pantalla, donde se observa la indexación de la imagen forense correspondiente al equipo **DELL W21B**, identificado con el número de activo **EPD00300.**

Al finalizar el proceso de **indexación de la imagen forense**, la herramienta **FTK Toolkit** identificó un total aproximado de **1.247.055 archivos**, los cuales fueron clasificados en diferentes categorías. Dentro de los resultados más relevantes se evidenciaron **362.251 documentos**, **148.027 archivos gráficos**, **100.797 archivos ejecutables**, **203.263 archivos comprimidos**, **726 bases de datos**, **1.235 archivos multimedia**, **187.962 carpetas** y **278.163 elementos correspondientes al sistema operativo o sistema de archivos**.

De igual manera, se identificaron **10.407 archivos de correo electrónico**, **19.770 archivos adjuntos de correo**, y **31.300 elementos relacionados con correos electrónicos**. Adicionalmente, se evidenció un volumen significativo de **513.057 archivos correspondientes a Slack/Free Space**, así como **440.618 archivos eliminados**, **211.946 archivos con extensiones erróneas**, **625.316 archivos clasificados como tipos desconocidos** y **38.934 archivos asociados a otros esquemas de cifrado**.

ESPACIO INTENCIONALMENTE DEJADO EN BLANCO

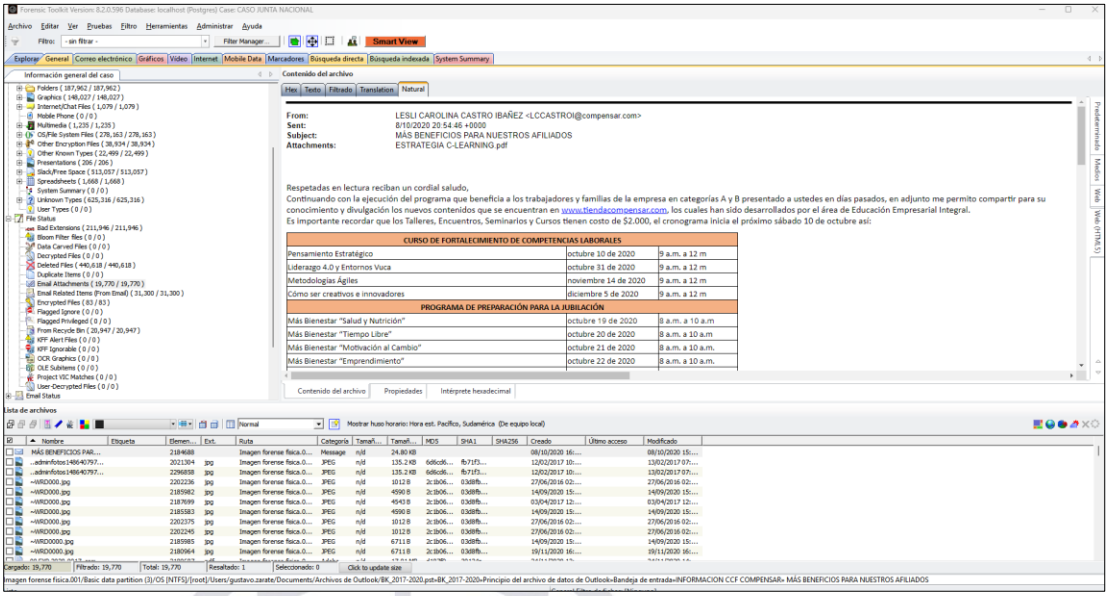


IMAGEN 39. Captura de pantalla, donde se observa los resultados de la indexación de la imagen forense correspondiente al equipo **DELL W21B**, identificado con el número de activo **EPD00300.**

3. Resultados de la búsqueda del archivo **"Alegatos Acción Popular"**

3.1. Computador portátil marca **Lenovo ThinkPad**, identificado con el número de activo **EPD00402**

Se procedió a realizar la búsqueda del archivo objeto de análisis en la pestaña **"Búsqueda indexada"** de la herramienta **FTK Toolkit**, utilizando como vectores de búsqueda las expresiones **"Alegatos Acción Popular"**, **"Alegatos Accion Popular"**, **"ALEGATOS ACCIÓN POPULAR"** y **"ALEGATOS ACCION POPULAR"**. Como resultado de dicho procedimiento, **no se obtuvieron coincidencias** para este equipo de cómputo.

La búsqueda fue ejecutada sobre un universo de **1.119.507 archivos**, previamente indexados y clasificados en diversas categorías, entre las que se destacan **documentos (257.066 archivos)**, **archivos gráficos (397.424)**, **archivos multimedia (1.434)**, **archivos de correo electrónico (151.392)**, **bases de datos (778)**, **archivos ejecutables (111.351)**, **presentaciones (248)** y **hojas de cálculo (19.334)**.

Con base en los procedimientos técnicos realizados, se concluye que **no fue posible localizar el archivo denominado "Alegatos Acción Popular"** dentro de la imagen forense analizada, **ni en el sistema de archivos activo, archivos eliminados, espacio libre, archivos adjuntos de correo electrónico, ni en los distintos artefactos indexados** por la herramienta FTK Toolkit. En consecuencia, desde el punto de vista **técnico-forense**, **no se evidencia que dicho archivo haya sido almacenado de forma local** en el equipo de cómputo objeto de análisis al momento de la adquisición, **o que haya dejado rastros digitales técnicamente recuperables**.

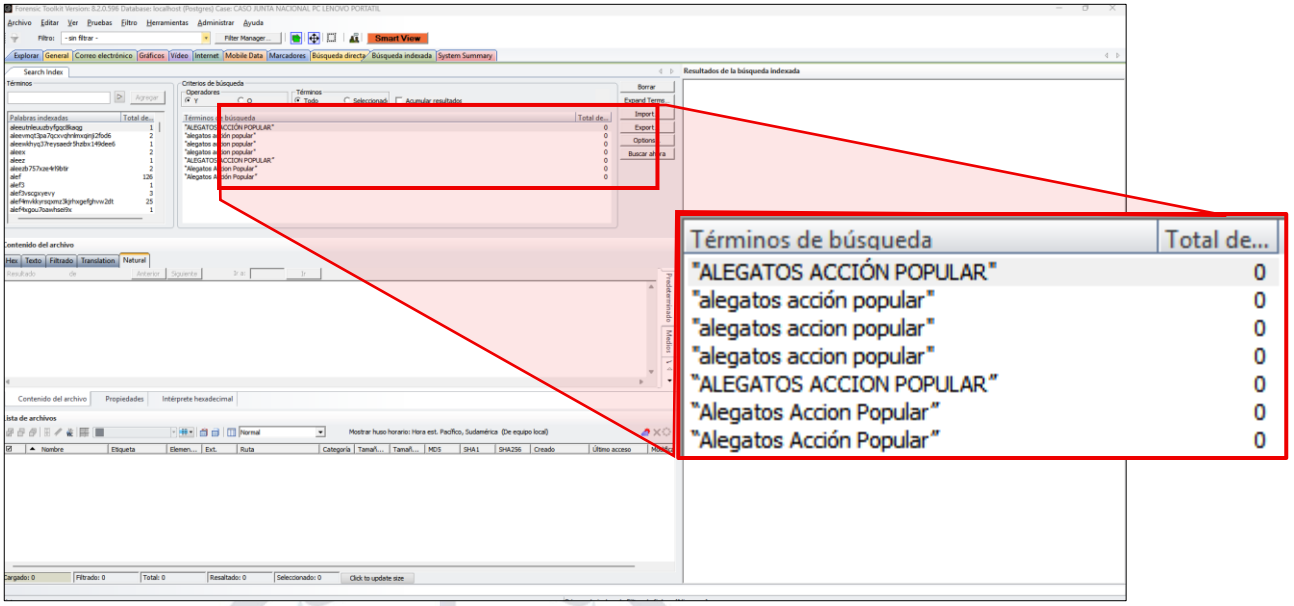


IMAGEN 40. Captura de pantalla, donde se observa la búsqueda indexada de la imagen forense del equipo **Lenovo ThinkPad**, identificado con el número de activo **EPD00402.**

3.2. Computador portátil marca **DELL**, modelo **W21B**, tipo todo en uno, con el número de activo **EPD00300.**

Al realizar la **búsqueda indexada** mediante la herramienta **FTK Toolkit**, utilizando como vector de búsqueda la expresión **"Alegatos Accion Popular"**, se obtuvieron **459 registros como resultados iniciales**. Dichos resultados corresponden a **coincidencias textuales indexadas**, las cuales se les realiza un **análisis individual y detallado**.

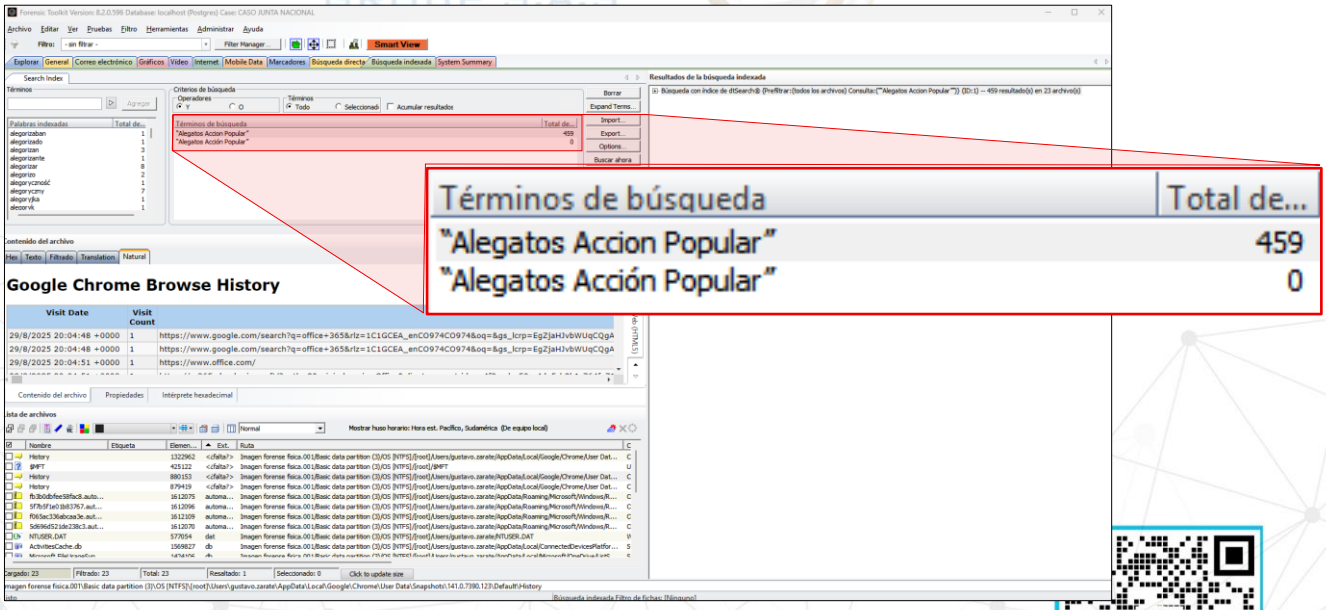
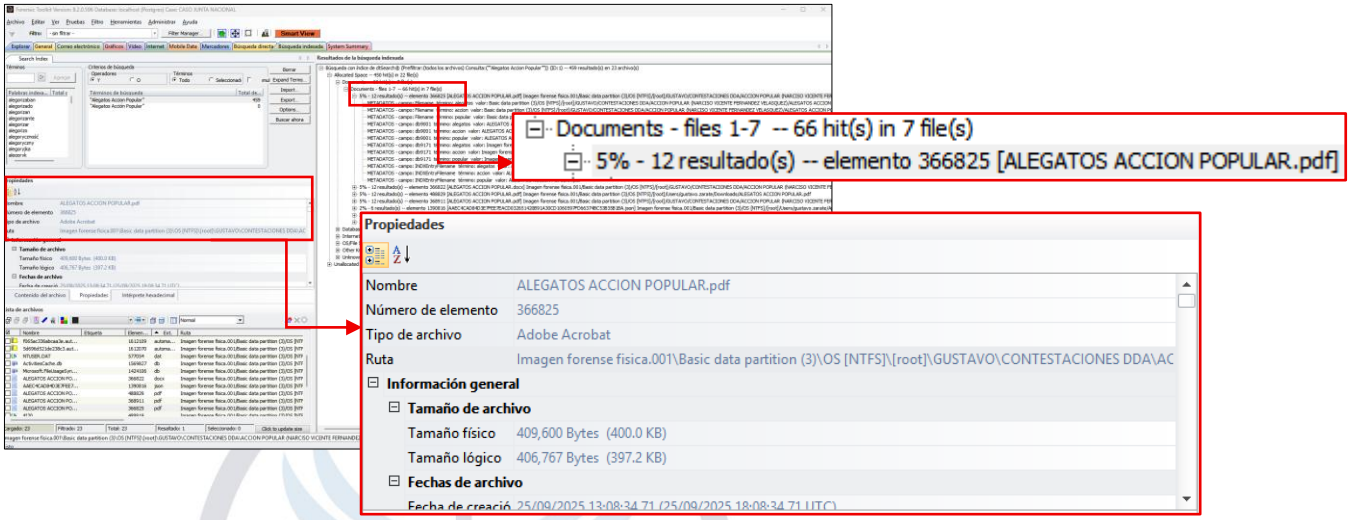


IMAGEN 41. Captura de pantalla, donde se observa la búsqueda indexada de la imagen forense del equipo **DELL**, identificado con el número de activo **W21B.**

Al verificar el espacio asignado encontramos 450 coincidencias dentro de 22 archivos existentes:

3.2.1. Documentos 66 hit(s) in 7 file(s)



Este archivo se almacena en la ruta "***Imagen forense fisica.001\Basic data partition (3)\OS [NTFS]\[root]\GUSTAVO\CONTESTACIONES DDA\ACCION POPULAR (NARCISO VICENTE FERNANDEZ VELASQUEZ)\ALEGATOS ACCION POPULAR.pdf***"

Al analizar los metadatos del archivo, se tuvieron en cuenta aquellos considerados más relevantes, de conformidad con lo solicitado en la orden de trabajo.

Nombre	ALEGATOS ACCION POPULAR.pdf
Número de elemento	366825
Tipo de archivo	Adobe Acrobat
Ruta	Imagen forense fisica.001\Basic data partition (3)\OS [NTFS]\[root]\GUSTAVO\CONTESTACIONES DDA\ACCION POPULAR (NARCISO VICENTE FERNANDEZ VELASQUEZ)\ALEGATOS ACCION POPULAR.pdf
Fecha de creación	25/09/2025 13:08:34.71 (25/09/2025 18:08:34.71 UTC)
Fecha de acceso	21/10/2025 11:32:40.36 (21/10/2025 16:32:40.36 UTC)
Fecha de modificación	25/09/2025 13:08:36.71 (25/09/2025 18:08:36.71 UTC)
Metadata Author	Kevin James Vargas Mendoza

Este archivo se almacena en la ruta "***Imagen forense fisica.001/Basic data partition (3)/OS [NTFS]/[root]/GUSTAVO/CONTESTACIONES DDA/ACCION POPULAR (NARCISO VICENTE FERNANDEZ VELASQUEZ)/ALEGATOS ACCION POPULAR.docx***"

Nombre	ALEGATOS ACCION POPULAR.docx
Número de elemento	366822

Tipo de archivo	Microsoft Word 2016
Ruta	Imagen forense fisica.001/Basic data partition (3)/OS [NTFS]/[root]/GUSTAVO/CONTESTACIONES DDA/ACCION POPULAR (NARCISO VICENTE FERNANDEZ VELASQUEZ)/ALEGATOS ACCION POPULAR.docx
Fecha de creación	23/9/2025 19:27:12
Fecha de acceso	24/10/2025 13:22:53
Fecha de modificación	25/9/2025 18:08:27
Metadata Author	Kevin James Vargas Mendoza
Último guardado por	Gustavo Eliecer Zarate Arias

Este archivo se almacena en la ruta "***Imagen forense fisica.001/Basic data partition (3)/OS [NTFS]/[root]/Users/gustavo.zarate/Downloads/ALEGATOS ACCION POPULAR.pdf***"

Nombre	ALEGATOS ACCIÓN POPULAR.pdf
Número de elemento	488829
Tipo de archivo	Adobe Acrobat
Ruta	Imagen forense fisica.001/Basic data partition (3)/OS [NTFS]/[root]/Users/gustavo.zarate/Downloads/ALEGATOS ACCION POPULAR.pdf
Fecha de creación	10/11/2025 14:42:44
Fecha de acceso	10/11/2025 19:09:15
Fecha de modificación	10/11/2025 14:42:45
Metadata Author	Kevin James Vargas Mendoza
Último guardado por	Gustavo Eliecer Zarate Arias

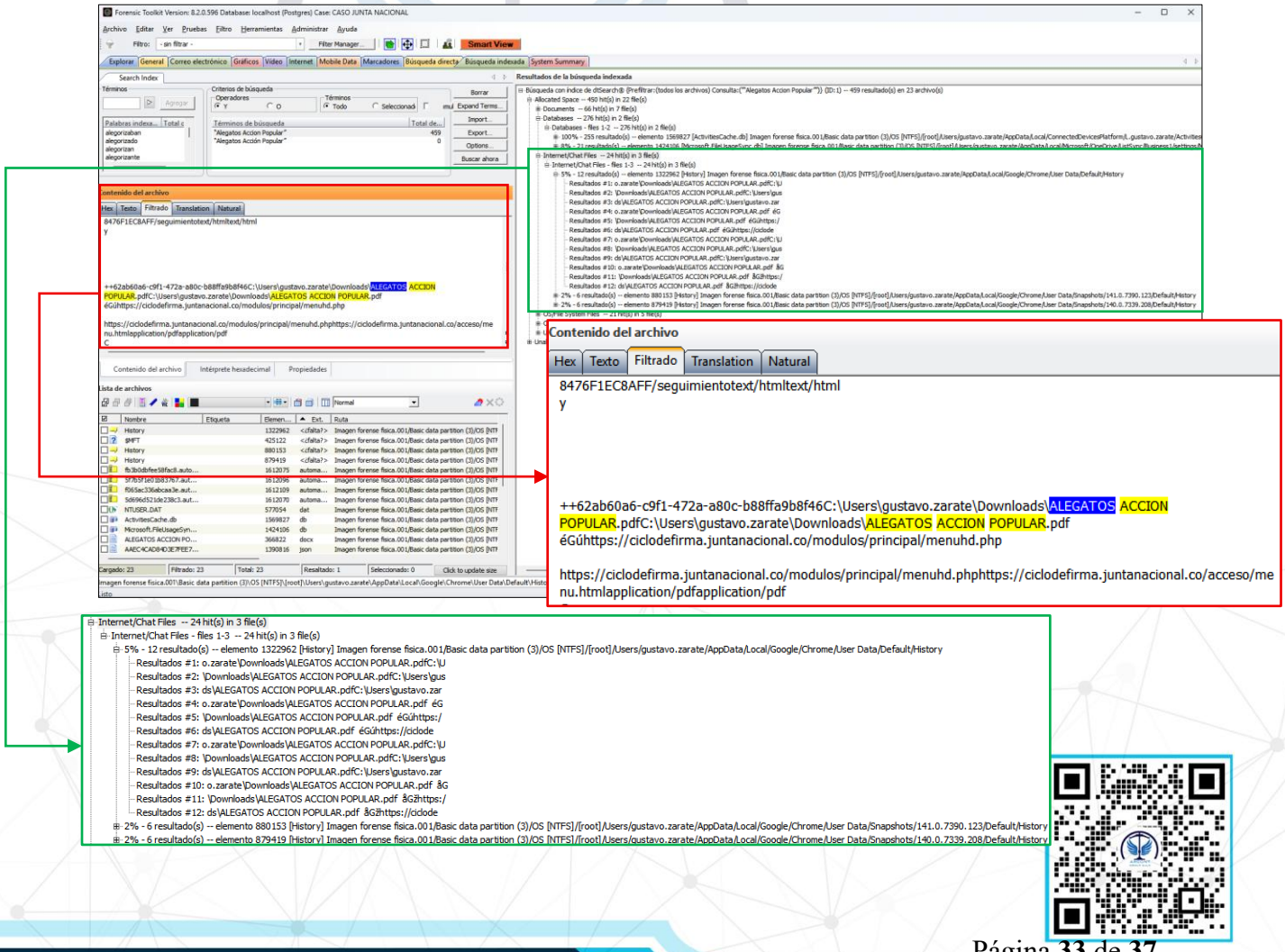
Este archivo se almacena en la ruta " ***Imagen forense fisica.001/Basic data partition (3)/OS [NTFS]/[root]/GUSTAVO/CONTESTACIONES DDA/ACCION POPULAR (NARCISO VICENTE FERNANDEZ VELASQUEZ)/ALEGATOS/ALEGATOS ACCION POPULAR.pdf***"

Nombre	ALEGATOS ACCIÓN POPULAR.pdf
Número de elemento	368911
Tipo de archivo	Adobe Acrobat
Ruta	Imagen forense fisica.001/Basic data partition (3)/OS [NTFS]/[root]/GUSTAVO/CONTESTACIONES DDA/ACCION POPULAR (NARCISO VICENTE FERNANDEZ VELASQUEZ)/ALEGATOS/ALEGATOS ACCION POPULAR.pdf
Fecha de creación	25/9/2025 19:37:38
Fecha de acceso	10/11/2025 14:41:04
Fecha de modificación	25/9/2025 19:37:40
Metadata Author	Kevin James Vargas Mendoza

Este archivo se almacena en la ruta "**Imagen forense fisica.001/Basic data partition (3)/OS [NTFS]/[root]/GUSTAVO/CONTESTACIONES DDA/ACCION POPULAR (NARCISO VICENTE FERNANDEZ VELASQUEZ)/ALEGATOS ACCION POPULAR.pdf**"

Nombre	ALEGATOS ACCIÓN POPULAR.pdf
Número de elemento	366825
Tipo de archivo	Adobe Acrobat
Ruta	Imagen forense fisica.001/Basic data partition (3)/OS [NTFS]/[root]/GUSTAVO/CONTESTACIONES DDA/ACCION POPULAR (NARCISO VICENTE FERNANDEZ VELASQUEZ)/ALEGATOS ACCION POPULAR.pdf
Fecha de creación	25/9/2025 18:08:34
Fecha de acceso	21/10/2025 16:32:40
Fecha de modificación	25/9/2025 18:08:36
Metadata Author	Kevin James Vargas Mendoza

3.2.2. Internet/Chat Files 24 hit(s) in 3 file(s)



La categoría **Internet/Cache Files** contiene artefactos generados por la navegación web y el acceso a plataformas en línea, tales como páginas web, archivos temporales, copias parciales de documentos, contenido de correos electrónicos web y metadatos asociados a accesos realizados desde el navegador. La presencia de coincidencias en esta categoría sugiere que el contenido objeto de análisis pudo haber sido consultado o visualizado mediante servicios web.

En el análisis de artefactos de navegación y archivos temporales, se identificó un registro que contiene un **identificador único (UUID)**, una **ruta local de descarga** correspondiente a ***C:\Users\gustavo.zarate\Downloads\ALEGATOS ACCION POPULAR.pdf***, así como una **URL asociada al *aplicativo Ciclo de Firma (https://ciclodefirma.juntanacional.co)***. Este hallazgo indica que el archivo denominado **"*ALEGATOS ACCION POPULAR.pdf*"** fue gestionado mediante el navegador web, asociado a una sesión del aplicativo referido y vinculado al perfil de usuario ***gustavo.zarate***, quedando evidencia de su descarga o intento de descarga registrada en artefactos de cache o bases de datos del sistema, sin que ello implique necesariamente la persistencia actual del archivo en el sistema de archivos.

Nombre	History
Tipo de archivo	Chrome History File
Ruta	Imagen forense fisica.001\Basic data partition (3)\OS [NTFS]\[root]\Users**gustavo.zarate**\AppData\Local\Google\Chrome\User Data\Default\History
Fecha de creación	4/10/2021 17:52:31
Fecha de acceso	10/11/2025 19:22:37
Fecha de modificación	10/11/2025 19:22:37

INTERPRETACIÓN DE RESULTADOS / CONCLUSIONES

Mediante el uso de herramientas forenses especializadas es posible identificar, recolectar, preservar y asegurar evidencia digital almacenada en equipos de cómputo. En el presente caso, se logró la preservación de **dos imágenes forenses**, correspondientes a: computador de escritorio marca **DELL**, modelo **W21B**, tipo "todo en uno", identificado con el número de activo **EPD00300**; y equipo portátil marca **Lenovo ThinkPad**, identificado con el número de activo **EPD00402**. Sobre dichas imágenes se realizó el respectivo proceso de análisis forense, el cual constituye el objeto del presente estudio.

1. Se ejecutaron procedimientos de adquisición forense conforme a prácticas de preservación e integridad (uso de herramientas forenses y verificación mediante valores hash), con el fin de garantizar la **integridad** y **autenticidad** de la evidencia digital obtenida.

2. En el equipo **Lenovo ThinkPad (EPD00402)**, tras ejecutar búsquedas indexadas con múltiples criterios (incluyendo "Alegatos Acción Popular" y variantes) sobre el universo de archivos indexados, **no se obtuvieron coincidencias** asociadas al archivo objeto de análisis en dicha imagen forense. En consecuencia, no fue posible localizar el archivo "Alegatos Acción Popular" ni evidenciar rastros técnicamente recuperables en el sistema de archivos activo, elementos eliminados, espacio libre, adjuntos u otros artefactos indexados para ese equipo.

3. Para el equipo **DELL W21B (EPD00300)**, la búsqueda indexada **sí arrojó resultados**, identificando el archivo **"ALEGATOS ACCION POPULAR.pdf"** almacenado en rutas bajo la estructura **GUSTAVO\CONTESTACIONES DDA\ACCION POPULAR**, lo cual evidencia la presencia del documento en el sistema analizado. Adicionalmente, se documentó la existencia de una versión en formato **.docx** (**"ALEGATOS ACCION POPULAR.docx"**) dentro de la misma estructura de carpetas, con metadatos asociados y registro de **"Último guardado por Gustavo Eliecer Zarate Arias"**. Respecto de los archivos identificados en este equipo (DELL), se registraron **metadatos relevantes**, incluyendo fechas de creación, acceso y modificación, así como metadatos de autoría y último guardado, los cuales constituyen indicadores técnicos de manejo y gestión del documento dentro del entorno analizado. Asimismo, se identificaron **rastros de descarga y/o gestión vía navegador** asociados a un perfil de usuario. En particular, se halló un artefacto de navegación con la ruta local **C:\Users\gustavo.zarate\Downloads\ALEGATOS ACCION POPULAR.pdf** y una URL vinculada al aplicativo **Ciclo de Firma**, lo que indica que el archivo fue gestionado mediante navegador y asociado al perfil **gustavo.zarate**.

4. En relación con el **equipo MacBook (EPD00354)**, no fue posible adquirir la imagen forense debido a las restricciones de cifrado del equipo y a que la clave suministrada no permitió el acceso. Se documentó la presencia de limitaciones técnicas (SSD soldada y chip de seguridad Apple T2), así como la necesidad de contar con la clave **FileVault** para proceder; pese a suministrarse una clave, esta no fue funcional, por lo cual no se logró ejecutar el procedimiento de copia y análisis.

5. Finalmente, en cuanto al **alcance frente a un posible acceso por terceras personas**, con lo reportado se acredita evidencia de gestión/descarga asociada al perfil **gustavo.zarate** (mediante artefactos del navegador) y la presencia de los archivos en rutas vinculadas a la carpeta "GUSTAVO". No obstante, con la información consignada en el informe, **no es posible establecer de manera concluyente** el acceso por otras personas distintas a los usuarios principales.

Se obtuvo firma hash por medio de la herramienta *HashCal* [1] del siguiente informe:

Herramienta forense	FTK Toolkit 8.2
Nombre del informe	Index.html
MD5 checksum	5b9ae66d1fb370eca638f74baff31fc5
SHA1 checksum	fa4ea16e3fcb36d6af30e6de67c314f0ff29222f
SHA256 checksum	90cc81d72fe8262eceddd5bee9114cbc4b56943e25d207a7b96c854f6ba4f108

Herramienta forense	FTK Toolkit 8.2
Nombre del informe	1.xhtml
MD5 checksum	ffc05b165c0164efa9467e5da7ab7882
SHA1 checksum	4c3735554a29c019ae4ddb10d781ad2f300dcfd3
SHA256 checksum	dec6e03237f384535bb07ee325300d0bc6fa393d4558a3423e2583b[illegible]3124

[1] ***HashCal*** Realiza cálculos de los códigos hash, sumas de comprobación y HMAC de sus archivos. Utiliza algoritmos como MD5, MD2, SHA-1, SHA-256, CRC32, ed2k Hash y otros para calcular el código hash de uno o varios archivos a la vez. Analiza parámetros como la ruta completa, el nombre y el formato.

Herramienta forense	FTK Toolkit 8.2
Nombre del informe	2.xhtml
MD5 checksum	a643e3936b182e28d94c12190f51c275
SHA1 checksum	f28f7898d86b28aa973a01c9c226d70909e669ee
SHA256 checksum	ade3f8e270aaaaec4bc89751c9d047398bc88b17fb7d4ce67774cd8b9eb01a4a

Herramienta forense	FTK Toolkit 8.2
Nombre del informe	3.xhtml
MD5 checksum	f304ba3cee2bf2b58d8f2c0e316f9e59
SHA1 checksum	1def92378844e58834bbb1a1a949a02d3e2ffda5
SHA256 checksum	c81faa2fc57be301e2c315ac206c5dd391ea0ac167003a6bb2eb33a47d36beed

Herramienta forense	FTK Toolkit 8.2
Nombre del informe	4.xhtml
MD5 checksum	1e763f456ccf2cc64e43f0796999bd82
SHA1 checksum	614a83da706aa37b84db4987642416bc767fe992
SHA256 checksum	be53fbc6b000396fb8005c6ed7ab484a5a784bbbe043834914ba67c74cf9f97d

Herramienta forense	FTK Toolkit 8.2
Nombre del informe	5.xhtml
MD5 checksum	9c02754b03de4de42e11fcd3288bc177
SHA1 checksum	459f5b458917166934c0921aece740736cb74ad7
SHA256 checksum	dd2028186278eafbe64d92a743f792659ccec6902ae40f9845319bc5580e75af

Herramienta forense	FTK Toolkit 8.2
Nombre del informe	6.xhtml
MD5 checksum	66dba151b245def07885d6e618982843
SHA1 checksum	0d126ec09bec485015a373b642c454b5b062653b
SHA256 checksum	c52e9499ebf4ec608fac010bebebcd72369c1e3729373b742f1fa5a647db8c9e

Para finalizar se procede a almacenar la totalidad de la información hallada en un medio de almacenamiento de información digital tipo óptico cumpliendo con todos los principios del protocolo de cadena de custodia, salvaguardando la AUTENTICIDAD, INTEGRIDAD y DISPONIBILIDAD de la información, conforme a los preceptos de la Ley 527 de 1999, norma que da valor probatorio al mensaje de datos (evidencia digital).

OBSERVACIONES

- La evidencia que se almacena en este DVD se guarda en el almacén de evidencias de la Unidad de Investigación Criminal de la Defensa, si las partes solicitan copia de esta evidencia se entregará en cualquier dispositivo de almacenamiento que se solicite.

ANEXOS

Un DVD de 4.7 GB identificado como "ANEXO DIGITAL 1 INFORME 20250112198 FL1 LABORATORIO DE INFORMÁTICA FORENSE", el cual contiene:

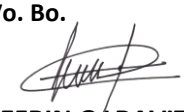
- Una carpeta identificada con el nombre de “Informe Forense” la cual corresponde a los resultados de la preservación de los correos electrónicos, este informe es generado por la herramienta FTK Toolkit 8.2 y se identifica como index.html.
- Una carpeta identificada como “Metadatos de los archivos” la cual contiene 6 archivos en formato .xhtml correspondiente a los metadatos analizados.

Cordialmente.



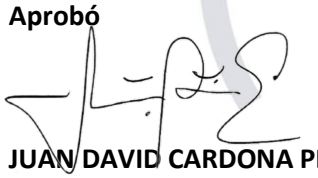
ANDRÉS DÍAZ SALAS[2].
PERITO EN INFORMÁTICA FORENSE
UNIDAD DE INVESTIGACIÓN CRIMINAL DE LA DEFENSA

Vo. Bo.



YEFRIN GARAVITO NAVARRO[3].
DIRECTOR DE LA UNIDAD DE INVESTIGACIÓN CRIMINAL DE LA DEFENSA
LABORATORIO DE INFORMÁTICA FORENSE

Aprobó



JUAN DAVID CARDONA PÉREZ[4]
CEO ARCONT GROUP SAS CIBERABOGADOS

---

2 **ANDRÉS DÍAZ SALAS:** Ingeniero de Sistemas, Perito en Informática Forense de la Unidad de Investigación Criminal de la Defensa, es Perito CiberJudicial por el Center for CIC de Boston University y AccessData Certified Examiner (ACE). Además, cuenta con certificaciones en Entrenamiento de Técnicas de Análisis Forense de Programas Maliciosos en Computadores, otorgada por la Escuela de Investigación Criminal, y en el uso de la herramienta MOBILedit Forensic de Compelson. Es profesor en la Universidad Sergio Arboleda, donde dicta las cátedras de Informática Forense y Ciberseguridad. Anteriormente, se desempeñó como instructor en Crímenes Contra el Sistema Bancario en la Procuraduría General de la Nación y en la Escuela del Ministerio Público Dra. Clara González de Behringer en Ciudad de Panamá. Cuenta con 12 años de experiencia como Investigador Criminal del Centro de Capacidades para la Ciberseguridad de Colombia (C4) de la Policía Nacional. Ha participado en diferentes intervenciones del Congreso Internacional de Derecho Penal y Cibercriminalidad, así como en el evento de Prevención del Fraude y Seguridad. También ha realizado el curso de formación de auditores internos en ISO 31000:2009 y ha recibido entrenamiento internacional en el uso básico de la herramienta Sentinel Visualizer.

3 **YEFRIN GARAVITO NAVARRO:** Ingeniero de Sistemas, Magister en Investigación Criminal de la Escuela de Investigación Criminal de la Policía Nacional, Magister en Criminología y Victimología de la Escuela de Postgrados de la Policía Nacional De Colombia, Especialista en informática forense de la Escuela de tecnología de la información y las comunicaciones de la Policía Nacional, Especialista en seguridad informática de la Universidad piloto de Colombia. Perfilador Criminal certificado por la (ABP – DIJIN), Entrenado en investigación cibernética por la KPNA (Korean National Pólice Agency), Miembro de la IACA (International Association of Crime Analysts), miembro de la plataforma de expertos EPE del EC3 de EUROPOL, director del grupo de investigaciones especiales y laboratorio de informática forense de la Unidad de Investigación Criminal de la Defensa (UID), 18 años de experiencia en el área de investigación judicial, Criminalística y ciencias forenses. Ha sido Investigador y perito testigo en diferentes Juzgados, Tribunales y ante la Corte Suprema de Justicia en diversos casos, cuenta con formación y actualización académica con Crandfield University, NIJ US Departament of Justice, Miami Dade Police, Dirección de Investigación Criminal e Interpol, KPNA entre otras entidades. Ponente Internacional en Perú, Argentina, México y otros países, docente de pregrado y postgrado de las universidades Rosario, Sergio Arboleda, Gran Colombia, Escuela de Tecnologías de la información y las comunicaciones de la Policía Nacional, Escuela de Posgrados de Policía, Escuela de Investigación Criminal Policía Nacional y de la Escuela de Guerra del ejército nacional, ha sido asesor y consultor internacional de la dirección de telemática de la Policía Nacional del Perú (PNP), de la Pan American Development Foundation, la Agencia Antinarcóticos y de Aplicación de Ley de Estados Unidos (INL) y la comisión de Acusación del Congreso de la República, participó como miembro de la delegación oficial de Colombia en cibercrimen ante las autoridades Europeas. Es autor de la Guía técnica sobre análisis forense y evidencia digital y Guía de Buenas Prácticas en Investigación Forense en Casos de Crimen Organizado de INL.

4 CIBER ABOGADO, Magister en Derecho de la Ciberseguridad y entorno digital, (Becario de la fundación Carolina en la Universidad de León / España). Magister en Derechos Humanos DDHH y Derecho Internacional De Los Conflictos Armados DICA. Conciliador en derecho. Ex funcionario de la fiscalía general de la Nación, Especialista en derecho penal y procesal penal, específicamente en el campo de los delitos informáticos, la cibercriminalidad. INGENIERO DE SISTEMAS. Especialista en seguridad informática, Especialista en Informática Forense. Consultor en SGSI-ISO 27001 y 27032, auditoría forense y métodos antifraude. Presidente del Instituto Iberoamericano de Derecho Digital y de la Ciberseguridad y presidente de la IAI División Colombia en el Subcomité de Informática Forense.

JUNTA NACIONAL DE CALIFICACIÓN DE INVALIDEZ	**ACTA DE ENTREGA SUPERVISION ORDEN DE COMPRA Y/O SERVICIO**	

*LA IMPRESIÓN DE ESTE DOCUMENTO CONSTITUYE UNA COPIA NO CONTROLADA

I. DATOS GENERALES

No. orden de compra y/o servicios:	OSG-0035-JNCI-2025
Valor de la orden:	14.235.000,00
Fecha de expedición de la orden:	11/11/2025
Fecha de vencimiento:	11/12/2025
Objeto de la orden:	Contratar los servicios de auditoría en informática forense y representación legal en derecho digital para la identificación, recolección, aseguramiento y análisis de evidencia digital en tres (3) equipos de cómputo de la Junta Nacional de Calificación de Invalidez
Fecha de prestación del servicio o entrega del bien:	-
Supervisor de la orden:	Estephany Cruz Suárez
Cargo:	Gestor Contractual
Dependencia:	Unidad de Gestión Contractual
Proveedor o prestador de servicio:	ARCONT GROUP SAS
Nit o cédula de ciudadanía:	901.138.375-9

II. BALANCE FINANCIERO DE LA ORDEN N° OSG-0035-JNCI-2025

Valor de la orden:	14.235.000,00
Valor pagado	7.117.500,00
Valor pendiente pago	7.117.500,00

III. INFORME DE LA PRESTACIÓN DE SERVICIOS O ENTREGA DE BIENES:

ITEM	SI	NO	JUSTIFIQUE	N/A
¿El bien o servicio cumplió con las especificaciones técnicas mínimas solicitadas?		x	Se recibió informe de laboratorio Misión de trabajo N°20250101011 de fecha 10 de febrero de 2026, por parte de Arcont Group SAS. No obstante, se recibe correo por parte de la	

			contadora Ana Paola Montaño, informando que el computador LENOVO fue recibido sin el cargador del equipo. De igual manera, el Doctor Cristian Collazos solicita se le requiera al contratista revisa el valor de la factura; toda vez que según el informe el computador MacBook modelo A2238, no pudo ser descifrado.	
¿El contratista cumplió con los tiempos pactados para la entrega del bien o la prestación del servicio?		x	El contratista entregó el informe final el día 10 de febrero de 2026	
¿Se llevó a cabo la instalación o puesta en funcionamiento de los bienes a entera satisfacción?				X
¿Se llevaron a cabo los mantenimientos preventivos o correctivos solicitados a entera satisfacción?				X
¿Se recibió el bien o la prestación del servicio a entera satisfacción?	X		Se recibió el informe de auditoría requerido por la Entidad.	

Como supervisor designado de la Orden de Prestación de servicios, certifico que cumplí con las funciones de verificación, vigilancia y control frente al cumplimiento del desarrollo de la orden No. OSG-0035-JNCI-2025.

Así mismo, se suscribe la presente Acta de Entrega de Supervisión, dejando constancia de que, a la fecha, se encuentran pendientes las siguientes gestiones:

1. Requerir formalmente al contratista para que emita pronunciamiento respecto del cargador correspondiente al equipo marca Lenovo, identificado con el número de activo EPD00300.
2. Solicitar al contratista la verificación de la factura que se encuentra pendiente, en atención a que no fue posible realizar el descifrado del computador MacBook, modelo A2238, circunstancia que impidió culminar la validación técnica requerida.

En consecuencia, una vez efectuadas y verificadas las gestiones anteriormente señaladas, la Entidad podrá proceder con el trámite de pago hasta por la suma de siete millones ciento diecisiete mil quinientos pesos ($7.117.500,00).

Por lo anterior, se firma en Bogotá DC, a los 27 días del mes de febrero de 2026.



Estephany Cruz Suárez
Gestor Contractual
Supervisor de la Orden

Anexo:

Informe final ARCONT GROUP SAS.

Bogotá D.C., 09 de marzo de 2026

Señores
ARCONT GROUP S.A.S.
Representante Legal: Juan David Cardona Pérez
Bogotá D.C.

Asunto: Respuesta a solicitud de pago del 50% final y solicitud de entrega completa de equipos.

Cordial saludo,

En atención a la solicitud presentada por ARCONT GROUP S.A.S. relacionada con el pago del cincuenta por ciento (50%) final, la Junta Nacional de Calificación de Invalidez se permite informar lo siguiente:

1. El día diecinueve (19) de noviembre de 2025 se suscribió el acta de salida de activos de las instalaciones de la Junta Nacional de Calificación de Invalidez, dentro de la cual se relacionaron los equipos retirados, conforme se evidencia a continuación:

JUNTA NACIONAL DE CALIFICACIÓN DE INVALIDEZ	FORMATO DE MOVIMIENTO, INGRESO Y/O SALIDA DE ACTIVOS FIJOS, BIENES Y O ELEMENTOS (TECNOLOGICOS)	FORMATO FO-UTC-12 28/05/2025 V.R: 1.1

INGRESO		SALIDA	X	MOVIMIENTO	FECHA: 19/11/2025

RELACIÓN DE BIENES

CANTIDAD	DESCRIPCIÓN
1	Portátil Lenovo Thinkpad E14, Serial: PF4W7BN2, Procesador: Core i5 1335U, Placa: EPD00402, SO Win11 pro, RAM 16GB, SSD NVMe 500GB.
1	portátil MacBook Pro-13 inch modelo: A2338 SN: NPKXD6TC6X PLACA: EPD00354 RAM: 8GB SSD: 256GB
1	EQUIPO DE COMPUTO PLACA: EPD00300 SN: GS642G3 Optiplex 3280 Core i5 10500T

OBSERVACIONES:
EQUIPOS PARA AUDITORIA

FIRMAS

RECIBE / ENTREGA TECNOLOGIA	REVISADO CONTABILIDAD	RECIBE/ENTREGA TRABAJADOR
Nombre:Cesar Andres Pachon Cargo: Profesional Mesa de Ayuda	Nombre: Diego Armando Rincón Cendales Cargo: Analista Contable Y Proveedores	Nombre: Andres Diaz Cargo: Perito / Auditor

2. En relación con el equipo de cómputo identificado con placa EDP00300, se deja constancia de que este fue entregado con su cable de corriente, tal como se evidencia en las fotografías contenidas en el informe de auditoría presentado por ARCONT.

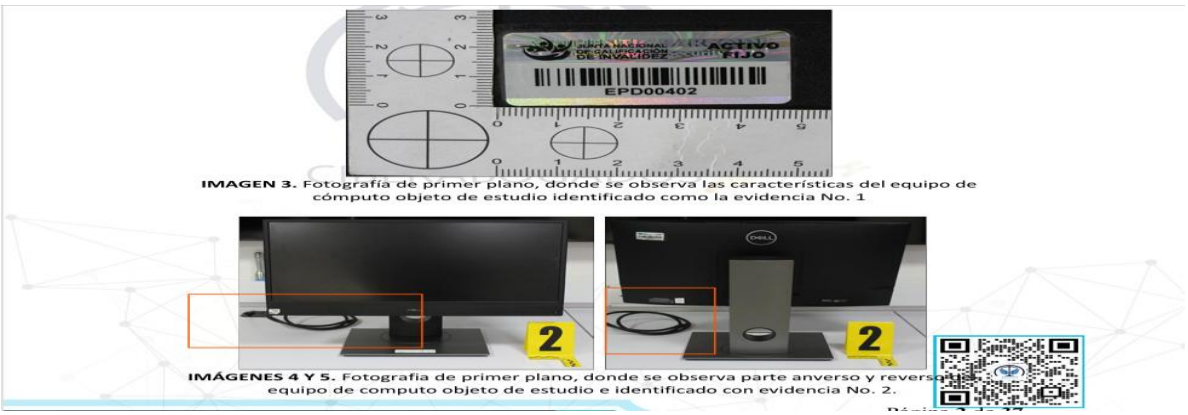


IMAGEN 3. Fotografía de primer plano, donde se observa las características del equipo de cómputo objeto de estudio identificado como la evidencia No. 1

IMÁGENES 4 Y 5. Fotografía de primer plano, donde se observa parte anverso y reverso del equipo de computo objeto de estudio e identificado con evidencia No. 2.

3. Posteriormente, el día veintiuno (21) de enero de 2026, los equipos ingresaron nuevamente a las instalaciones de la Junta Nacional de Calificación de Invalidez. No obstante, al momento de su recepción se dejó constancia de que el equipo de cómputo con

placa EDP00300 fue entregado por ARCONT sin el cable de corriente, tal como se registra en la anotación realizada por la persona encargada de recibir los equipos, como se muestra a continuación:

JUNTA NACIONAL DE CALIFICACIÓN DE INVALIDEZ	FORMATO DE MOVIMIENTO, INGRESO Y/O SALIDA DE ACTIVOS FIJOS, BIENES Y O ELEMENTOS (TECNOLOGICOS)	FORMATO FO-UTC-12	
		28/05/2025	V.R: 1.1

INGRESO	X	SALIDA		MOVIMIENTO	FECHA: 21/01/2026

RELACIÓN DE BIENES	
CANTIDAD	DESCRIPCIÓN
1	Portátil Lenovo Thinkpad E14, Serial: PF4W7BN2, Procesador: Core i5 1335U, Placa: EPD00402, SO Win11 pro, RAM 16GB, SSD NVMe 500GB
1	portátil MacBook Pro-13 inch modelo: A2338 SN: NPKXD6TC6X PLACA: EPD00354 RAM: 8GB SSD: 256GB
1	EQUIPO DE COMPUTO PLACA: EPD00300 SN: GS642G3 Optiplex 3280 Core i5 10500T

OBSERVACIONES:
equipos que ingresan como resultado del proceso de auditoría. El equipo con placa EPD00354 continúa asignado al Dr. Cristian Collazos; los demás equipos quedan disponibles para el área de TI. El equipo EDP00300 ingresa sin cable corriente.

FIRMAS

Firmado digitalmente por Luis Angel Contreras Caldas		
RECIBE / ENTREGA TECNOLOGIA	REVISADO CONTABILIDAD	RECIBE/ENTREGA TRABAJADOR
Nombre:Luis Angel Contreras Caldas	Nombre: Diego Armando Rincón Cendales	Nombre:Cesar Andres Pachon
Cargo: Tecnologo de soporte	Cargo: Analista Contable Y Proveedores	Cargo: Profesional Mesa de Ayuda

4. En virtud de lo anterior, la Junta Nacional de Calificación de Invalidez solicita de manera formal a ARCONT GROUP S.A.S. realizar la entrega del cable de corriente correspondiente al equipo de cómputo con placa EDP00300, con el fin de verificar la devolución completa de los equipos que fueron retirados previamente de las instalaciones de la entidad.

5. De igual manera, se solicita remitir el certificado de pago de aportes al Sistema de Seguridad Social Integral, suscrito por el representante legal de la persona jurídica y con fecha actual, requisito necesario para continuar con el trámite correspondiente.

Agradecemos realizar el envío de la información y realizar la entrega del elemento solicitado a la mayor brevedad posible, con el fin de continuar con las gestiones administrativas correspondientes.

Cordialmente,

Ana Meneses.

Ana Belly Meneses Rosales
Profesional Contractual
Junta Nacional de Calificación de Invalidez

ACTA DE ENTREGA DE ELEMENTOS

En Bogotá a los 18 días del mes de marzo de 2026, se deja constancia por medio de la presente acta que se realiza la entrega de un (01) cargador nuevo y original, correspondiente a un (01) computador marca DELL, modelo W21B, tipo todo en uno, con el número de activo EPD00300.

Lo anterior se deja expresamente consignado en atención a que, conforme a la verificación realizada, el cargador original del equipo nunca fue recibido ni llegó junto con el mismo. En consecuencia, y con el fin de garantizar la funcionalidad, uso y correcta operación del equipo, se procedió a realizar la compra de un cargador completamente nuevo y original, el cual se entrega en esta misma fecha. Según el informe adjunto, al momento del ingreso del equipo no se evidenció cable de corriente, y el cable visible en las fotografías correspondía a un cable HDMI, no al cable de carga.

En virtud de lo anterior, se deja constancia de que:

1. El cargador inicialmente correspondiente al equipo no fue recibido.
2. Pese a ello, se efectuó la compra de un nuevo cargador original.
3. En la fecha se hace entrega material de dicho cargador nuevo y original.
4. Con esta entrega se suple la ausencia del cargador no recibido inicialmente.

Para constancia, se firma la presente acta por las partes que intervienen.

ENTREGA:

Nombre: William Alejandro Tique Calderon
Cargo: Director Community Manager
Fecha: 18 de marzo del 2026

RECIBE:

Nombre: Cesar Andres Yachin Gordillo
Cargo: Profesional Mesa de Ayuda
Fecha: 18-03-26

Scanned with CamScanner

NÚMERO ÚNICO DE CASO: N/A	
SOLICITANTE: JUNTA NACIONAL	**MISIÓN DE TRABAJO:** 20250101011
UNIDAD ASIGNADA: LABORATORIO DE INFORMÁTICA FORENSE	**ABOGADO:** ALEJANDRO MEJÍA ORTIZ
CIUDAD, FECHA Y HORA: BOGOTÁ D.C., 20 DE ABRIL DE 2026, 14:00 HORAS	

Señores
JUNTA NACIONAL DE CALIFICACIÓN DE INVALIDEZ
Bogotá. D.C.

Conforme a lo establecido en los artículos 210, 255, 257, 261,275 y artículos 218, nos permitimos rendir el siguiente informe ejecutivo que detalla los procedimientos realizados.

RESUMEN EJECUTIVO

En cumplimiento de la solicitud formulada por la Junta Nacional de Calificación de Invalidez, se ejecutó el procedimiento pericial de informática forense sobre tres equipos de cómputo: un DELL W21B, un portátil Lenovo ThinkPad y un portátil MacBook A223B. El alcance del estudio comprendió la obtención de imágenes forenses, la preservación e indexación de la evidencia digital y la verificación de la presencia, gestión o rastros asociados al archivo denominado “Alegatos Acción Popular”, conforme a protocolos de informática forense y estándares internacionales aplicables, entre ellos la ISO 27037.

Como resultado de la intervención, se logró la preservación forense de los equipos Lenovo ThinkPad y DELL W21B mediante adquisición técnica controlada, empleo de herramientas forenses especializadas, uso de bloqueador de escritura y verificación de integridad a través de valores hash. Las imágenes obtenidas fueron posteriormente indexadas y sometidas a búsqueda técnica del archivo objeto de análisis. En el caso del Lenovo, la búsqueda no arrojó coincidencias técnicamente recuperables; en contraste, en el DELL sí se identificaron archivos coincidentes, metadatos relevantes y artefactos de navegación asociados a su gestión y descarga dentro del perfil analizado.

En relación con el MacBook A223B, es preciso señalar que la actuación pericial se desarrolló dentro del máximo alcance técnicamente viable, con observancia de los principios de integridad, preservación y no alteración de la evidencia digital. Durante la intervención se realizó la fijación fotográfica, la inspección técnica del equipo, la verificación de su arquitectura de almacenamiento y la evaluación del método de adquisición forense procedente. De esta valoración se estableció que el equipo cuenta con una unidad SSD soldada directamente a la placa lógica y con chip de seguridad Apple T2, condiciones que impiden la aplicación de métodos tradicionales de extracción física del medio de almacenamiento, como sí ocurrió en los demás equipos examinados. En consecuencia, la ruta técnicamente procedente para este dispositivo depende de técnicas de adquisición lógica o adquisición en vivo, condicionadas por el acceso legítimo al volumen cifrado mediante una clave válida de FileVault.

En desarrollo de dicha actuación, se solicitó la credencial necesaria para habilitar el acceso forense al contenido cifrado. Según consta en el informe, fue suministrada una clave, la cual fue sometida a validación técnica y a intentos controlados de restablecimiento de acceso, actuaciones que fueron

registradas fotográficamente. No obstante, dicha credencial no resultó funcional para habilitar el descifrado del volumen ni para continuar con la adquisición de la información. En tal sentido, la ausencia de imagen forense del MacBook no obedece a inactividad pericial, sino a una restricción técnica real y verificable derivada del cifrado efectivo del dispositivo y de la falta de una credencial operativa al momento de la intervención.

Sobre este equipo se adelantaron labores periciales concretas y especializadas, entre ellas: documentación e inspección técnico-fotográfica, identificación de su configuración de seguridad, determinación de la imposibilidad de extracción física del medio, evaluación de técnicas forenses compatibles con macOS, validación de la clave suministrada y ejecución de intentos controlados de restablecimiento de FileVault. Tales actividades constituyen trabajo pericial material y metodológicamente sustentado, orientado a preservar la evidencia y a agotar el alcance técnico seguro de intervención sobre el dispositivo.

Asimismo, desde el punto de vista forense, no resultaba procedente insistir en nuevos intentos no soportados por una credencial válida, toda vez que ello podía comprometer la integridad del sistema, alterar el estado lógico del dispositivo, afectar artefactos potencialmente relevantes para el análisis o activar restricciones adicionales de seguridad, en contravía de los principios de preservación de la evidencia digital. Por tal razón, la intervención se mantuvo dentro de parámetros técnicamente seguros, trazables y compatibles con las buenas prácticas periciales, privilegiando la conservación del valor probatorio de la información sobre maniobras invasivas o potencialmente disruptivas.

En el equipo DELL W21B se halló el archivo “ALEGATOS ACCION POPULAR.pdf” en rutas del sistema bajo la estructura GUSTAVO\CONTESTACIONES DDA\ACCION POPULAR, así como una versión en formato .docx, ambas con metadatos de creación, acceso, modificación, autoría y último guardado. Adicionalmente, se identificaron rastros de descarga y gestión a través del navegador, vinculados al perfil gustavo.zarate y al aplicativo Ciclo de Firma. En el equipo Lenovo, por su parte, la búsqueda exhaustiva dentro del universo indexado no evidenció coincidencias recuperables del archivo objeto de análisis. Bajo ese contexto, la incidencia técnica presentada con el MacBook no alteró el sentido de los resultados obtenidos ni modificó los hallazgos consolidados a partir de la evidencia forense válidamente adquirida y analizada en los demás equipos.

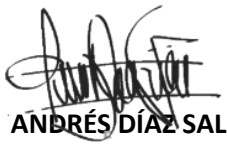
OBSERVACIONES

- La evidencia obtenida se guarda en el almacén de evidencias de la Unidad de Investigación Criminal de la Defensa, si las partes solicitan copia de esta evidencia se entregará en cualquier dispositivo de almacenamiento que se solicite.

ANEXOS

- Sin anexos para el presente informe ejecutivo el cual finaliza en tres (03) folios.

Cordialmente.



ANDRÉS DÍAZ SALAS[1].
PERITO EN INFORMÁTICA FORENSE
UNIDAD DE INVESTIGACIÓN CRIMINAL DE LA DEFENSA

Vo. Bo.



YEFRIN GARAVITO NAVARRO[2].
DIRECTOR DE LA UNIDAD DE INVESTIGACIÓN CRIMINAL DE LA DEFENSA
LABORATORIO DE INFORMÁTICA FORENSE

Aprobó



JUAN DAVID CARDONA PÉREZ[3]
CEO ARCONT GROUP SAS CIBERABOGADOS

---

1 **ANDRÉS DÍAZ SALAS:** Ingeniero de Sistemas, Perito en Informática Forense de la Unidad de Investigación Criminal de la Defensa, es Perito CiberJudicial por el Center for CIC de Boston University y AccessData Certified Examiner (ACE). Además, cuenta con certificaciones en Entrenamiento de Técnicas de Análisis Forense de Programas Maliciosos en Computadores, otorgada por la Escuela de Investigación Criminal, y en el uso de la herramienta MOBILedit Forensic de Compelson. Es profesor en la Universidad Sergio Arboleda, donde dicta las cátedras de Informática Forense y Ciberseguridad. Anteriormente, se desempeñó como instructor en Crímenes Contra el Sistema Bancario en la Procuraduría General de la Nación y en la Escuela del Ministerio Público Dra. Clara González de Behringer en Ciudad de Panamá. Cuenta con 12 años de experiencia como Investigador Criminal del Centro de Capacidades para la Ciberseguridad de Colombia (C4) de la Policía Nacional. Ha participado en diferentes intervenciones del Congreso Internacional de Derecho Penal y Cibercriminalidad, así como en el evento de Prevención del Fraude y Seguridad. También ha realizado el curso de formación de auditores internos en ISO 31000:2009 y ha recibido entrenamiento internacional en el uso básico de la herramienta Sentinel Visualizer.

2 **YEFRIN GARAVITO NAVARRO:** Ingeniero de Sistemas, Magister en Investigación Criminal de la Escuela de Investigación Criminal de la Policía Nacional, Magister en Criminología y Victimología de la Escuela de Postgrados de la Policía Nacional De Colombia, Especialista en informática forense de la Escuela de tecnología de la información y las comunicaciones de la Policía Nacional, Especialista en seguridad informática de la Universidad piloto de Colombia. Perfilador Criminal certificado por la (ABP – DIJIN), Entrenado en investigación cibernética por la KPNA (Korean National Pólice Agency), Miembro de la IACA (International Association of Crime Analysts), miembro de la plataforma de expertos EPE del EC3 de EUROPOL, director del grupo de investigaciones especiales y laboratorio de informática forense de la Unidad de Investigación Criminal de la Defensa (UID), 18 años de experiencia en el área de investigación judicial, Criminalística y ciencias forenses. Ha sido Investigador y perito testigo en diferentes Juzgados, Tribunales y ante la Corte Suprema de Justicia en diversos casos, cuenta con formación y actualización académica con Crandfield University, NIJ US Departament of Justice, Miami Dade Police, Dirección de Investigación Criminal e Interpol, KPNA entre otras entidades. Ponente Internacional en Perú, Argentina, México y otros países, docente de pregrado y postgrado de las universidades Rosario, Sergio Arboleda, Gran Colombia, Escuela de Tecnologías de la información y las comunicaciones de la Policía Nacional, Escuela de Posgrados de Policía, Escuela de Investigación Criminal Policía Nacional y de la Escuela de Guerra del ejército nacional, ha sido asesor y consultor internacional de la dirección de telemática de la Policía Nacional del Perú (PNP), de la Pan American Development Foundation, la Agencia Antinarcóticos y de Aplicación de Ley de Estados Unidos (INL) y la comisión de Acusación del Congreso de la República, participó como miembro de la delegación oficial de Colombia en cibercrimen ante las autoridades Europeas, es autor de la Guía técnica sobre análisis forense y evidencia digital y Guía de Buenas Prácticas en Investigación Forense en Casos de Crimen Organizado de INL.

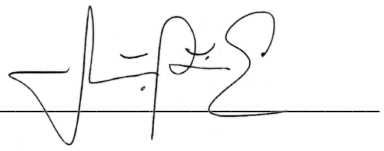
3 CIBER ABOGADO, Magister en Derecho de la Ciberseguridad y entorno digital, (Becario de la fundación Carolina en la Universidad de León / España). Magister en Derechos Humanos DDHH y Derecho Internacional De Los Conflictos Armados DICA. Conciliador en derecho. Ex funcionario de la fiscalía general de la Nación, Especialista en derecho penal y procesal penal, específicamente en el campo de los delitos informáticos, la cibercriminalidad. INGENIERO DE SISTEMAS. Especialista en seguridad informática, especialista en Informática Forense. Consultor en SGSI-ISO 27001 y 27032, auditoría forense y métodos antifraude. Presidente del Instituto Iberoamericano de Derecho Digital y de la Ciberseguridad y presidente de la IAI División Colombia en el Subcomité de Informática Forense.

DECLARACIÓN JURAMENTADA DE PAGOS DE SEGURIDAD SOCIAL Y APORTES PARAFISCALES

Yo Juan David Cardona Pérez identificado (a) con c.c. 16079489 de Manizales Representante Legal de acuerdo con lo señalado en el artículo 9 de la Ley 828 de 2003, DECLARO BAJO LA GRAVEDAD DE JURAMENTO, y con sujeción a las sanciones que para tal efecto establece el Código Penal en su artículo 442, que he efectuado el pago por concepto mis aportes y el de mis empleados (esto último en caso de tener empleados a cargo) a los sistemas de salud, pensiones, riesgos laborales, cajas de compensación familiar, Instituto Colombiano de Bienestar familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA), durante los últimos seis (06) meses calendario legalmente exigibles a la fecha de presentación de nuestra propuesta.

En caso de que el proveedor no tenga personal a cargo y por ende no esté obligado a efectuar el pago de aportes parafiscales y seguridad social, debe también bajo la gravedad de juramento indicar esta circunstancia en el presente anexo.

Dada en Bogotá a los (12) dias del mes de marzo de 2026

FIRMA 

NOMBRE DE QUIEN DECLARA Juan David Cradona Pérez

NOTA: El presente certificado deberá ser suscrito por el Representante Legal del proveedor y el Contador Público o Revisor Fiscal.