MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

Dirección General de Investigaciones y Apoyo Tecnológico a la Investigación Penal

Laboratorio de Análisis Técnico de Telecomunicaciones

INFORME PERICIAL

AUTORIDAD REQUIRENTE:

Juzgado Federal Criminal y Correccional De Lomas de Zamora N° 2

CAUSA N° FLP 38935/2023

LEGAJO DATIP N.°: 12084

1. INTRODUCCIÓN

En el marco de la causa N° FLP 38935/2023, el Juzgado Federal Criminal y Correccional De Lomas de Zamora N° 2 solicitó a esta Dirección General de Investigaciones y Apoyo Tecnológico a la Investigación Penal (DATIP), la adquisición forense de los elementos remitidos. Además, se dará respuesta a uno de los puntos de pericia propuestos por la autoridad requirente en el oficio firmado el 29 de junio de 2026 **sobre el pendrive denominado "*efecto 50*"**, el cual se transcribirá a continuación:

"i. determinen las características técnicas de cada uno de los archivos examinados, incluidos su formato, resolución, duración, tasa de cuadros, códec, metadatos o sus datos exif disponibles y demás datos que permitan establecer sus condiciones de producción y conservación".

A su vez, se informa que los restantes puntos de pericia del mencionado oficio **serán derivados al Laboratorio de Multimedia Forense de esta Dirección General**.

El Ing. Pablo Rodríguez Romeo, perito por parte de la defensa de Martin Insaurralde y el Ing. Darío Piccirilli (quien presenta y retiene para sí DNI 11.864.535), manifiestan "*la necesidad de estar presentes en el inicio de las tareas correspondientes al Laboratorio de Multimedia Forense de esta Dirección General, por lo cual se requiere la notificación correspondiente*".

Por otro lado, este Laboratorio se expedirá sobre los siguientes puntos de peritaje especificados en el oficio firmado con fecha 02 de julio de 2026, también **sobre el pendrive denominado "*efecto 50*"**:

"a- Analizando los archivos aportados, se informe la fecha cierta de creación, como así también si pudo ser modificada previo a su análisis pericial.

b- Se informe si los archivos aportados mantienen la correcta cadena de custodia como su correspondiente resguardo, realizando para ello la comparación hash. Se verifique la existencia de algoritmos de seguridad "Hash". En caso de existir, se proceda a realizar la comparación correspondiente.

c- Se realice un cotejo de imagen y determine inequívocamente si es posible establecer a identidad de la o las personas que se encuentran en el video.

d- Se informe si los metadatos de un archivo son factibles de ser adulteradas.

e- Se informe el método para determinar que un archivo no fue adulterado, modificado o cambiado en el transcurso del tiempo.

f- Se verifique la autenticidad, con el objetivo de analizar y verificar el origen real, contexto de la información aportada y el método de obtención del dato.

g- Se establezca la integridad de la información a peritar con el objetivo de verificar que el material no fue alterado, analizando por ejemplo si existe algún algoritmo de seguridad aplicado, y en ese caso calcularlo sobre los datos y compararlos.

En caso de no existir algoritmos como los mencionados, se deberá informar expresamente tal situación.

I.- Verificar la existencia de la cadena de custodia de los elementos aportados, a los efectos de conocer su trazabilidad.

II.- Verificar la forma en que se ha aportado la evidencia para el análisis pericial, es decir el nivel y estado de "preservación" de los elementos y su identificación.

III.- Se analicen e informen los metadatos de los archivos analizados, explicitando nombre del archivo, fecha de creación, acceso y modificación, y si es posible identificación

IV.- Se informen si la información remitida para su análisis fue obtenida mediante una extracción forense realizada conforme a los estándares de seguridad de la información, reservación de evidencia digital y cadena de custodia que rigen en la materia, y bajo los protocolos técnicos generalmente aplicados para el tratamiento de evidencia digital. En caso de no haberse dado cumplimiento a dichos estándares y protocolos, deberán informarlo expresamente, precisando en qué consistió el déficit detectado y si ello permite garantizar o no, la integridad, autenticidad y trazabilidad de los datos remitidos".

Finalmente, respecto a la tarjeta Micro SD, identificada como "***efecto 51***" en el oficio del día 29 de junio de 2026, se aclara que se realizará una adquisición forense y posterior procesamiento, quedando los resultados a resguardo en el **disco destino** a la espera de ser analizados por la autoridad requirente. En caso de resultar necesario, se podrá ampliar el dictamen técnico valorando los archivos que allí pudieran encontrarse.

Para verificar el estado del material probatorio al comienzo de la medida, referenciarse al acta de desintervención del día 07 del julio de 2026, en relación a la existencia de una memoria del tipo Micro SD en lugar del pendrive mencionado en la cadena de custodia correspondiente al elemento identificado como "***efecto 51***".

El presente informe da cuenta del proceso pericial de adquisiciones forenses llevadas a cabo por este Laboratorio, siguiendo las buenas prácticas de la informática forense establecidas en el *Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital* Minseg-MPF 2023, y las recomendaciones generadas por esta Dirección General en el marco de la experiencia propia de sus profesionales en el desarrollo y desenvolvimiento de las labores periciales.

2. ELEMENTOS REMITIDOS

- Un (1) pendrive de color plateado con la inscripción "*LA NACION PERIODISMO DE CALIDAD*" (**efecto 1**).

- Una (1) tarjeta micro SD marca Kingston de 32 GB de capacidad (**efecto 2**), dentro de su correspondiente adaptador SD.

3. DESARROLLO DE LAS OPERACIONES TÉCNICAS

Para llevar a cabo el procedimiento sobre dispositivos remitidos, se utilizó el siguiente equipamiento:

- **Hardware:**
  - Duplicador forense FALCON NEO2.
- **Almacenamiento:**
  - **Disco Destino:** disco rígido externo marca Seagate (s/n NACSGC8A - inventario PGN00186156) de 1 TB de capacidad.
- **Software:**
  - Autopsy (versión 4.22.1).
  - Cellebrite Inseyets Phiyical Analyzer (versión 10.10.0.1069).

3.1. DETALLE DE LOS PROCEDIMIENTOS:

El día 07 de julio de 2026 se llevaron a cabo las siguientes operaciones:

. - Con respecto al **efecto 1,** se lo conectó al duplicador forense mediante un puerto USB. Seguidamente, se conectó el **disco destino**, donde se resguardarán los resultados del proceso, verificando que se encontraba vacío, tras lo cual se le dio formato. Luego, se ejecutó el proceso de adquisición de imagen forense. Más tarde, se verificó que el proceso finalizó de forma correcta, tras lo cual se apagó el duplicador y se desconectaron el efecto 1 y el disco destino de forma segura.

. - Con respecto al **efecto 2,** se lo conectó al duplicador forense mediante puertos USB, utilizando el adaptador UFED Memory Card Reader. Seguidamente, se conectó el **disco destino**, donde se resguardarán los resultados del proceso, verificando que contenía los resultados obtenidos respecto del efecto 1. Luego, se ejecutó el proceso de adquisición de imagen forense. Más tarde, se verificó que el proceso finalizó de forma correcta, tras lo cual se apagó el duplicador y se desconectaron el efecto 2 y el disco destino de forma segura.

4. PRESERVACIÓN DE LAS IMÁGENES FORENSES

Archivos resultantes	Códigos HASH
IF_1.E01 IF_1.pdf	**MD5:** f1b70131552fd72f3ef3c6b8211b052e **SHA1:** 6142825e773d6a1f331f887cf011bebbc7057ec3
IF_2.E01 IF_2.pdf	**MD5:** a254576392f2b8750ae6ec8c97b5c21d **SHA1:** 06476fb1d9207936bfe013308d4677ada8a3a74a

5. PROCESAMIENTO DE LAS IMÁGENES FORENSES CON AUTOPSY Y PA

Se procesaron los **efectos 1 y 2** con el software AUTOPSY, utilizando los siguientes módulos:

- **Recent Activity:** extrae la actividad del usuario tal como la guardan los navegadores web (incluidas las búsquedas web), los programas instalados y el sistema operativo. También ejecuta la herramienta "Regripper", lo que le permite ver qué actividad ha ocurrido en los últimos siete días de uso, qué sitios web se visitaron, qué hizo la máquina y a qué se conectó.
- **File Type Identification:** este módulo identifica archivos basándose en su código interno, descartando su extensión.
- **Keyword search:** permite buscar determinadas palabras dentro del contenido de los archivos. También permite buscar genéricamente direcciones URL, cuentas de mail, números telefónicos, etc. Cabe destacar que, si la lista es muy general, se puede producir una gran cantidad de resultados y muchos de ellos pueden ser falsos positivos. Por ejemplo, si se indican palabras que pueden aparecer de forma masiva en un dispositivo (como por ejemplo system, card, memory, etc.), o números sin contexto de referencia. En caso de no seleccionar palabras específicas, este módulo permite realizar búsquedas en otra instancia de análisis, indicando manualmente las palabras a buscar.
- **Email Parser:** identifica archivos de formato MBOX, EML y PST, extrayendo los correos electrónicos.

Para analizar las indexaciones, se deberá abrir el archivo de cada caso, con extensión **"AUT"** (correspondiente al procesamiento descripto) **mediante el software Autopsy.** Los casos de Autopsy se encuentran en las siguientes rutas dentro del **disco destino**:

- ***Index_IF_1***
- ***Index_IF_2***

Por otro lado, se procesaron las imágenes forenses utilizando el software *Cellebrite Physical Analyzer* y se generaron los reportes correspondientes que fueron almacenados en el **disco destino**.

IF_1 (efecto 1):

Legacy

E01 Case information

Acquired Date:	1783435238
Acquired software version:	2.1u1rc0
Case Number:	12084
dc:	0
Evidence Number:	1
Media model:	Flash Disk
Media serial number:	SU804S110248
Platform/operating system:	FALCON-NEO
System Date:	1783435238
Unique Description:	IF_1

E01 Case information 2

Acquired Date:	1783435238
Acquired software version:	2.1u1rc0
Case Number:	12084
Evidence Number:	1
Platform/operating system:	FALCON-NEO
System Date:	1783435238
Unique Description:	IF_1

IF_2 (efecto 2):

Legacy

E01 Case information

Acquired Date:	1783435808
Acquired software version:	2.1u1rc0
Case Number:	12084
dc:	0
Evidence Number:	2
Media model:	uSD FRSC iDuo Re
Media serial number:	000000000505
Platform/operating system:	FALCON-NEO
System Date:	1783435808
Unique Description:	IF_2

E01 Case information 2

Acquired Date:	1783435808
Acquired software version:	2.1u1rc0
Case Number:	12084
Evidence Number:	2
Platform/operating system:	FALCON-NEO
System Date:	1783435808
Unique Description:	IF_2

6. PUNTOS DE PERITAJE

Con respecto a los puntos que constan en el oficio firmado el 29 de junio de 2026 sobre el contenido almacenado en el pendrive denominado "*efecto 50*", de común acuerdo entre los peritos, se le dará contestación al siguiente punto:

"i. determinen las características técnicas de cada uno de los archivos examinados, incluidos su formato, resolución, duración, tasa de cuadros, códec, metadatos o sus datos exif disponibles y demás datos que permitan establecer sus condiciones de producción y conservación".

De acuerdo a lo procesado y recuperado por el software PA, el dispositivo presenta el siguiente contenido (Imágenes 1 y 2):

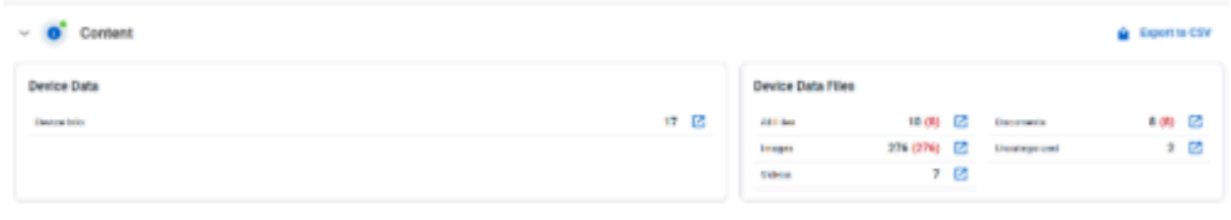


Imagen 1

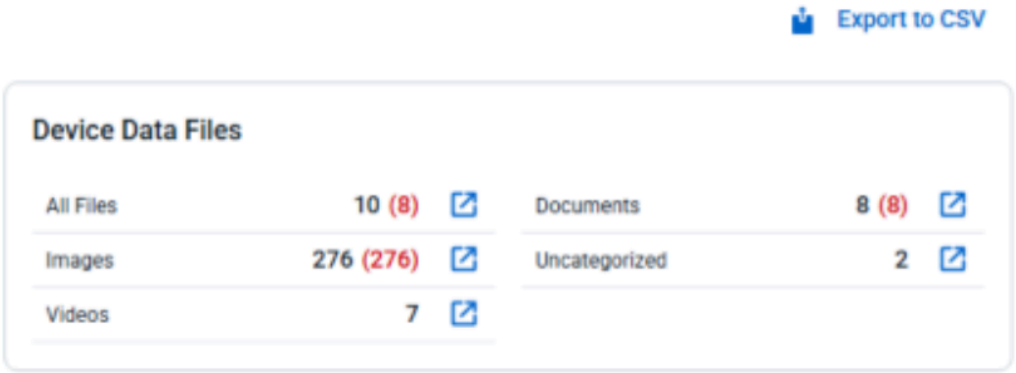


Imagen 2

Dentro de la categoría "Media", se encontraron 283 archivos de los cuales 276 se encuentran eliminados y fueron recuperados por la herramienta forense.

Esta cantidad de archivos se describe de la siguiente manera (Imagen 3):

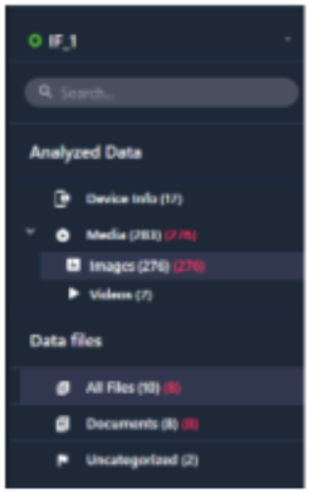


Imagen 3

Como se puede visualizar en la imagen anterior, de los 283 archivos que se encuentran en la categoría "Media", 276 corresponden a imágenes, las cuales fueron eliminadas y recuperadas por el software forense.

A continuación, se muestra una captura de dicho apartado en donde se puede visualizar que la totalidad de estos archivos corresponden a fotos en formato ".jpg", las cuales no serán objeto de análisis de este informe (Imagen 4):

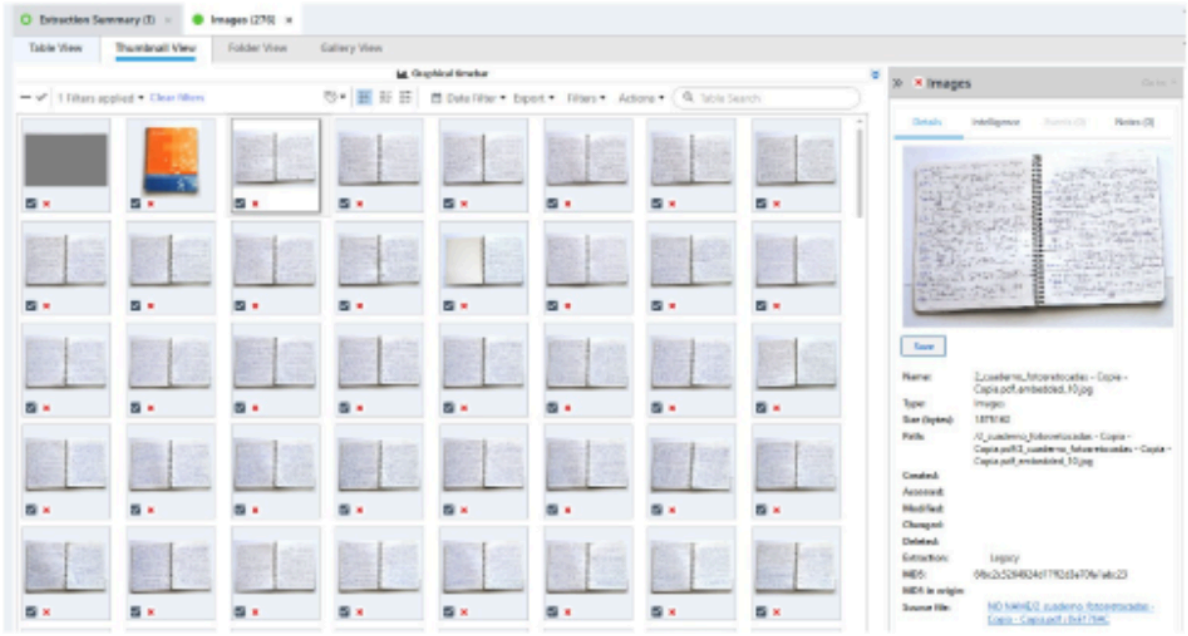


Imagen 4

Por otro lado, en el apartado "Media" también se encontraron siete (7) videos, los cuales serán objeto de análisis de este informe (Imagen 5):

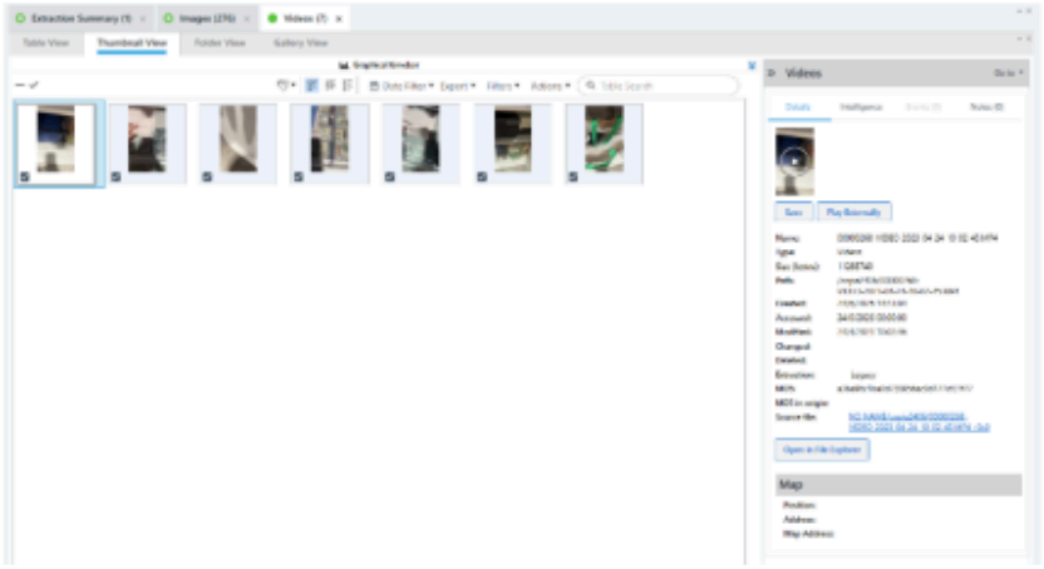


Imagen 5

Seguidamente, se adjuntan capturas de pantalla del software forense en donde se muestran los metadatos asociados a cada video y un *frame* del mismo (Imágenes 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18 y 19):

Video 1:

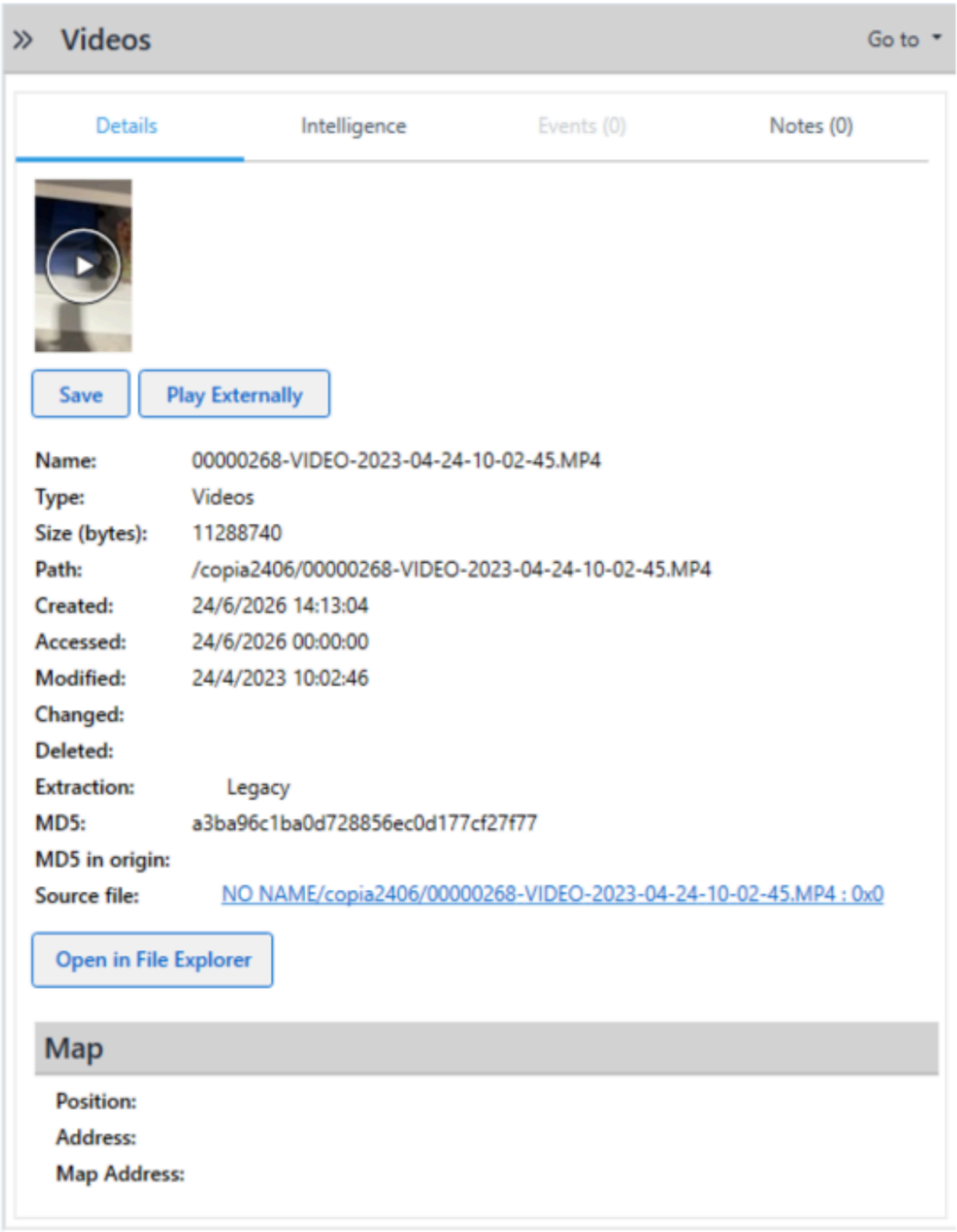


Imagen 6

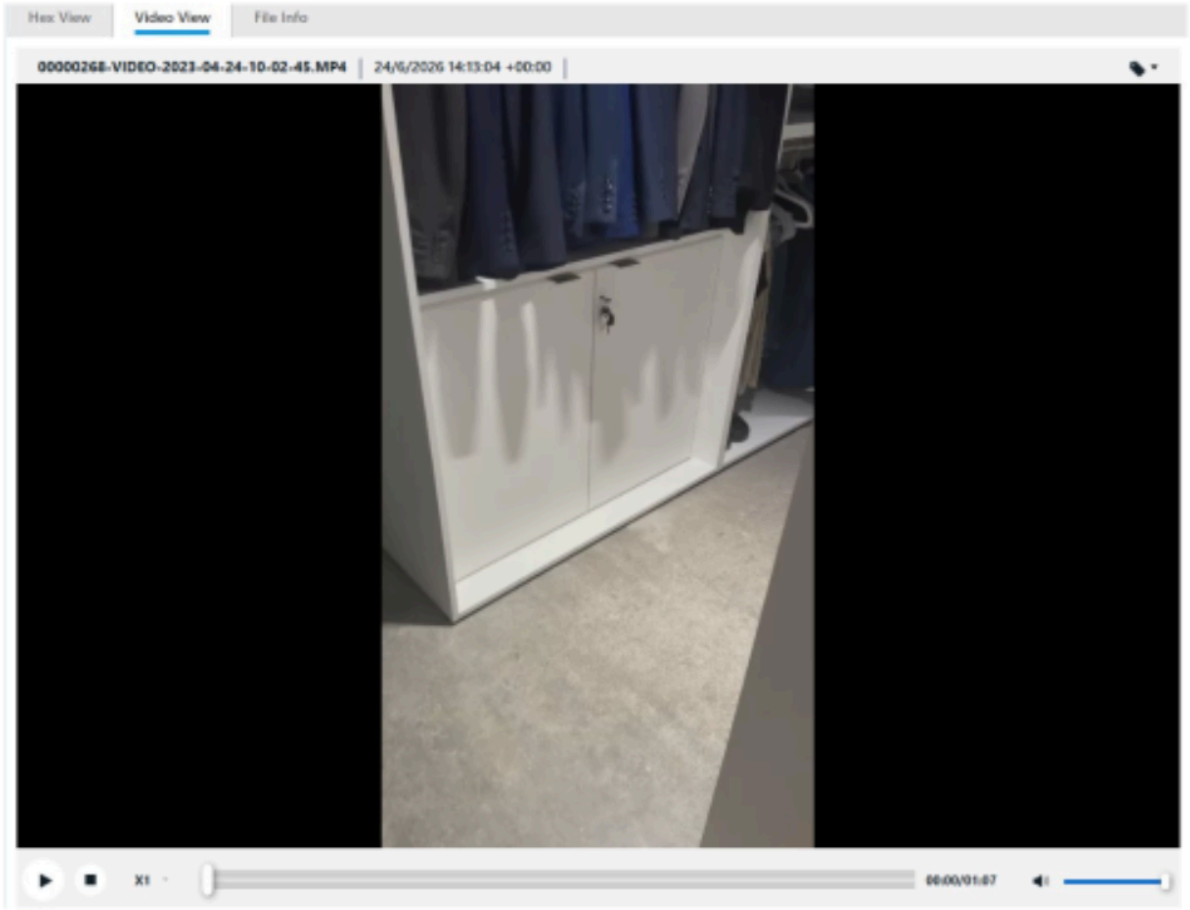

Hex View
Video View
File Info
00000268-VIDEO-2023-04-24-10-02-45.MP4
24/6/2026 14:13:04 +00:00
X1
00:00/01:07

Imagen 7

Video 2:

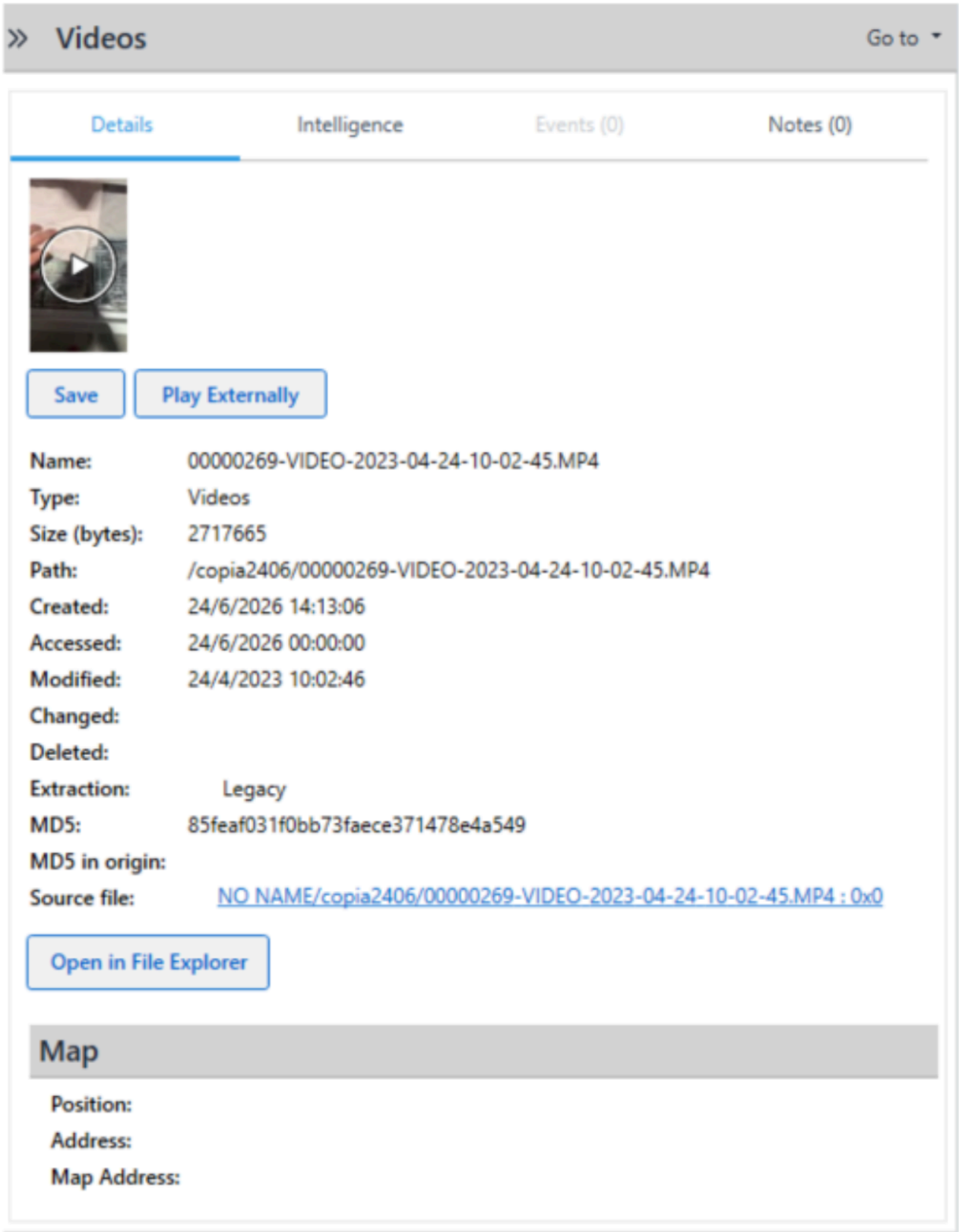


Imagen 8

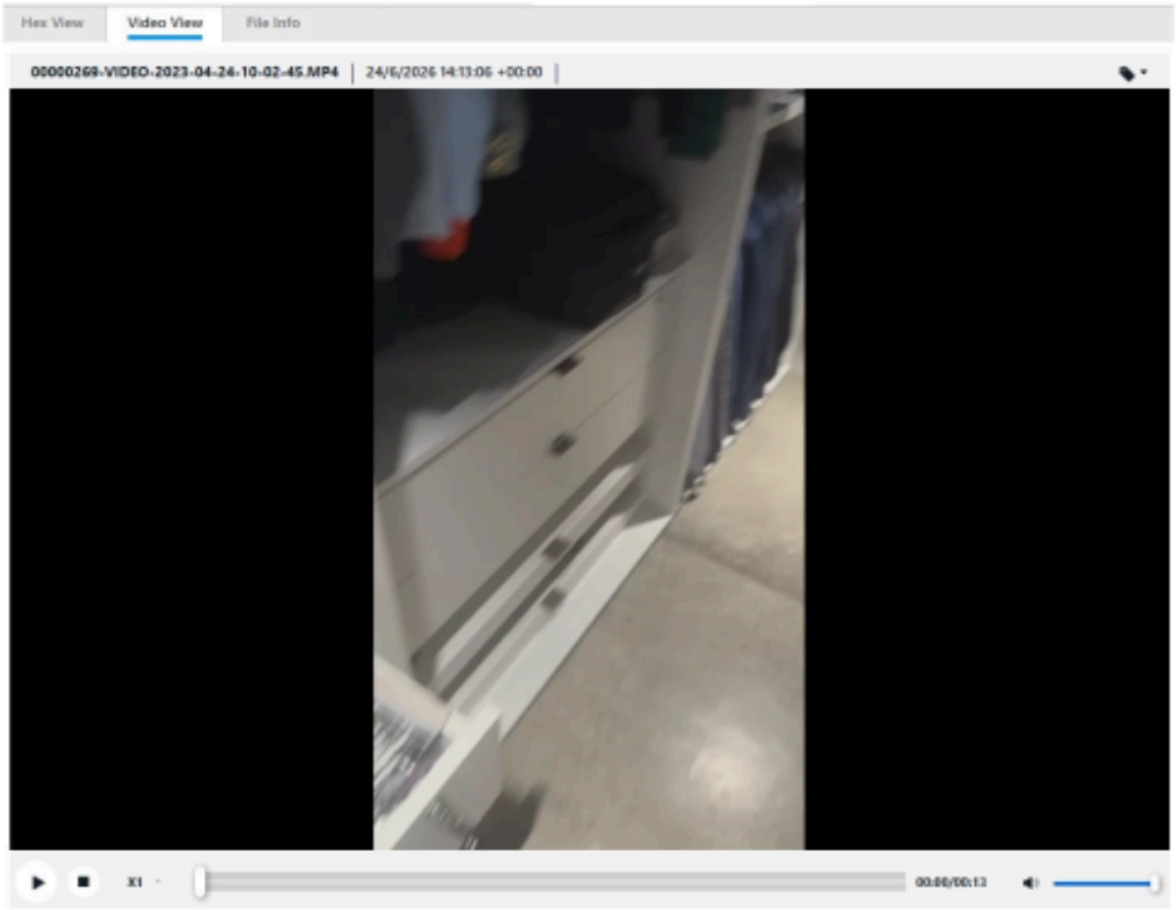

Hex View
Video View
File Info
00000269-VIDEO-2023-04-24-10-02-45.MP4
24/6/2026 14:13:06 +00:00
X1
00:00/00:13

Imagen 9

Video 3:

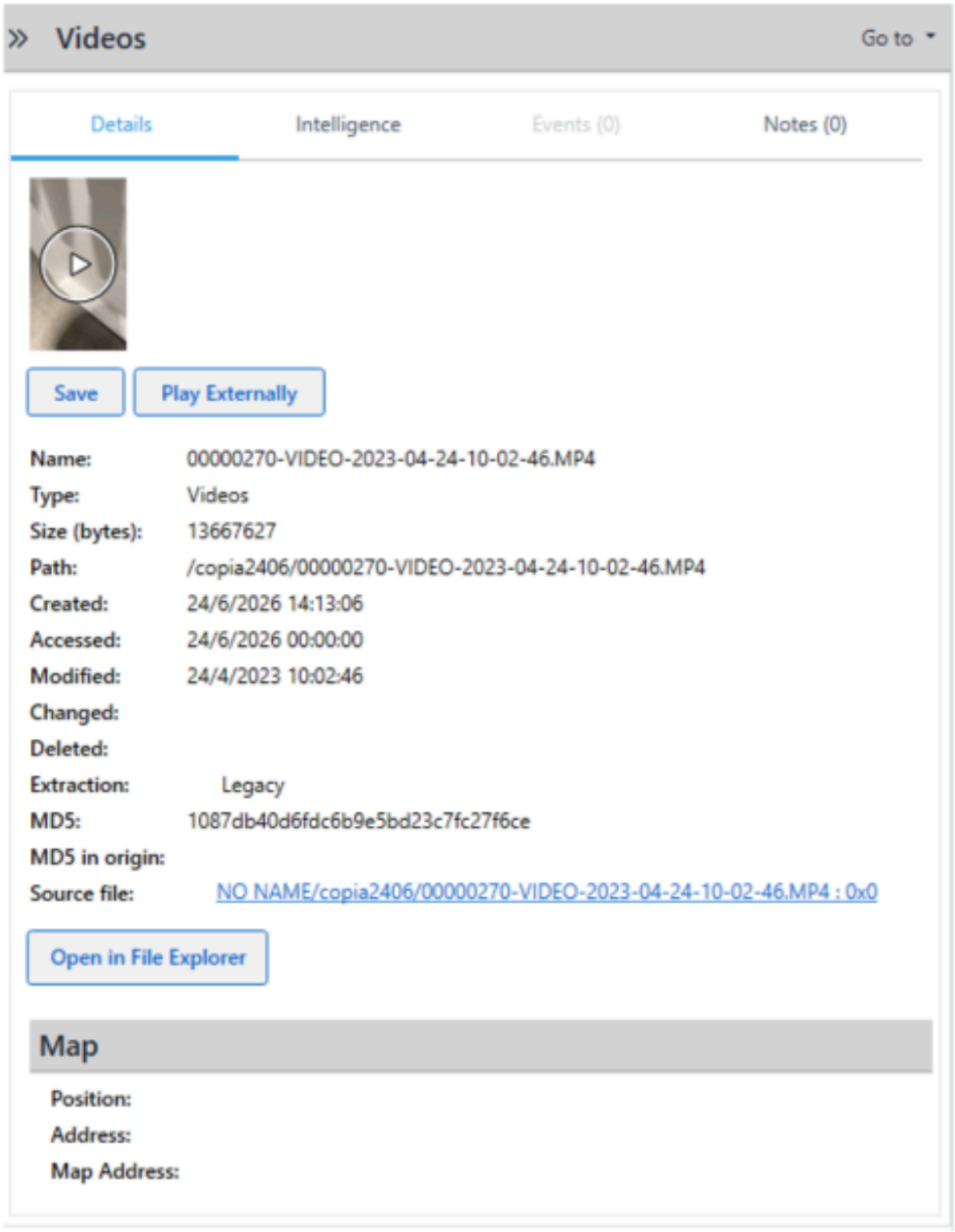


Imagen 10

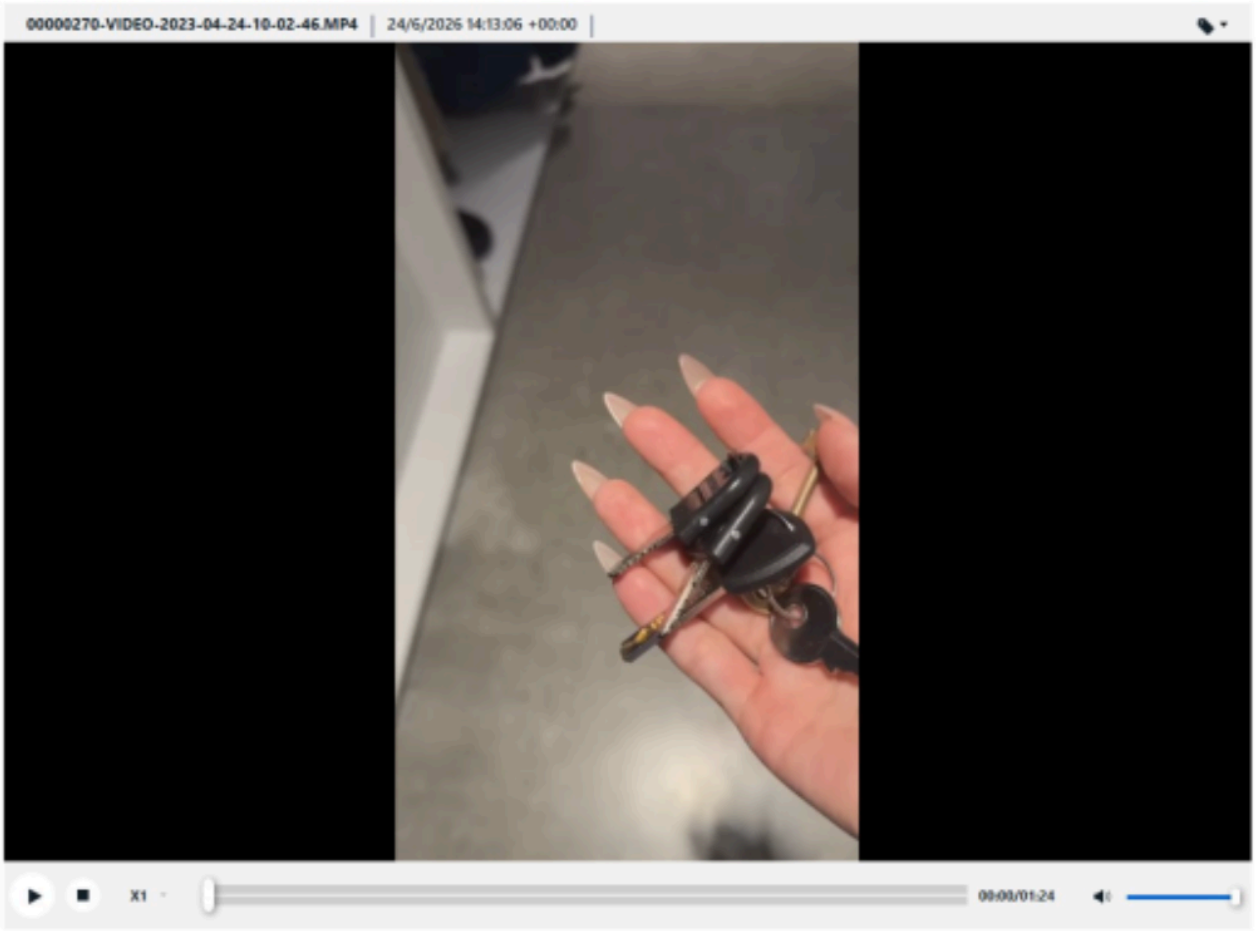

00000270-VIDEO-2023-04-24-10-02-46.MP4
24/6/2026 14:13:06 +00:00
X1
00:00/01:24

Imagen 11

Video 4:

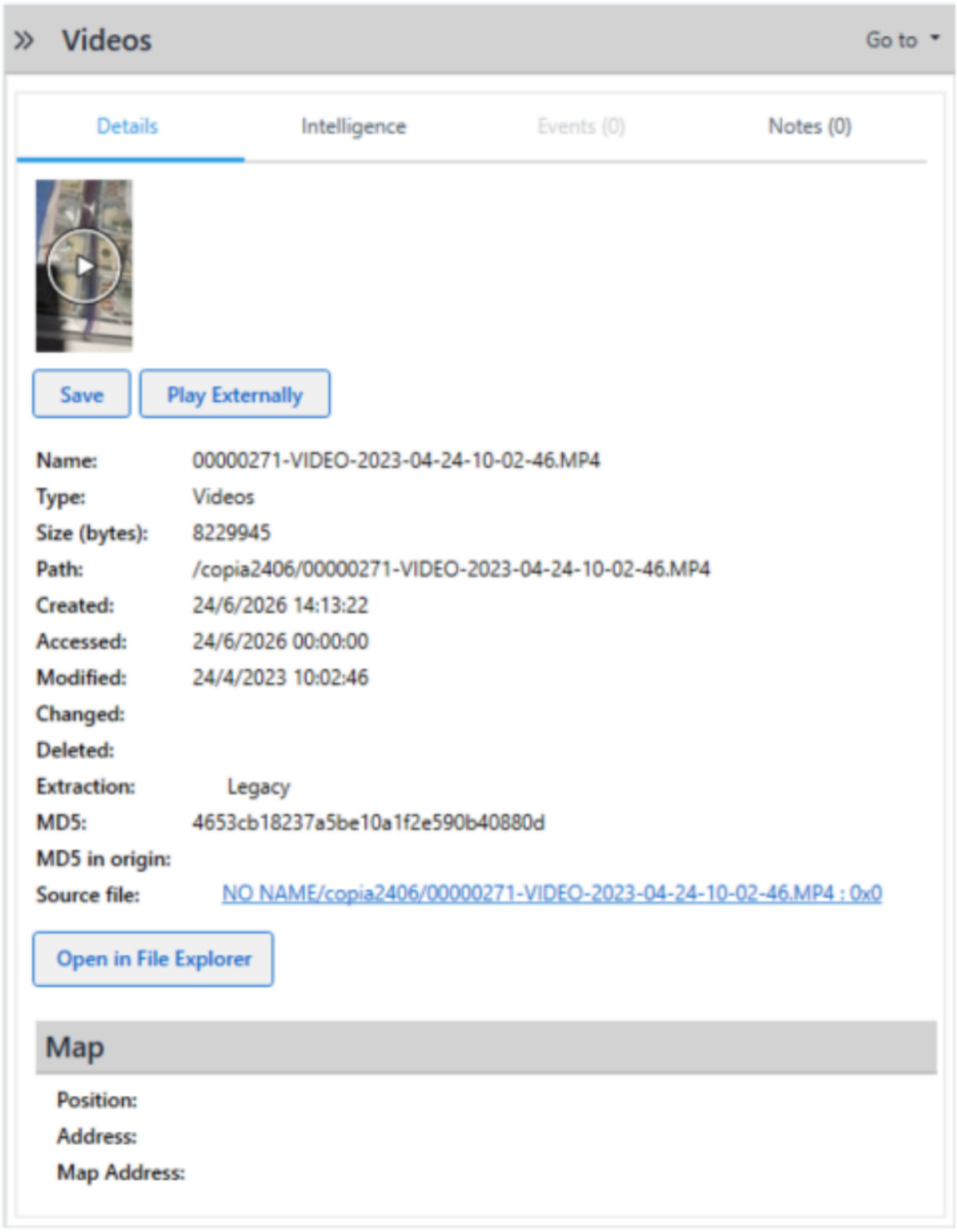


Imagen 12

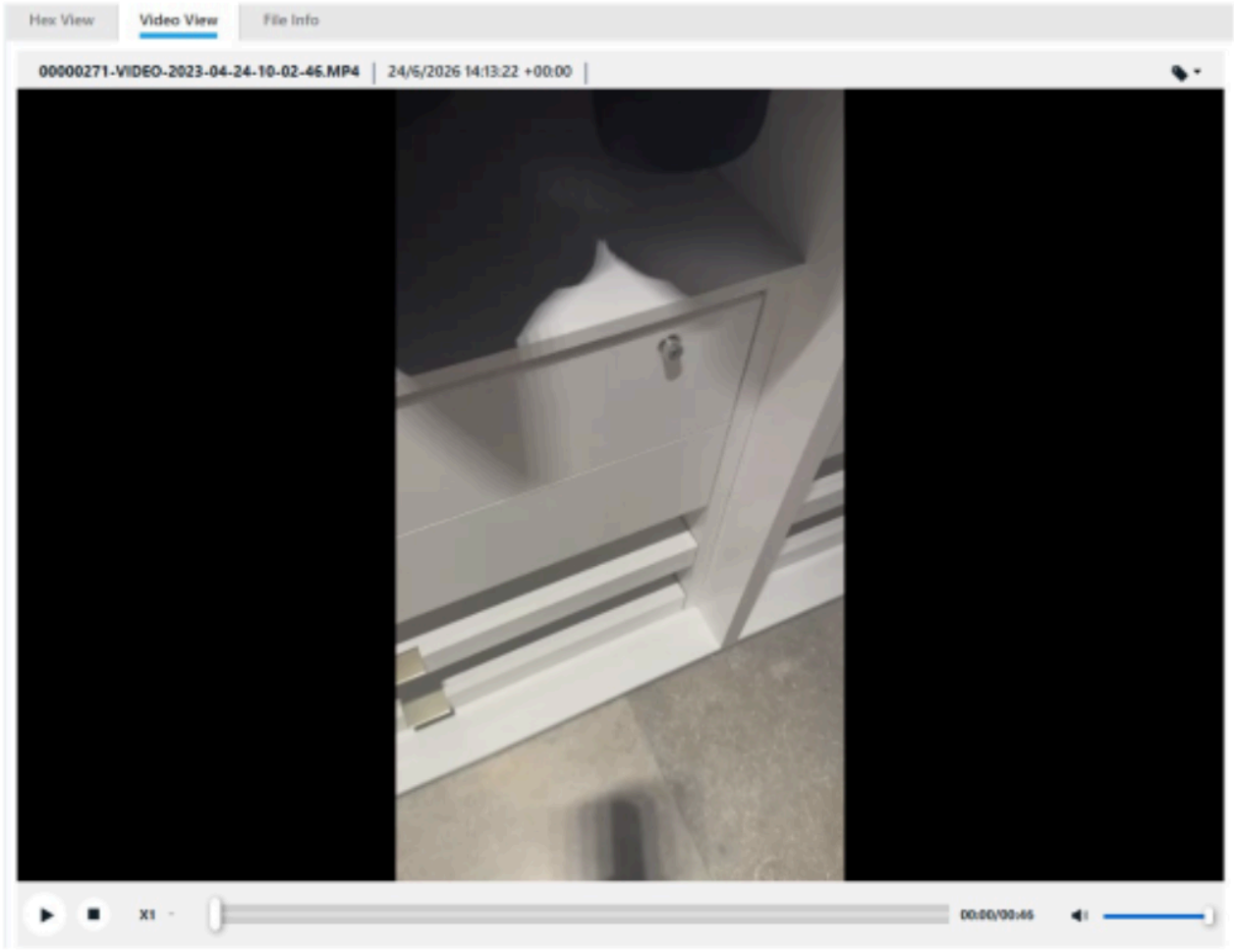

Hex View
Video View
File Info
00000271-VIDEO-2023-04-24-10-02-46.MP4
24/6/2026 14:13:22 +00:00
X1
00:00/00:46

Imagen 13

Video 5:

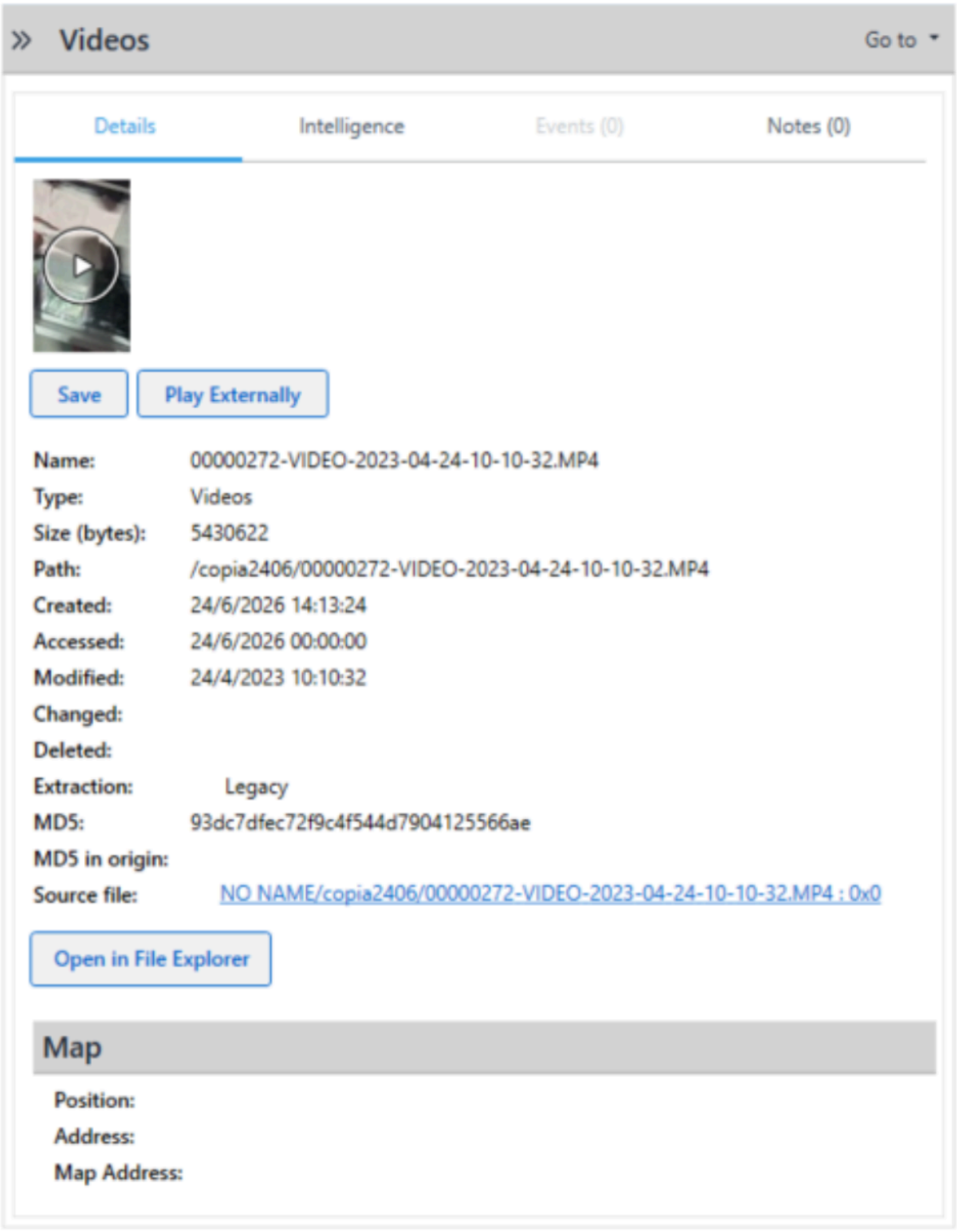


Imagen 14

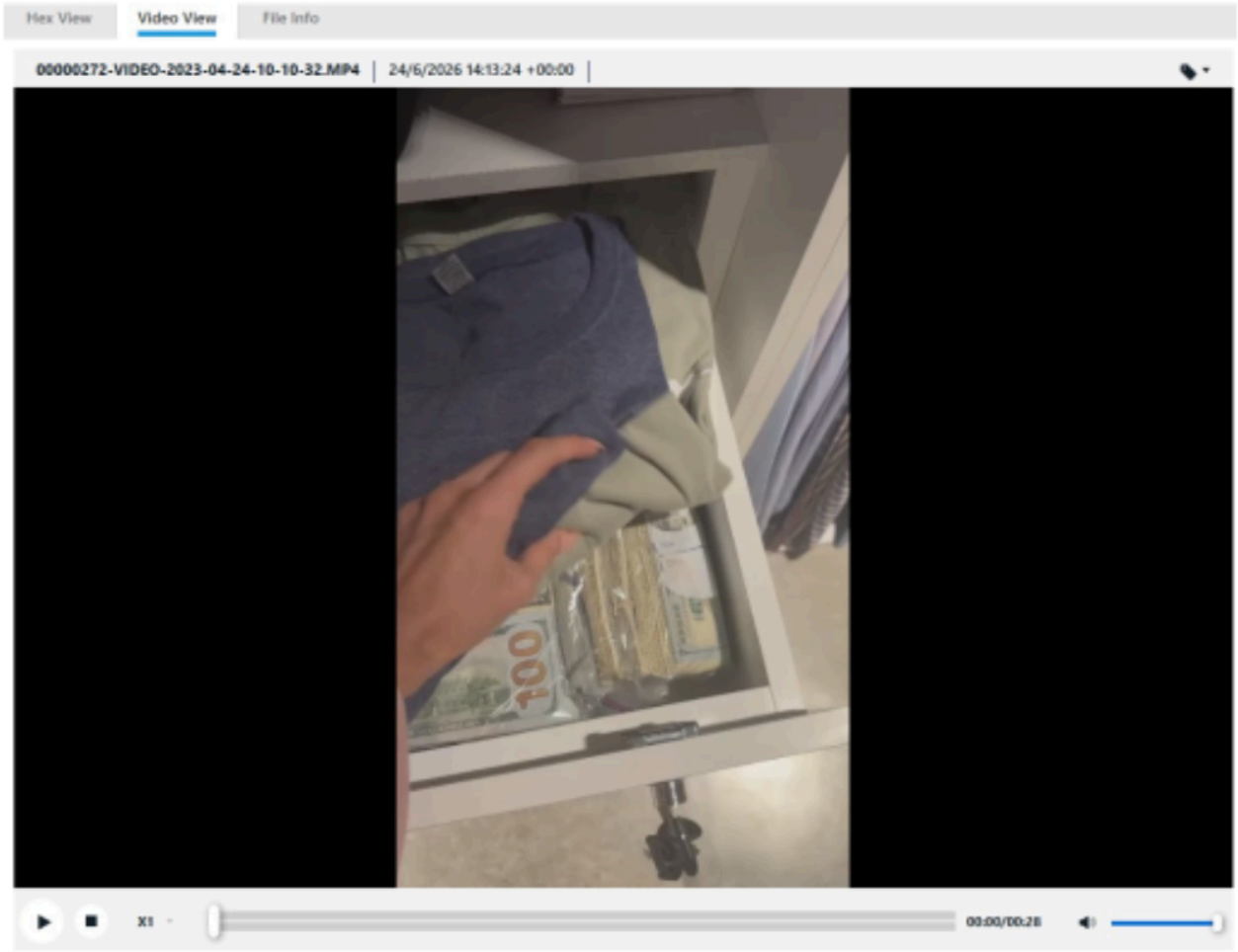

Hex View
Video View
File Info
00000272-VIDEO-2023-04-24-10-10-32.MP4
24/6/2026 14:13:24 +00:00
X1
00:00/00:28

Imagen 15

Video 6:

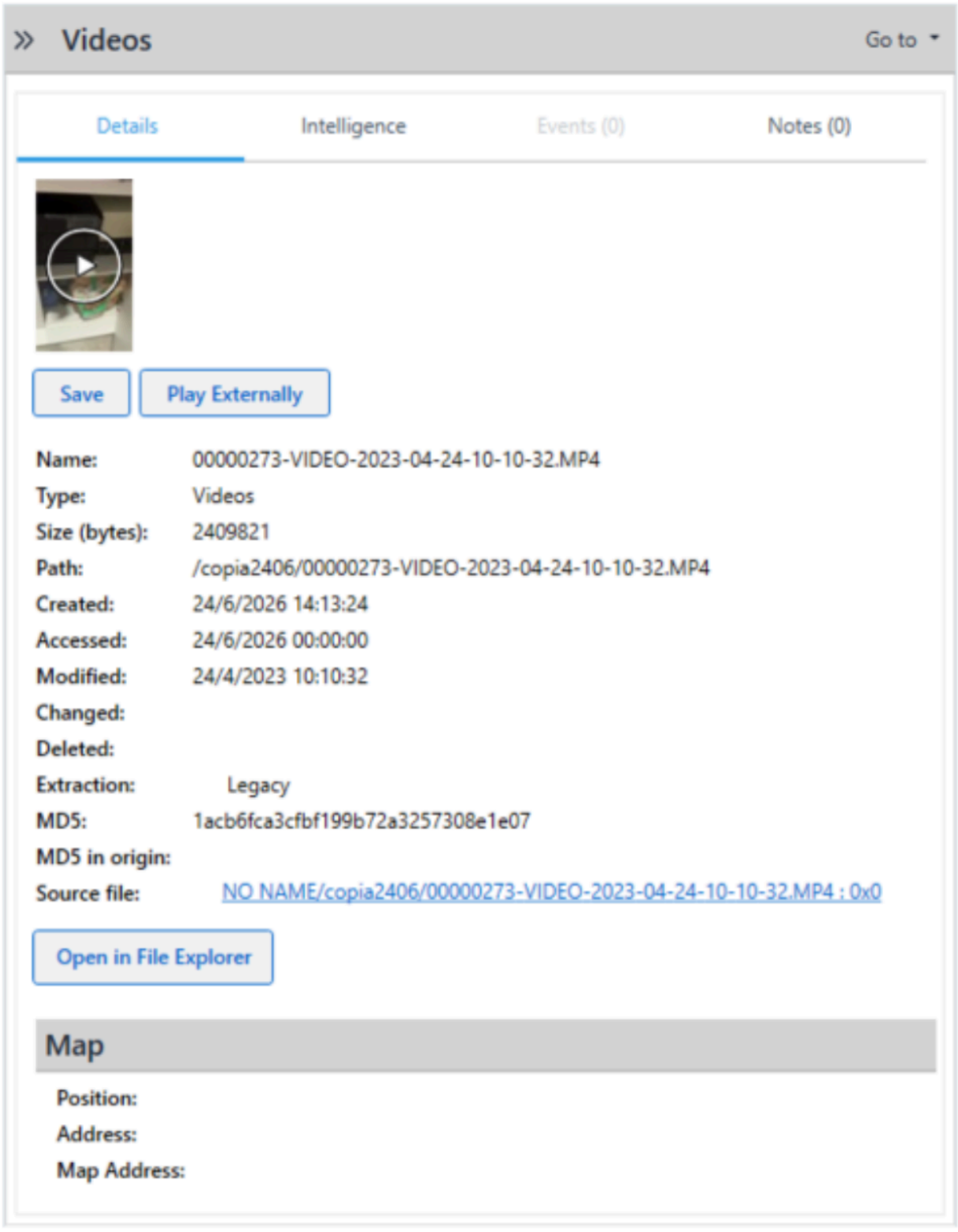


Imagen 16

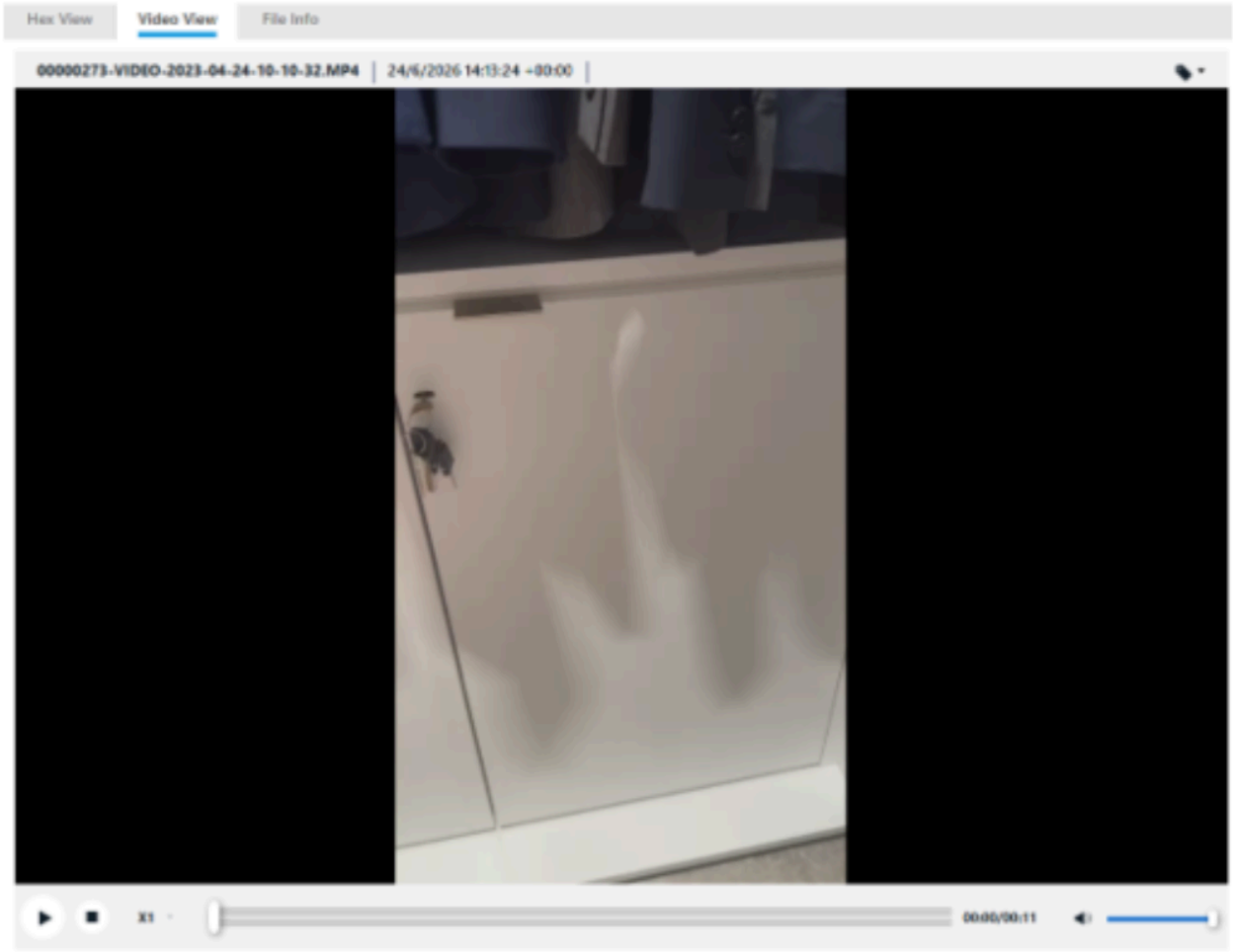

Hex View
Video View
File Info
00000273-VIDEO-2023-04-24-10-10-32.MP4
24/6/2026 14:13:24 +00:00
X1
00:00/00:11

Imagen 17

Video 7:

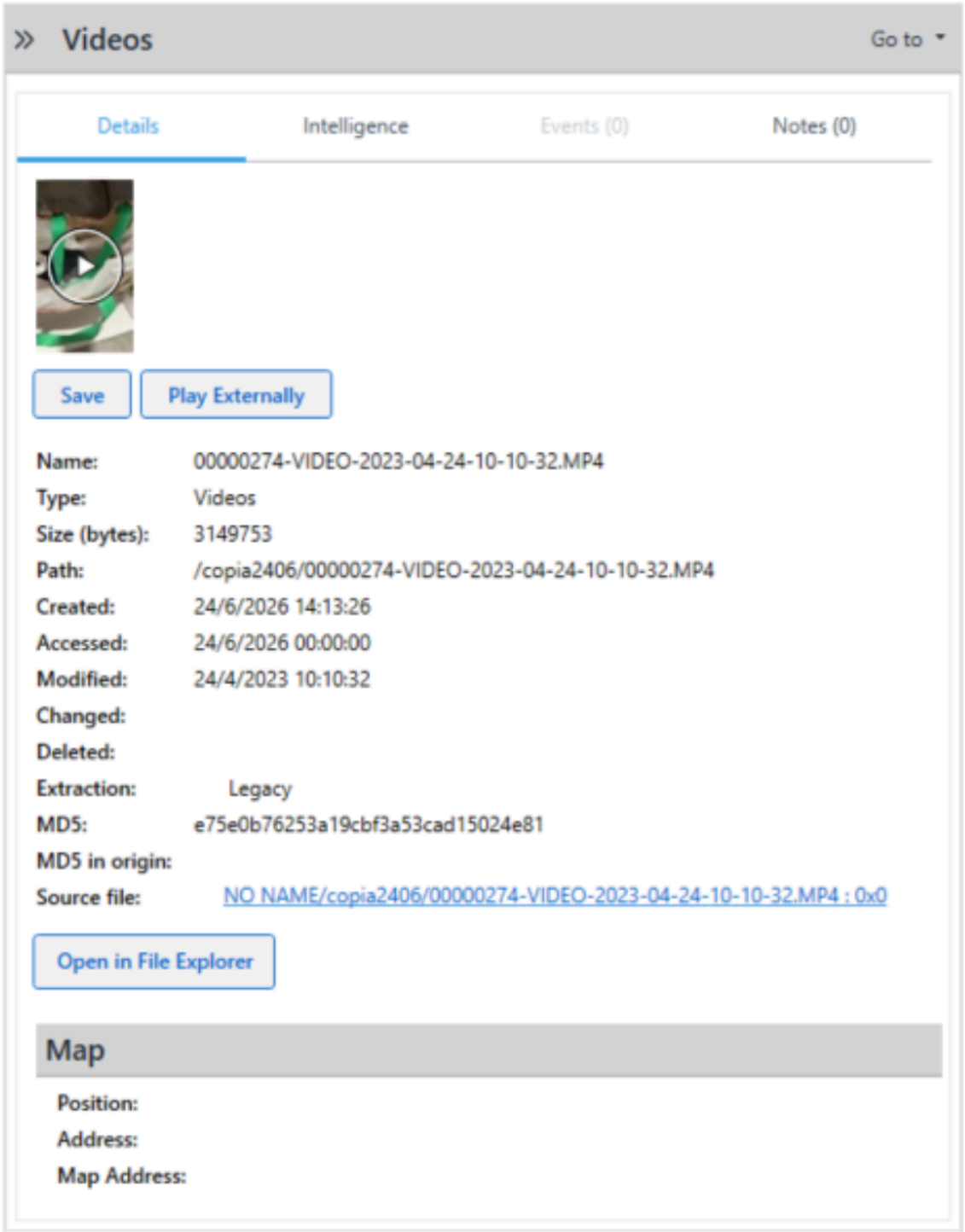


Imagen 18

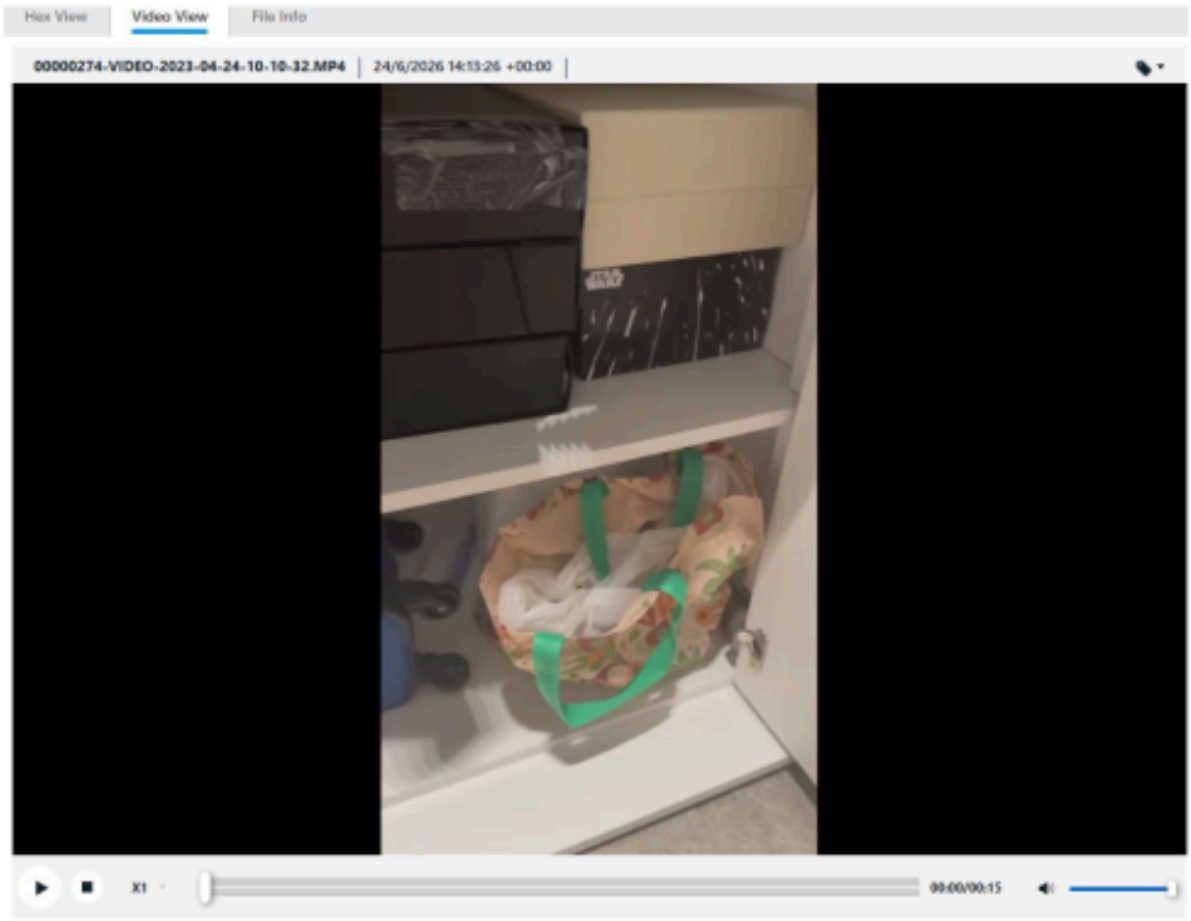
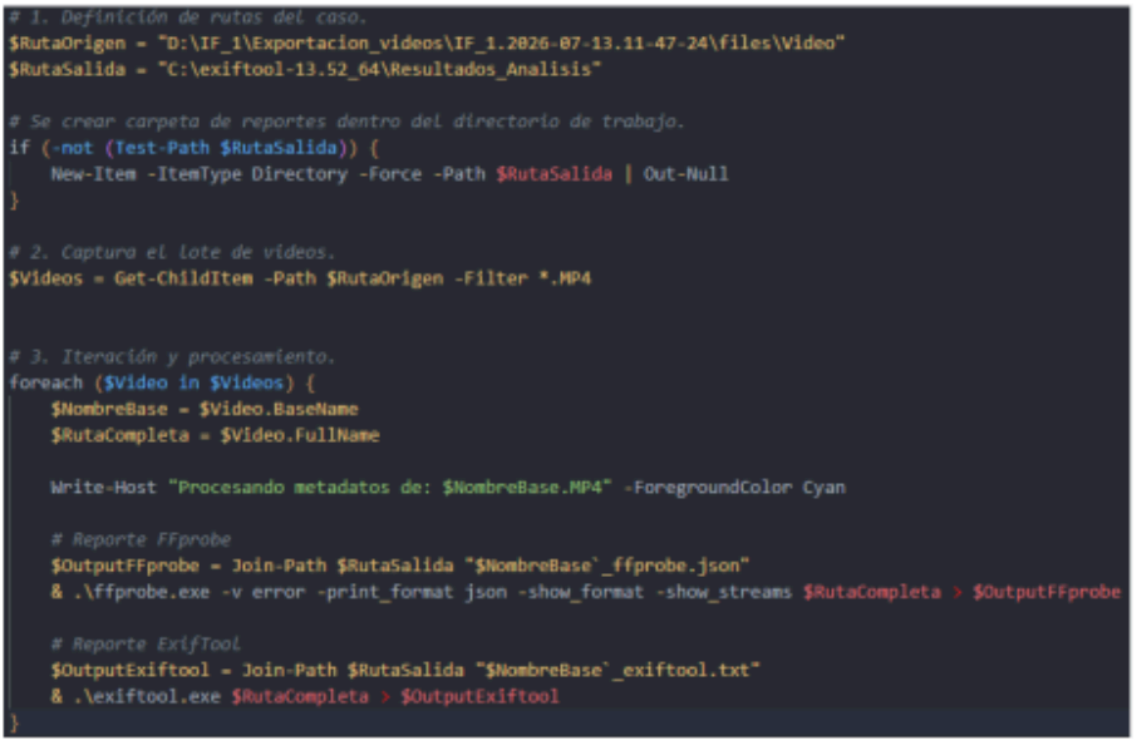


Imagen 19

De este análisis surge que la denominación de los videos se registra de forma secuencial (es decir, desde el 268 al 274).

Por otro lado, se verifica que la fecha de creación y de acceso presenta el dato del "24/06/2026". Esta situación puede representar el registro de las fechas en las cuales el video fue "creado" en el *file system* (FAT32) del *pendrive* (producto de la copia del video al pendrive), no correspondiendo a la fecha de creación del video en sí. Sin embargo, **el metadato de fecha de modificación se mantiene**, incluso luego de la copia.

Con el fin de profundizar el análisis técnico sobre los archivos con extensión *".MP4"* resguardados en el pendrive, se procedió a realizar la exportación de los siete videos y se utilizaron las herramientas *exiftool* y *ffprobe* a través del siguiente *script* en la consola *powershell* de la PC forense (Imagen 20):



```powershell
# 1. Definición de rutas del caso.
$RutaOrigen = "D:\IF_1\Exportacion_videos\IF_1.2026-07-13.11-47-24\files\Video"
$RutaSalida = "C:\exiftool-13.52_64\Resultados_Analisis"

# Se crear carpeta de reportes dentro del directorio de trabajo.
if (-not (Test-Path $RutaSalida)) {
    New-Item -ItemType Directory -Force -Path $RutaSalida | Out-Null
}

# 2. Captura el lote de videos.
$Videos = Get-ChildItem -Path $RutaOrigen -Filter *.MP4


# 3. Iteración y procesamiento.
foreach ($Video in $Videos) {
    $NombreBase = $Video.BaseName
    $RutaCompleta = $Video.FullName

    Write-Host "Procesando metadatos de: $NombreBase.MP4" -ForegroundColor Cyan

    # Reporte FFprobe
    $OutputFFprobe = Join-Path $RutaSalida "$NombreBase`_ffprobe.json"
    & .\ffprobe.exe -v error -print_format json -show_format -show_streams $RutaCompleta > $OutputFFprobe

    # Reporte ExifTool
    $OutputExiftool = Join-Path $RutaSalida "$NombreBase`_exiftool.txt"
    & .\exiftool.exe $RutaCompleta > $OutputExiftool
}
```

Imagen 20. Script en PowerShell

En este script se utilizaron los siguientes comandos:

- *.\ffprobe.exe -v error -print_format json -show_format -show_streams $RutaCompleta > $OutputFFprobe.*
- *.\exiftool.exe $RutaCompleta > $OutputExiftool*

Con respecto a la herramienta *ffprobe.exe,* se utilizaron los siguientes parámetros con el objetivo de mejorar la salida de la información:

- -v error: Omite el volcado de cabeceras predeterminadas (información de compilación, créditos de la herramienta y librerías).
- -print_format json: Fuerza la estructuración de la salida de datos bajo el estándar JSON (*JavaScript Object Notation*). Esto organiza la información en una matriz de claves y valores.
- -show_format: Proporciona los metadatos globales del archivo, incluyendo el nombre exacto de la estructura del contenedor (ej. mov, mp4), número de flujos internos, tamaño exacto del archivo en bytes, tasa de bits global (*bitrate*) y las marcas de tiempo globales de creación si estuvieran expuestas en la cabecera del archivo.

- -show_streams: Descompone de forma aislada los flujos de datos individuales encapsulados (video y audio), exponiendo:
    - Los códecs de compresión utilizados (ej. h264, hevc).
    - La resolución espacial exacta (width x height).
    - La tasa de cuadros por segundo y sus vectores de cálculo (r_frame_rate / avg_frame_rate).
    - La configuración del perfil del códec.

Con respecto a la herramienta *exiftool*, se realizó la ejecución sin parámetros de filtrado, para realizar la extracción de la estructura de metadatos del archivo de forma completa, a nivel de binario, *parseando* (organizando) todas las tablas disponibles según la especificación del tipo de contenedor.

Los resultados de este procesamiento fueron resguardados en el **disco destino** en la ruta: "\Reporte IF_1\Resultados_Analisis" (Imagen 21).

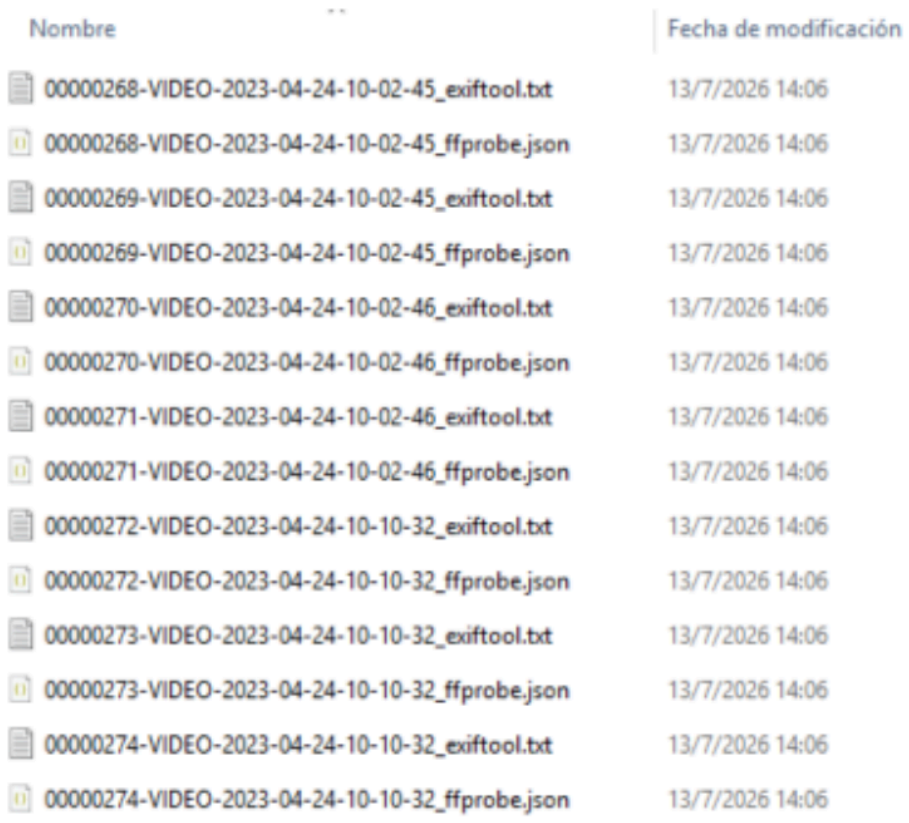


Imagen 21

Se adjuntan capturas de pantalla de los resultados obtenidos con ambas herramientas sobre el **video 1,** a modo ilustrativo (Imágenes 22, 23, 24, 25 y 26). Esta misma operatoria fue realizada sobre el resto de los videos.

exiftool.exe:

00000268-VIDEO-2023-04-24-10-02-45_exiftool.txt

```
ExifTool Version Number         : 13.52
File Name                       : 00000268-VIDEO-2023-04-24-10-02-45.MP4
Directory                       : D:/IF_1/Exportacion_videos/IF_1.2026-07-13.11-4
File Size                       : 11 MB
File Modification Date/Time     : 2023:04:24 10:02:46-03:00
File Access Date/Time           : 2026:07:13 14:06:47-03:00
File Creation Date/Time         : 2026:07:13 11:55:52-03:00
File Permissions                : -rw-rw-rw-
File Type                       : MP4
File Type Extension             : mp4
MIME Type                       : video/mp4
Major Brand                     : MP4 v2 [ISO 14496-14]
Minor Version                   : 0.0.0
Compatible Brands               : mp42, isom
Movie Header Version            : 0
Create Date                     : 0000:00:00 00:00:00
Modify Date                     : 0000:00:00 00:00:00
Time Scale                      : 44100
Duration                        : 0:01:08
Preferred Rate                  : 1
Preferred Volume                : 100.00%
Preview Time                    : 0 s
Preview Duration                : 0 s
Poster Time                     : 0 s
Selection Time                  : 0 s
Selection Duration              : 0 s
Current Time                    : 0 s
Next Track ID                   : 3
Track Header Version            : 0
Track Create Date               : 0000:00:00 00:00:00
Track Modify Date               : 0000:00:00 00:00:00
Track ID                        : 1
Track Duration                  : 0:01:08
Track Layer                     : 0
Track Volume                    : 100.00%
Image Width                     : 480
Image Height                    : 848
Graphics Mode                   : srcCopy
Op Color                        : 0 0 0
Compressor ID                   : avc1
Source Image Width              : 480
Source Image Height             : 848
X Resolution                    : 72
Y Resolution                    : 72
```

Imagen 22

```
Bit Depth                       : 24
Color Profiles                  : nclx
Color Primaries                 : BT.709
Transfer Characteristics        : BT.709
Matrix Coefficients             : BT.709
Video Full Range Flag           : Limited
Video Frame Rate                : 59.898
Matrix Structure                : 1 0 0 0 1 0 0 0 1
Media Header Version            : 0
Media Create Date               : 0000:00:00 00:00:00
Media Modify Date               : 0000:00:00 00:00:00
Media Time Scale                : 44100
Media Duration                  : 0:01:08
Media Language Code             : und
Handler Type                    : Audio Track
Balance                         : 0
Audio Format                    : mp4a
Audio Channels                  : 2
Audio Bits Per Sample           : 16
Audio Sample Rate               : 44100
Media Data Size                 : 11255799
Media Data Offset               : 32941
Image Size                      : 480x848
Megapixels                      : 0.407
Avg Bitrate                     : 1.33 Mbps
Rotation                        : 0
```

Imagen 23

ffprobe.exe:



Imagen 24

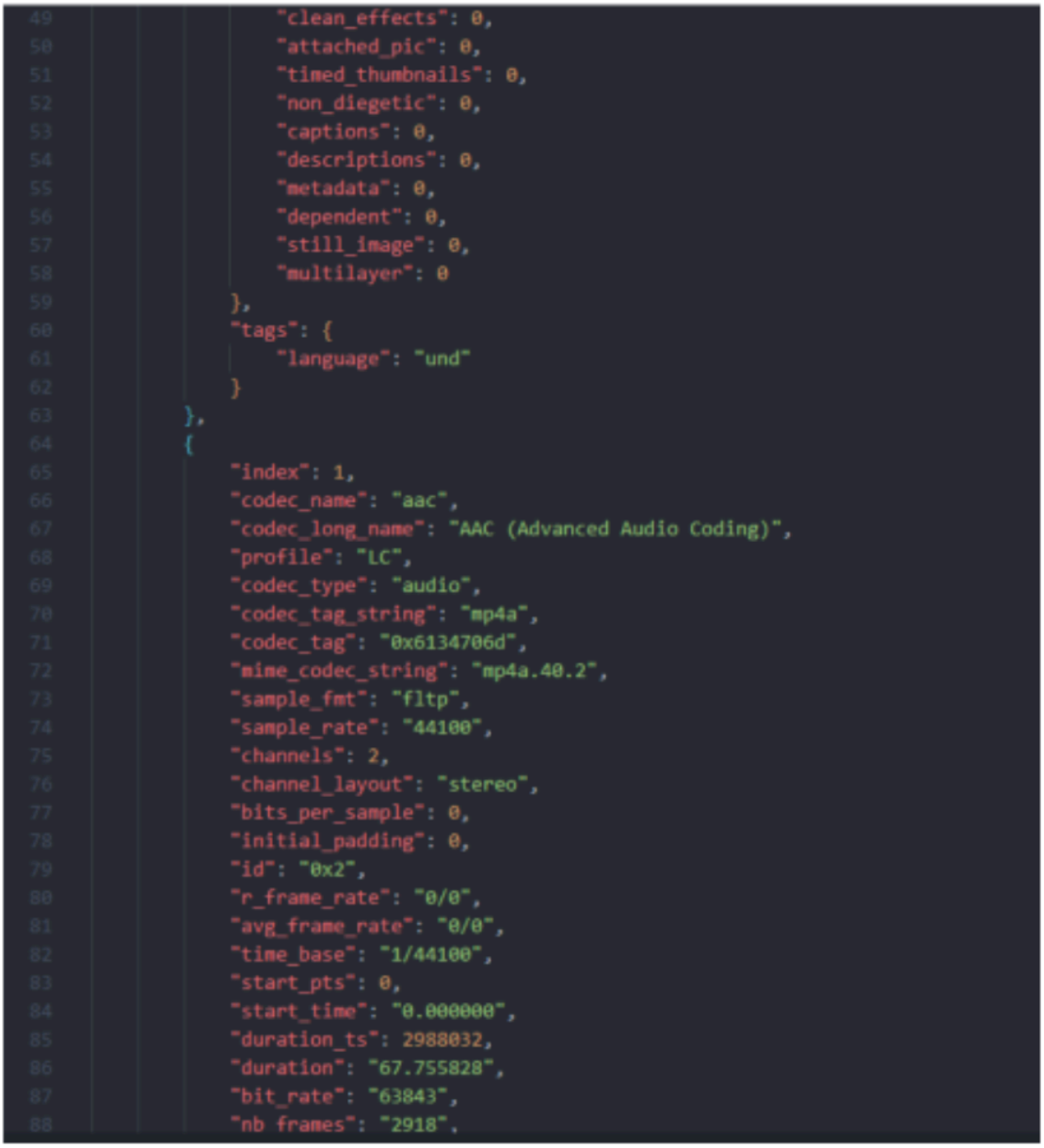
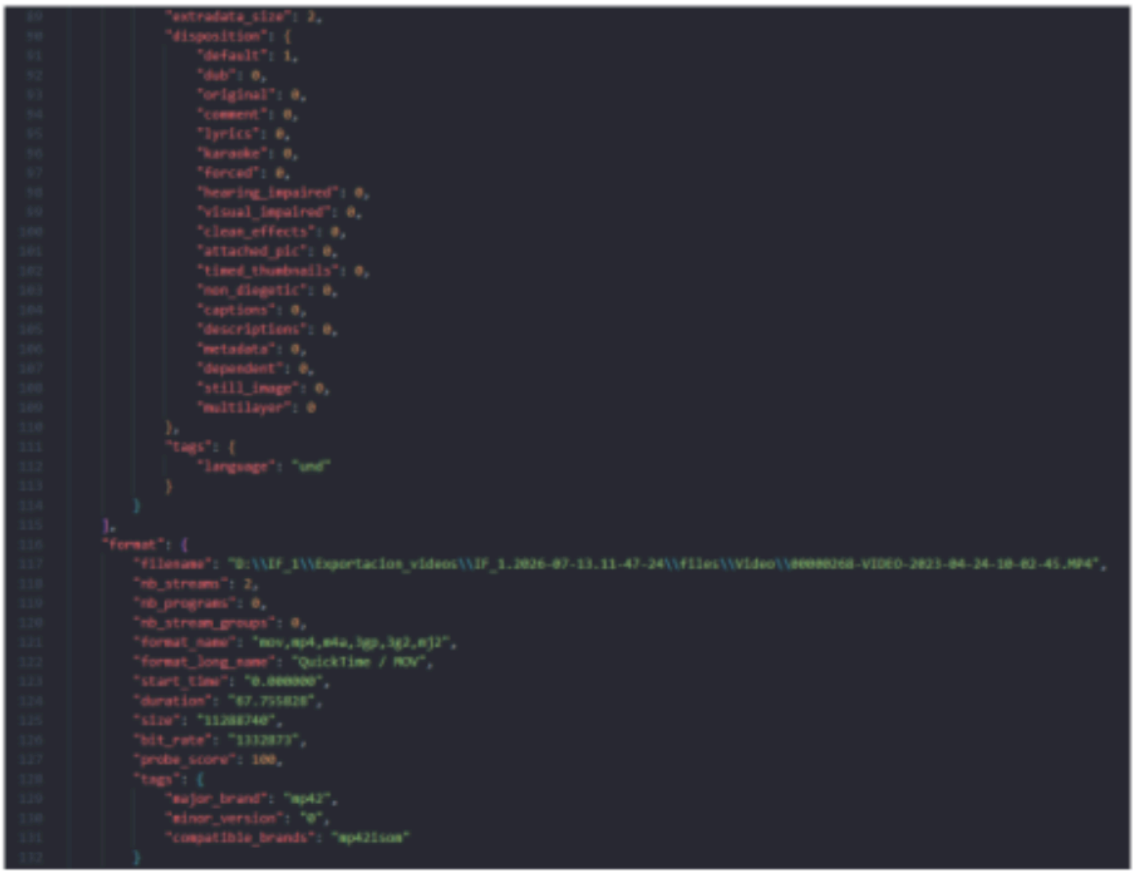

"clean_effects": 0,
"attached_pic": 0,
"timed_thumbnails": 0,
"non_diegetic": 0,
"captions": 0,
"descriptions": 0,
"metadata": 0,
"dependent": 0,
"still_image": 0,
"multilayer": 0
},
"tags": {
"language": "und"
}
},
{
"index": 1,
"codec_name": "aac",
"codec_long_name": "AAC (Advanced Audio Coding)",
"profile": "LC",
"codec_type": "audio",
"codec_tag_string": "mp4a",
"codec_tag": "0x6134706d",
"mime_codec_string": "mp4a.40.2",
"sample_fmt": "fltp",
"sample_rate": "44100",
"channels": 2,
"channel_layout": "stereo",
"bits_per_sample": 0,
"initial_padding": 0,
"id": "0x2",
"r_frame_rate": "0/0",
"avg_frame_rate": "0/0",
"time_base": "1/44100",
"start_pts": 0,
"start_time": "0.000000",
"duration_ts": 2988032,
"duration": "67.755828",
"bit_rate": "63843",
"nb_frames": "2918",

Imagen 25



```
            "extradata_size": 2,
            "disposition": {
                "default": 1,
                "dub": 0,
                "original": 0,
                "comment": 0,
                "lyrics": 0,
                "karaoke": 0,
                "forced": 0,
                "hearing_impaired": 0,
                "visual_impaired": 0,
                "clean_effects": 0,
                "attached_pic": 0,
                "timed_thumbnails": 0,
                "non_diegetic": 0,
                "captions": 0,
                "descriptions": 0,
                "metadata": 0,
                "dependent": 0,
                "still_image": 0,
                "multilayer": 0
            },
            "tags": {
                "language": "und"
            }
        }
    ],
    "format": {
        "filename": "D:\\IF_1\\Exportacion_videos\\IF_1.2026-07-13.11-47-24\\files\\Video\\00000268-VIDEO-2023-04-24-10-02-45.MP4",
        "nb_streams": 2,
        "nb_programs": 0,
        "nb_stream_groups": 0,
        "format_name": "mov,mp4,m4a,3gp,3g2,mj2",
        "format_long_name": "QuickTime / MOV",
        "start_time": "0.000000",
        "duration": "67.755828",
        "size": "11288740",
        "bit_rate": "1332873",
        "probe_score": 100,
        "tags": {
            "major_brand": "mp42",
            "minor_version": "0",
            "compatible_brands": "mp42isom"
        }
```


Imagen 26

Del análisis de los resultados arrojados por las herramientas *exiftool* y *ffprobe*, se constató que las propiedades y los metadatos internos del contenedor multimedia (.MP4) **coinciden en su totalidad** con los elementos previamente verificados e indexados mediante el software *Cellebrite Physical Analyzer*.

Se desestiman los campos "*File Access Date/Time: 2026:07:13 14:06:47-03:00*" y "*File Creation Date/Time: 2026:07:13 11:55:52-03:00*" ya que registran la fecha de trabajo sobre la exportación realizada para poder procesar los elementos con las herramientas mencionadas anteriormente.

A partir de esta validación, se determinan las siguientes condiciones técnicas, de producción y conservación para el archivo **00000268-VIDEO-2023-04-24-10-02-45.MP4**:

El elemento digital corresponde a un contenedor multimedia con formato **QuickTime / MP4v2 (especificación ISO 14496-14)**. Presenta una resolución de **480x848 píxeles** con un escaneo de tipo progresivo, una duración exacta de **1 minuto y 7 segundos** (67.75 segundos), y una tasa de cuadros por segundo de **59.898 FPS**.

El análisis binario realizado mediante *exiftool* arrojó que las marcas temporales internas de captura *(Create Date, Modify Date, Track Create Date* y *Media Create Date)* se encuentran completamente en cero (0000:00:00 00:00:00). Esto indica que el archivo **no presenta los metadatos de origen del video**, y que fue sometido a un proceso de intermediación tecnológica previo (por ejemplo, edición, transcodificación o transferencia mediante aplicaciones de mensajería social / multimedia / transferencia de archivos como *WhatsApp, Telegram, signal, wetransfer, facebook, wechat, etc*), las cuales pueden remover los metadatos de hardware del dispositivo de origen.

Con respecto a su almacenamiento actual en el pendrive, se identificó que las fechas de Creación y Ultimo Acceso registran marcas temporales recientes (**24 de junio de 2026**) en el análisis realizado en el *Physical Analyzer*, producto de la transferencia o copiado de los archivos hacia este pendrive (hacia el nuevo *file system*). Sin embargo, aparece como fecha de última modificación el dia **24 de abril de 2023,** la que en base a lo dicho anteriormente, no resulta concluyente.

Por otro lado, se identificó que los siete (7) videos se encuentran almacenados dentro de un directorio denominado "*copia2406*" (Imágenes 27 y 28).

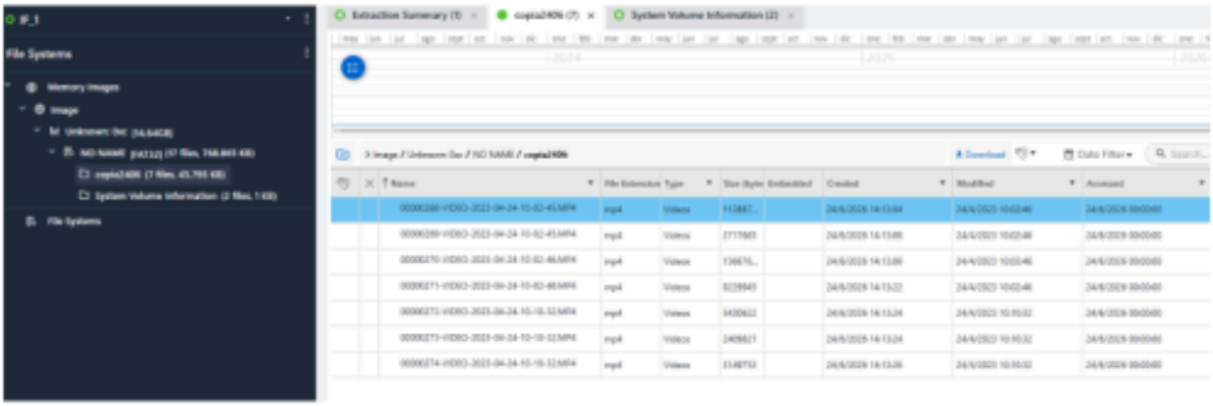


Imagen 27

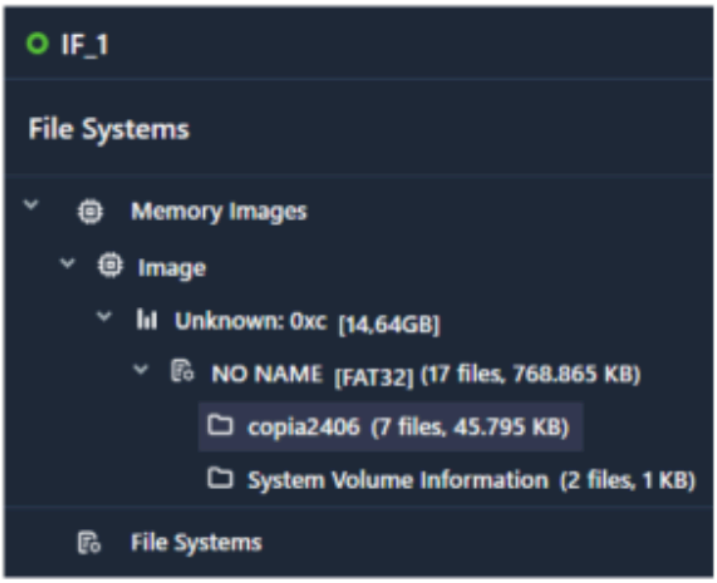


Imagen 28

A continuación, se da respuesta a los siguientes puntos especificados por la autoridad requirente en el oficio firmado el 02 de julio de 2026:

a- ***Analizando los archivos aportados, se informe la fecha cierta de creación, como así también si pudo ser modificada previo a su análisis pericial.***

Tal como se describió anteriormente, las fechas de creación y de acceso registran marcas temporales del **24 de junio de 2026**, producto de la transferencia o copiado de los archivos hacia el pendrive (hacia el nuevo *file system*). La fecha de modificación no resulta concluyente, por lo cual no es posible determinar de forma clara y fehaciente la fecha cierta de creación.

Por otro lado, el análisis mediante la herramienta *exiftool* arrojó que las marcas temporales internas de captura se encuentran en cero, por lo que podemos asegurar que se han perdido los metadatos de origen.

De igual forma, se adjuntan los *timestamp* registrados en cada uno de los siete (7) videos.

Video 1:

- Nombre del archivo: 00000268-VIDEO-2023-04-24-10-02-45.MP4
- Fecha de creación: 24/6/2026 14:13:04
- Fecha de acceso: 24/6/2026 00:00:00

- **Fecha de modificación: 24/4/2023 10:02:46**

Video 2:

- Nombre del archivo: 00000269-VIDEO-2023-04-24-10-02-45.MP4
- Fecha de creación: 24/6/2026 14:13:06
- Fecha de acceso: 24/6/2026 00:00:00
- **Fecha de modificación: 24/4/2023 10:02:46**

Video 3:

- Nombre del archivo: 00000270-VIDEO-2023-04-24-10-02-46.MP4
- Fecha de creación: 24/6/2026 14:13:06
- Fecha de acceso: 24/6/2026 00:00:00
- **Fecha de modificación: 24/4/2023 10:02:46**

Video 4:

- Nombre del archivo: 00000271-VIDEO-2023-04-24-10-02-46.MP4
- Fecha de creación: 24/6/2026 14:13:22
- Fecha de acceso: 24/6/2026 00:00:00
- **Fecha de modificación: 24/4/2023 10:02:46**

Video 5:

- Nombre del archivo: 00000272-VIDEO-2023-04-24-10-10-32.MP4
- Fecha de creación: 24/6/2026 14:13:24
- Fecha de acceso: 24/6/2026 00:00:00
- **Fecha de modificación: 24/4/2023 10:10:32**

Video 6:

- Nombre del archivo: 00000273-VIDEO-2023-04-24-10-10-32.MP4
- Fecha de creación: 24/6/2026 14:13:24

- Fecha de acceso: 24/6/2026 00:00:00
- **Fecha de modificación: 24/4/2023 10:10:32**

Video 7:

- Nombre del archivo: 00000274-VIDEO-2023-04-24-10-10-32.MP4
- Fecha de creación: 24/6/2026 14:13:26
- Fecha de acceso: 24/6/2026 00:00:00
- **Fecha de modificación: 24/4/2023 10:10:32**

Es de destacar expresamente que la fecha de modificación visualizada en el software forense PA **coincide en horas, minutos y segundos** en los videos identificados anteriormente en este informe como 1, 2, 3 y 4, como también en los videos identificados como 5, 6 y 7, respectivamente. Este comportamiento indicaría, entre otros motivos, una modificación manual de metadatos utilizando herramientas para tal fin o una transferencia de estos archivos desde un file system primigenio hacia un nuevo file system, en un momento determinado, realizando la operación de transferencia o copiado simultáneamente para todos los artefactos, quedando de esta forma afectado el metadato de modificación de cada archivo de manera coincidente para todos los involucrados.

Por ende, esta fecha si pudo haber sido modificada previo a su análisis pericial y no es posible determinar a ciencia cierta el metadato correcto debido a la falta del sistema de archivos original donde fueron creados los artefactos, el cual permitiría llevar a cabo la correlación completa entre los metadatos de los archivos y los metadatos del file system.

b- Se informe si los archivos aportados mantienen la correcta cadena de custodia como su correspondiente resguardo, realizando para ello la comparación hash. Se verifique la existencia de algoritmos de seguridad "Hash". En caso de existir, se proceda a realizar la comparación correspondiente.

Tal como consta en el acta de desintervención del 07 de julio de 2026, el dispositivo se encontraba dentro de *"un sobre marrón del Poder Judicial de la Nación cerrado y firmado en su pliegue de acceso, que presenta la inscripción FLP 38935/2023 EFECTO N°50 LEX 100"*, junto con su correspondiente planilla de cadena de custodia.

En cuanto a la imagen forense realizada sobre el dispositivo, presenta los siguientes

códigos HASH:

- **MD5:** f1b70131552fd72f3ef3c6b8211b052e
- **SHA1:** 6142825e773d6a1f331f887cf011bebbc7057ec3

En cuanto al contenido analizado, los siete (7) videos no presentan ningún documento adjunto que índique su código HASH anterior a la extracción realizada en esta DATIP, por lo que no es posible realizar la comprobación solicitada. El software *Physical Analyzer* calcula el código HASH con el algoritmo MD5 a los archivos procesados durante la pericia, los cuales se adjuntan a continuación:

Nombre de archivo	HASH MD5
00000268-VIDEO-2023-04-24-10-02-45.MP4	a3ba96c1ba0d728856ec0d177cf27f77
00000269-VIDEO-2023-04-24-10-02-45.MP4	85feaf031f0bb73faece371478e4a549
00000270-VIDEO-2023-04-24-10-02-46.MP4	1087db40d6fdc6b9e5bd23c7fc27f6ce
00000271-VIDEO-2023-04-24-10-02-46.MP4	4653cb18237a5be10a1f2e590b40880d
00000272-VIDEO-2023-04-24-10-10-32.MP4	93dc7dfec72f9c4f544d7904125566ae
00000273-VIDEO-2023-04-24-10-10-32.MP4	1acb6fca3cfbf199b72a3257308e1e07
00000274-VIDEO-2023-04-24-10-10-32.MP4	e75e0b76253a19cbf3a53cad15024e81

Por otro lado, se calculó el código HASH con los algoritmos SHA1 y MD5 de los siete (7) archivos exportados (Imagen 29):

Filename	MD5	SHA1
00000268-VIDEO-2023-04-24-10-02-45.MP4	a3ba96c1ba0d728856ec0d177cf27f77	25aa1370b501d734f742d6e5072e9d643faca39c
00000269-VIDEO-2023-04-24-10-02-45.MP4	85feaf031f0bb73faece371478e4a549	7b50be5c37f3140722e60dcadb55780ece7d33ce
00000270-VIDEO-2023-04-24-10-02-46.MP4	1087db40d8fdc6b9e5bd23c7fc27f6ce	6fc0e6098dd2d8c0c2fce0fd0398152005fd7658
00000271-VIDEO-2023-04-24-10-02-46.MP4	4653cb18237a5be10a1f2e590b40880d	575cef1d63c3dfafed6c98ffc70589169312ee72
00000272-VIDEO-2023-04-24-10-10-32.MP4	93dc7dfec72f9c4f544d7904125566ae	77d7b85e6c414d5689b2a908e0362f5c77925b2f
00000273-VIDEO-2023-04-24-10-10-32.MP4	1acb6fca3cfbf199b72a3257308e1e07	7874f3c28bc28c88611d50c13b887dbd2e571560
00000274-VIDEO-2023-04-24-10-10-32.MP4	e75e0b76253a19cbf3a53cad15024e81	4cc1a869f31498c3626ede4d25db49023cfbb483

Imagen 29

c- Se realice un cotejo de imagen y determine inequívocamente si es posible establecer a identidad de la o las personas que se encuentran en el video.

Se dará intervención al Laboratorio de Multimedia Forense de la DATIP.

d- Se informe si los metadatos de un archivo son factibles de ser adulteradas.

En base a lo expuesto en el punto "a" del presente informe se señala que esta posibilidad existe.

Nota aclaratoria: Es importante para el desarrollo de un dictamen pericial poder obtener el sistema de archivos original donde los artefactos informáticos de interés fueron generados, para poder validar su estructura y correlacionar sus metadatos con los metadatos del sistema de archivos, pudiendo dictaminar sobre una posible adulteración con una explicación técnica detallada.

e- Se informe el método para determinar que un archivo no fue adulterado, modificado o cambiado en el transcurso del tiempo.

No existe un método único para determinar una adulteración de metadatos sobre un archivo informático. Como primera medida, se necesita adquirir el sistema de archivos original donde fueron creados/modificados los archivos de interés. Con un volcado exitoso del sistema de archivos se pueden emplear distintas técnicas de la ingeniería informática para relevar completamente los metadatos de ese sistema junto con los metadatos de los archivos involucrados, intentando verificar las correlaciones habituales en función del tipo de file system (o sistema de archivos) y sus características. En este tipo de análisis, es posible dictaminar respecto a la afectación de metadatos o comportamientos no habituales que podrán sugerir una implantación de información o adulteración de las características técnicas de algún determinado artefacto informático.

Por otro lado, en caso de contar con un elemento informático secuestrado en el marco de una causa penal, las buenas prácticas de la informática forense recomiendan realizar siempre como primera medida (excepto casos especiales) una adquisición forense con obtención

de códigos HASH de los empaquetados resultantes, con el objeto de garantizar integridad del material probatorio desde ese momento en adelante. Esta práctica evitaría cuestionamientos ulteriores sobre la adquisición, manteniendo siempre el código HASH de ese empaquetados como resguardo de integridad de esa porción de prueba digital.

Es de señalar expresamente que en el caso de las pruebas aportadas no existió cálculo alguno de algoritmos HASH que acompañara a las mismas, por lo tanto NO es posible garantizar la integridad y trazabilidad de la información aportada desde su origen.

f- Se verifique la autenticidad, con el objetivo de analizar y verificar el origen real, contexto de la información aportada y el método de obtención del dato.

Como ya se ha explicitado, al no contar con el *File System** de origen de los videos, no es posible determinar la autenticidad y el origen real de los elementos analizados. Como tampoco el contexto de la información aportada y el método de obtención del dato.

**File System: estructura utilizada por el sistema operativo para la organización de los archivos dentro de los medios de almacenamiento.*

g- Se establezca la integridad de la información a peritar con el objetivo de verificar que el material no fue alterado, analizando por ejemplo si existe algún algoritmo de seguridad aplicado, y en ese caso calcularlo sobre los datos y compararlos.

En caso de no existir algoritmos como los mencionados, se deberá informar expresamente tal situación.

Conforme lo desarrollado en las respuestas a los puntos de pericia "b" y "e" no es posible verificar la integridad del material analizado.

I.- Verificar la existencia de la cadena de custodia de los elementos aportados, a los efectos de conocer su trazabilidad.

Tal como se indica en el punto "b" de este informe, se pudo verificar la planilla de cadena de custodia del pendrive aportado, según consta en el acta de desintervención del 07 de julio del 2026.

II.- Verificar la forma en que se ha aportado la evidencia para el análisis pericial, es decir el nivel y estado de "preservación" de los elementos y su identificación.

Tal como consta en el acta de desintervención del 07 de julio de 2026, el elemento se

III.- Se analicen e informen los metadatos de los archivos analizados, explicitando nombre del archivo, fecha de creación, acceso y modificación, y si es posible identificación de quien los generó.

La respuesta al punto se considera desarrollada en el punto "a" del presente informe. Por otro lado, no posible determinar la identificación de quien generó los videos.

IV.- Se informen si la información remitida para su análisis fue obtenida mediante una extracción forense realizada conforme a los estándares de seguridad de la información, reservación de evidencia digital y cadena de custodia que rigen en la materia, y bajo los protocolos técnicos generalmente aplicados para el tratamiento de evidencia digital. En caso de no haberse dado cumplimiento a dichos estándares y protocolos, deberán informarlo expresamente, precisando en qué consistió el déficit detectado y si ello permite garantizar o no, la integridad, autenticidad y trazabilidad de los datos remitidos.

El pendrive contiene archivos producto de una copia simple o transferencia, no pudiendo determinar su origen, integridad, autenticidad y trazabilidad de los datos, tal como se señaló en los puntos anteriores de este informe.

A partir de la intervención de este Laboratorio, se logró adquirir la imagen forense del dispositivo, calculando los códigos HASH correspondientes.

7. CONCLUSIONES

Por todo lo expuesto anteriormente, es posible concluir en lo siguiente:

1) Tal como se describió anteriormente, las fechas de creación y de acceso registran marcas temporales del **24 de junio de 2026**, producto de la transferencia o copiado de los archivos hacia el pendrive, con un nuevo file system o sistema de archivos La fecha de modificación de los archivos no resulta concluyente, por lo cual no es posible determinar de forma clara y fehaciente la fecha cierta de creación de la información aportada como prueba.

Por otro lado, el análisis mediante la herramienta *exiftool* arrojó que las marcas temporales internas de captura se encuentran en cero, por lo que podemos asegurar que se han perdido algunos de los metadatos de origen, posiblemente al copiar los archivos por aplicaciones de mensajería multimedia o similares, donde se produce el truncamiento de metadatos, situación que no permite tener una trazabilidad adecuada del origen de los archivos ana-

lizados.

Es de destacar expresamente que la fecha de modificación visualizada en el software forense PA coincide en horas, minutos y segundos en los videos identificados anteriormente en este informe como 1, 2, 3 y 4, como también en los videos identificados como 5, 6 y 7, respectivamente. Por ende, esta fecha **SI** pudo haber sido modificada previo a su análisis pericial

2) En cuanto al contenido analizado, los siete (7) videos no presentan ningún documento adjunto que índique su código HASH anterior a la extracción realizada en esta DATIP por estos peritos, por lo que no es posible realizar la comparación de algoritmos de seguridad requerida en el punto de pericia, lo que hubiera permitido asegurar la trazabilidad y autenticidad de los mismos, en relación a su origen.

3) En base a lo desarrollado en los puntos "*a", "e" y "f"* del presente dictamen se concluye lo siguiente:

Al no contar con el *File System* de origen de los videos, no es posible determinar la autenticidad y el origen real de los elementos analizados. Como tampoco el contexto de la información aportada, el método de obtención del dato y la identificación de quien generó los videos.

Por otro lado, se manifiesta que siempre es posible la modificación de un metadato aislado de un archivo mediante distintas técnicas informáticas. Como ya fue mencionado, al no contar con la estructura original del sistema de archivos donde fueron generados y habitaron los videos de interés no es posible llevar a cabo un análisis integral que permita validar la actual triada de metadatos.

5) El pendrive contiene archivos producto de una copia simple o transferencia, no pudiendo determinar su origen, integridad, autenticidad y trazabilidad.

No obstante lo expuesto, se señala que en la desintervención del 7/07/2026 – sobre la cadena de custodia "***Efecto N°51 Lex 100"***:

- inicialmente se expresa ***"Conteniendo en su interior un pendrive-", registrada internamente como #12084 (9),".***
- pero en realidad existía ***una (1) tarjeta micro SD marca Kingston de 32 GB de capacidad, dentro de su correspondiente adaptador SD.***

Por lo expuesto se advierte una significativa divergencia entre la descripción de la mencionada cadena de custodia (pendrive) y el elemento finalmente verificado en el interior del sobre de la evidencia aportada (memoria SD), afectando la autenticidad y trazabilidad de los elementos aportados para el análisis pericial.

8. CONTENIDO DE LOS ENTREGABLES

En el **disco destino** se entregan los resultados de las extracciones, las adquisiciones de imagen forense y su posterior indexación y procesamiento con las herramientas forenses.

Por último, se transfirió el acta de desintervención, el anexo fotográfico, el presente informe técnico pericial y los reportes técnicos generados por el duplicador forense a la carpeta compartida ubicada en la ruta **\\repo.nas01.mpf.gov.ar\Lab_DATIP\12084\07-07-2026.**

Estos archivos fueron puestos a disposición de la autoridad requirente en la sección "Compartido contigo" del sistema NUBE del Ministerio Público Fiscal.

9. RESGUARDO DE LOS EFECTOS

. - Se cerraron las cadenas de custodia externas #**12084 (8 y 9)**.

. - Respecto al **efecto 1**, se lo colocó dentro de una bolsa plástica debidamente cerrada, firmada y termosellada. A su vez, se lo colocó en un sobre de papel madera del MPF cerrado y firmado con cadena de custodia **DATIP #12084 (12)**, creada a estos fines el día 16 de julio de 2026.

. - Respecto al **efecto 2**, se lo colocó dentro de una bolsa plástica debidamente cerrada, firmada y termosellada. A su vez, se lo colocó en un sobre de papel madera del MPF cerrado y firmado con cadena de custodia **DATIP #12084 (13)**, creada a estos fines el día 16 de julio de 2026.

. - Se resguardó el **disco destino** dentro de un sobre de papel madera del MPF con cadena de custodia #**DATIP 12084 (14)**, creada a estos fines el día 04 de agosto de 2026.

9.1. EFECTOS RESGUARDADOS

Cadena de custodia DATIP #12084 (12):





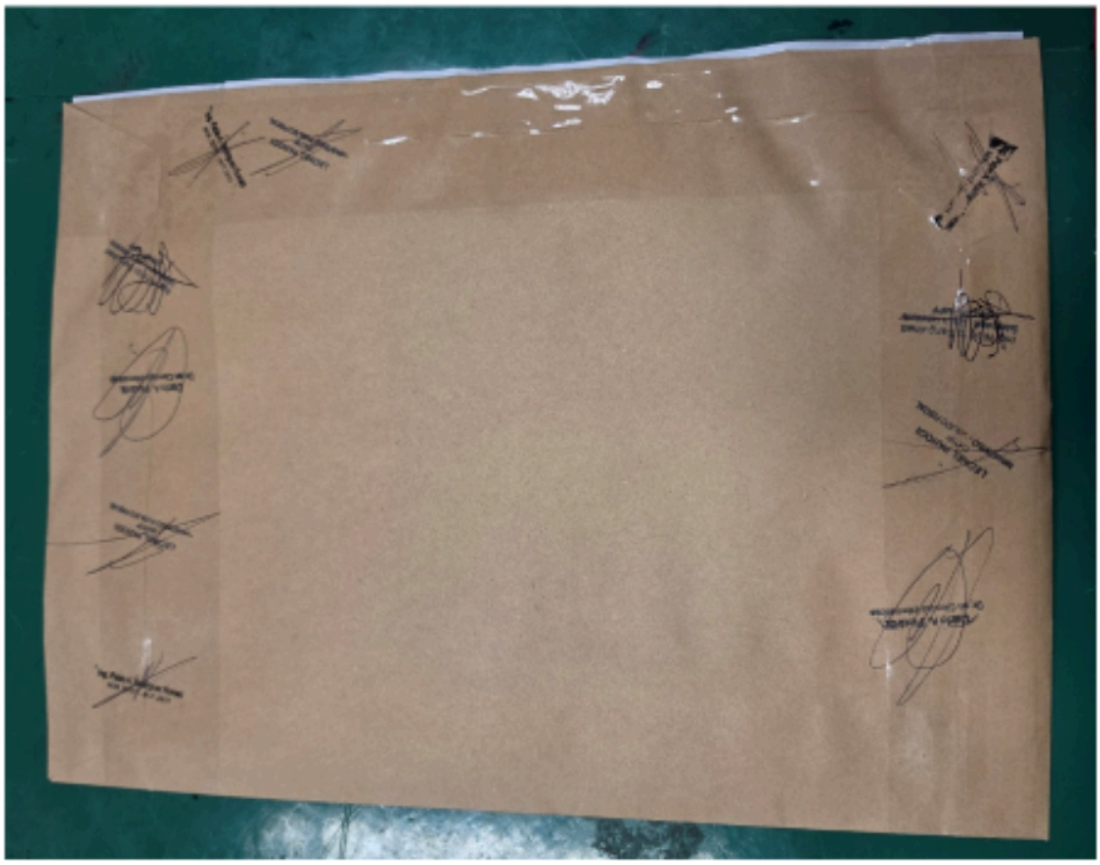

FORMULARIO DE CADENA DE CUSTODIA PARA EL MINISTERIO PUBLICO FISCAL DE LA NACION
ES COPIA



Cadena de custodia DATIP #12084 (13):







A los efectos que se estime corresponda, se deja constancia que el presente informe fue realizado por quienes suscriben, el Ing, Pablo A. Rodríguez Romeo, (MN 5117 – MP 2411), perito por parte de la defensa de Martin Insaurralde, el Ing. Darío a Piccirilli, DNI 11.864.535 (Matricula C.P.C.I.B.A. 0672), perito por parte de la defensa de Sofía Clérici, el Ing. Leonel Parodi (DNI 43.036.200) y el Ing. Nicolás Sanguineti (DNI 31.824.316), funcionario a cargo de los Laboratorios de Análisis Técnico de Informática y Telecomunicaciones de la DATIP.

Buenos Aires, 04 de agosto de 2026.

MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

ANEXO: REPORTES TÉCNICOS DE IMAGEN FORENSE

Efecto 1:

Audit Log

Vendor: Logicube
Product: Falcon-Neo2
Software Version: 2.1u1
Build Date: Nov 21, 2025 13:31:53 PST
Unit Serial Number: 223372
Time (Local): 11:40:32 (-03 -0300)
Date: Jul 07, 2026

Operation Parameters

Mode: DriveToFile
Method: E01Capture
Captured Partition: 0
Hash: SHA-1+MD5
Image Path: /var/repo/usb-d2
LBA Count: 30720000
Source Logical Sector Size: 512
Segment Size: WholeDisk
Compression Level: Default
Hash Enabled: True
Verify Hash: True
Unlock HPA: True
Unlock DCO/ACS3: True
Error Granularity: 1
Result: SUCCESS
Duration: 00:22:23
Time at Completion: 12:02:55

Hash Information

LBA Count: 30720000
Sector Size: 512
Hash Type: SHA-1
Source Hash: 6142825e773d6a1f331f887cf011bebbc7057ec3
Secondary Hash Type: MD5
Secondary Source Hash: f1b70131552fd72f3ef3c6b8211b052e

Verify Information

Drive 1

Bay: USB_D2/0ED4996C168D9CEF
LBA Count: 30720000
Sector Size: 512
Hash Type: SHA-1
Hash: 6142825e773d6a1f331f887cf011bebbc7057ec3
Result: Pass

Case Information

Case/File Name: IF_1
Case ID: 12084
Examiner:
Evidence ID: 1

Case Notes:

Efecto 2:

Audit Log

Vendor: Logicube
Product: Falcon-Neo2
Software Version: 2.1u1
Build Date: Nov 21, 2025 13:31:53 PST
Unit Serial Number: 223372
Time (Local): 11:50:05 (-03 -0300)
Date: Jul 07, 2026

Operation Parameters

Mode: DriveToFile
Method: E01Capture
Captured Partition: 0
Hash: SHA-1+MD5
Image Path: /var/repo/usb-d2
LBA Count: 61069312
Source Logical Sector Size: 512
Segment Size: WholeDisk
Compression Level: Default
Hash Enabled: True
Verify Hash: True
Unlock HPA: True
Unlock DCO/ACS3: True
Error Granularity: 1
Result: SUCCESS
Duration: 00:22:41
Time at Completion: 12:12:46

Hash Information

LBA Count: 61069312
Sector Size: 512
Hash Type: SHA-1
Source Hash: 06476fb1d9207936bfe013308d4677ada8a3a74a
Secondary Hash Type: MD5
Secondary Source Hash: a254576392f2b8750ae6ec8c97b5c21d

Verify Information

Drive 1

Bay: USB_D2/0ED4996C168D9CEF
LBA Count: 61069312
Sector Size: 512
Hash Type: SHA-1
Hash: 06476fb1d9207936bfe013308d4677ada8a3a74a
Result: Pass

Case Information

Case/File Name: IF_2
Case ID: 12084
Examiner:
Evidence ID: 2
Case Notes: