Informe Pericial 1.2: Análisis de Metadatos

Tarea 1.2 para la asignatura Auditoría Informática II

Autor:
Arturo Rivero Dutra

Fecha:
17/02/2026

Índice

Identificación

Caso: Práctica de análisis de metadatos de 3 ficheros no relacionados entre sí

Código identificador: UNI_1_2

Responsable del informe: Arturo Rivero Dutra

Entidad que solicitó el análisis: Universidad Complutense de Madrid

Persona a la que va dirigido el informe: María Inmaculada Pardines Lence

Fecha de emisión del informe: 17 de febrero de 2026

Antecedentes

La entidad que solicitó el análisis forense descrito en el presente informe requería la obtención de 3 ficheros diferentes no necesariamente conexos, así como la posterior extracción y análisis de sus respectivos metadatos.

Objetivos

- Analizar los metadatos asociados a documentos DOC, PDF e imágenes para evitar que a través de estos documentos haya fuga de información.

Análisis del Laboratorio Forense

El presente análisis forense ha sido realizado en un laboratorio consistente en 3 elementos diferentes:

1. Una Máquina Virtual la cual ha sido exclusivamente utilizada para usar la herramienta FOCA:

   Sistema Operativo (VM): Windows 11 25H2
   Nivel de Parcheado/Build: Build 26200.6584
   Arquitectura: x64, 12GB RAM, 30GB Disco

2. Una Máquina Física, *host* de la MV anterior, la cual ha sido utilizada para orquestar y organizar el análisis, además de para ejecutar todas las demás herramientas mencionadas en el presente informe:

   Sistema Operativo (VM): Windows 11 25H2
   Nivel de Parcheado/Build: Build 26200.7840
   Arquitectura: x64, 24GB RAM, 389GB Disco

3. Un dispositivo móvil utilizado únicamente para generar la evidencia de la imagen descrita posteriormente:

   Modelo: OnePlus Nord AC2001
   Sistema Operativo (VM): Android 12
   Arquitectura: ARM, 8GB RAM, 128GB Disco

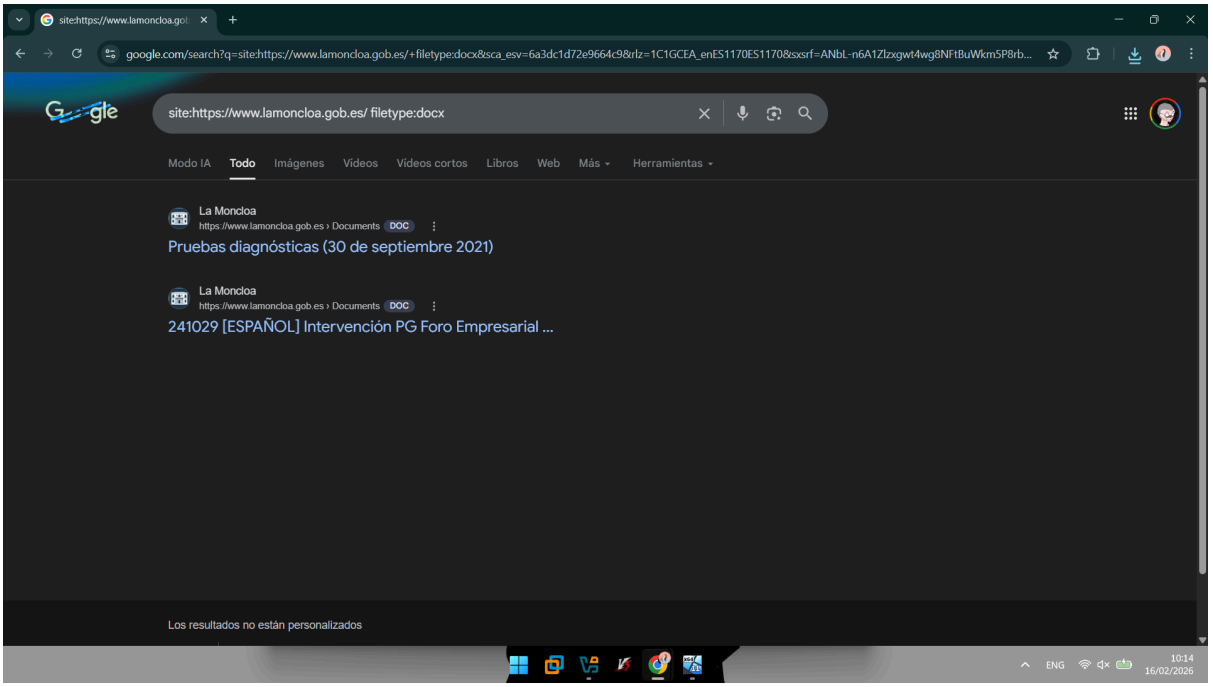
Ciclo de Vida de la Evidencias Digitales

1. Documento “.docx”

Adquisición de la Evidencia

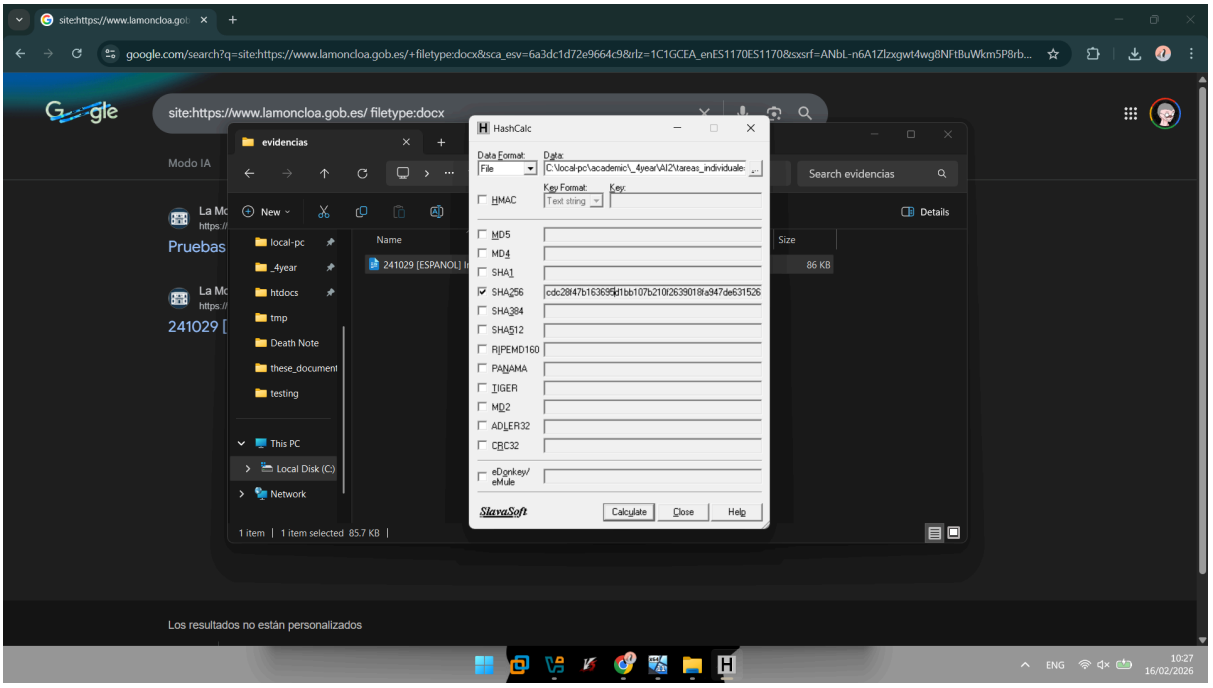
Para la obtención de esta evidencia se tenía como objetivo un archivo *.docx*. Se optó por la utilización de Google Dorks especificando la web oficial de La Moncloa como objetivo y el tipo de fichero *.docx* de acuerdo a la siguiente búsqueda:

> *site:https://www.lamoncloa.gob.es/ filetype:docx*



Se seleccionó el segundo resultado y se procedió a descargarlo.

Una vez obtenido el fichero *241029 [ESPAÑOL] Intervención PG Foro Empresarial España-India.docx*, la primera acción tomada fue calcular su *hash SHA-256* para capturar la integridad de la evidencia original. Para ello, se empleó el programa HashCalc:

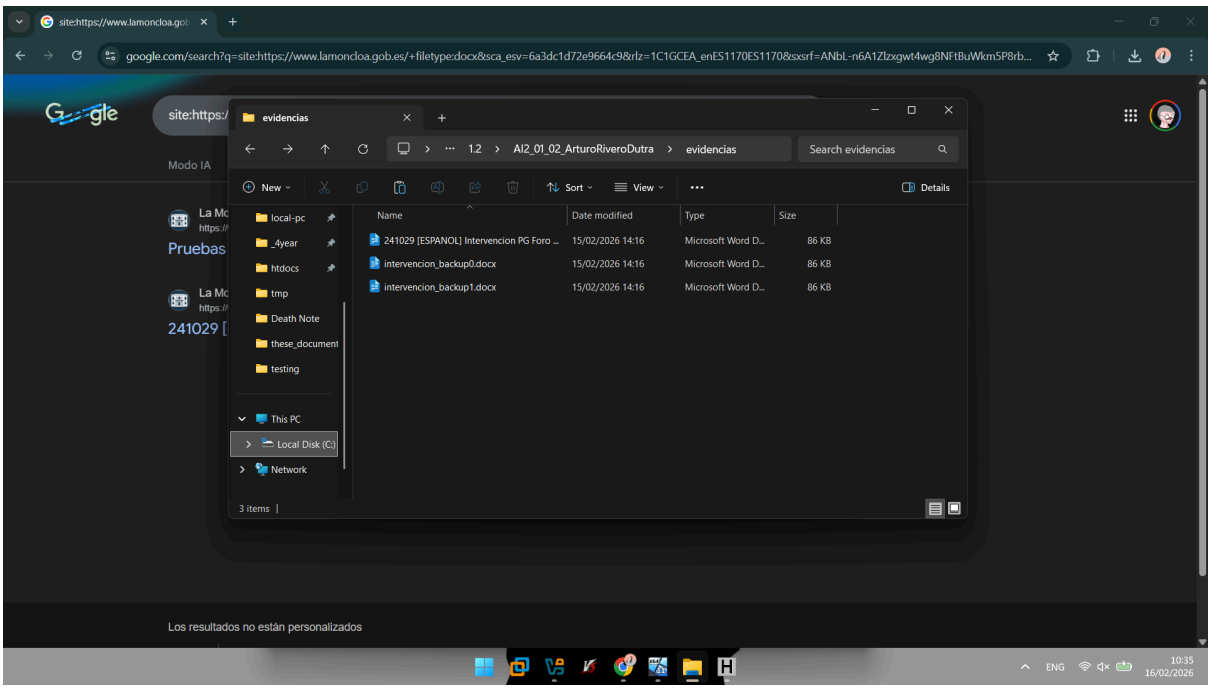


Obteniendo así el siguiente *hash*:

cdc28f47b163695d1bb107b210f2639018fa947de631526b58a32efe2e637fc5

Nota: Se tuvo que cambiar el nombre del fichero a *241029 [ESPANOL] Intervencion PG Foro Empresarial Espana-India.docx* ya que HashCalc no acepta rutas con caracteres especiales (a saber: *ñ, ó*). Sin embargo esta acción no compromete la integridad de los datos originales en absoluto puesto que lo único que se ha modificado es la entrada en el directorio local, los datos del fichero permanecieron intactos.

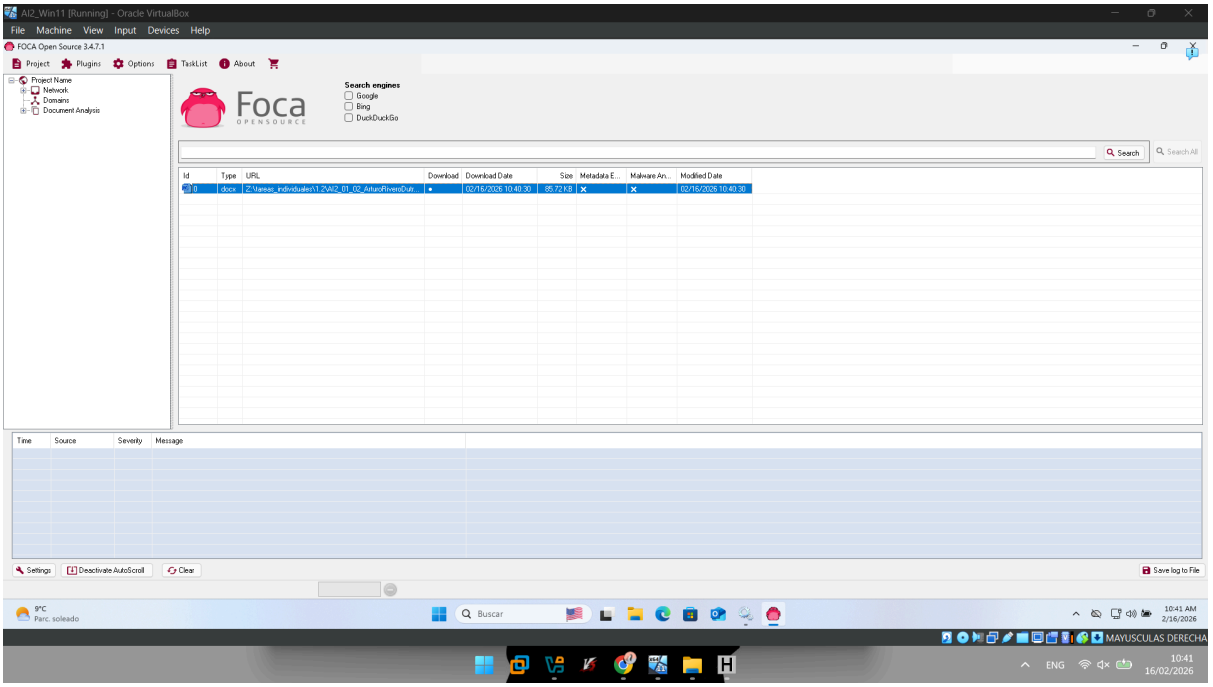
Después, con tal de asegurar la calidad en el análisis forense cumpliendo con las buenas prácticas descritas en la *ISO/IEC 27037*, se procedió a realizar una primera copia de la evidencia bajo el nombre de *intervencion_backup0.docx* la cual fue debidamente resguardada en un entorno aislado. Posteriormente se realizó una segunda copia nombrada *intervencion_backup1.docx* en la cual fue donde se procedió a continuación con el análisis.



Análisis de la Evidencia

El documento en cuestión se trata de una transcripción de la intervención del presidente del Gobierno, Pedro Sánchez, en la inauguración del Foro Empresarial España-India que tuvo lugar en Bombay, el 29 de octubre de 2024.

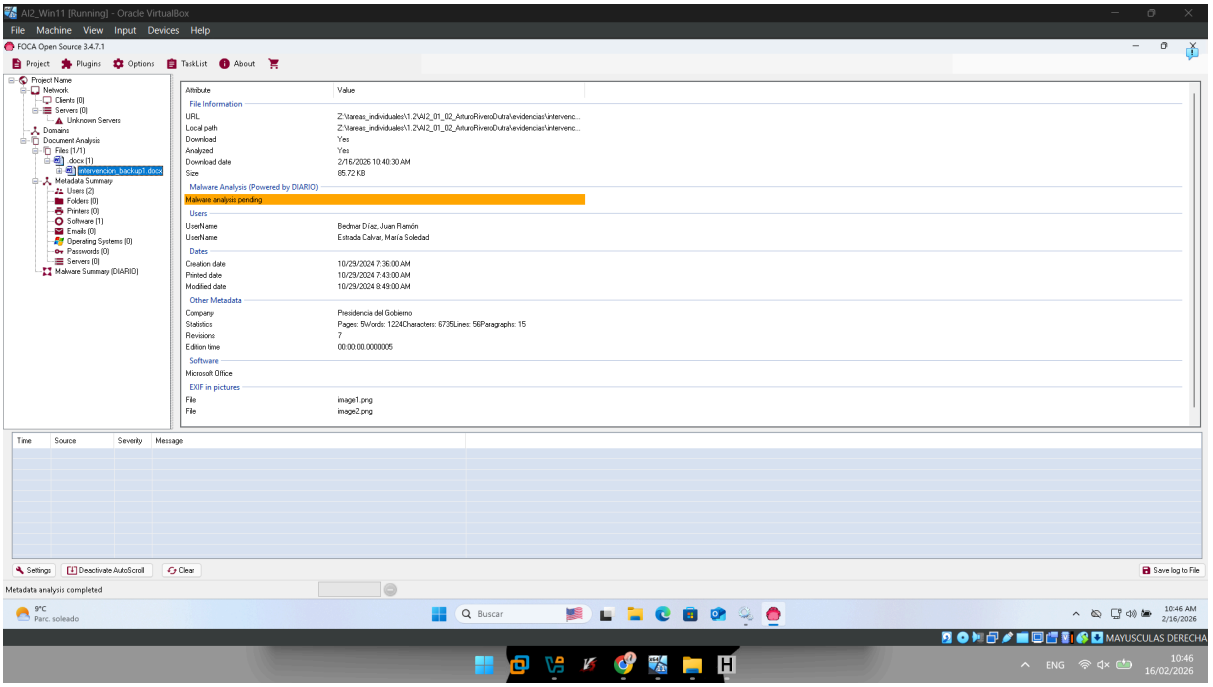
Se comenzó el análisis de los metadatos arrancando la herramienta FOCA en la máquina virtual e importando el documento en cuestión:



Acto seguido se realizó la extracción y análisis de los metadatos:

- *Click derecho sobre el fichero > Extract All Metadata*
- *Click derecho sobre el fichero > Analyze All Metadata*

Obteniendo así los metadatos que se muestran a continuación:



Así, si bien se examina, se logró obtener la siguiente información de especial relevancia:

- Nombres de Usuario:

    - Juan Ramón Bedmar Díaz
    - María Soledad Estrada Calvar

      Esta información permite la atribución directa que identifica las personas físicas que han interactuado con el documento.

- Organización:
    - Presidencia del Gobierno

      Confirma el origen institucional del documento, el cual es coherente con el mismo puesto que se trata de una transcripción de un discurso del presidente del gobierno.

- Historial de Fechas:
    - Creación: 10/29/2024 a las 7:36
    - Impresión: 10/29/2024 a las 7:43
    - Modificación: 10/29/2024 a las 8:49 AM

      En primera instancia se puede observar que la fecha es coherente con el nombre que poseía el fichero:

      241029 [ESPAÑOL] Intervención PG Foro Empresarial España-India.docx

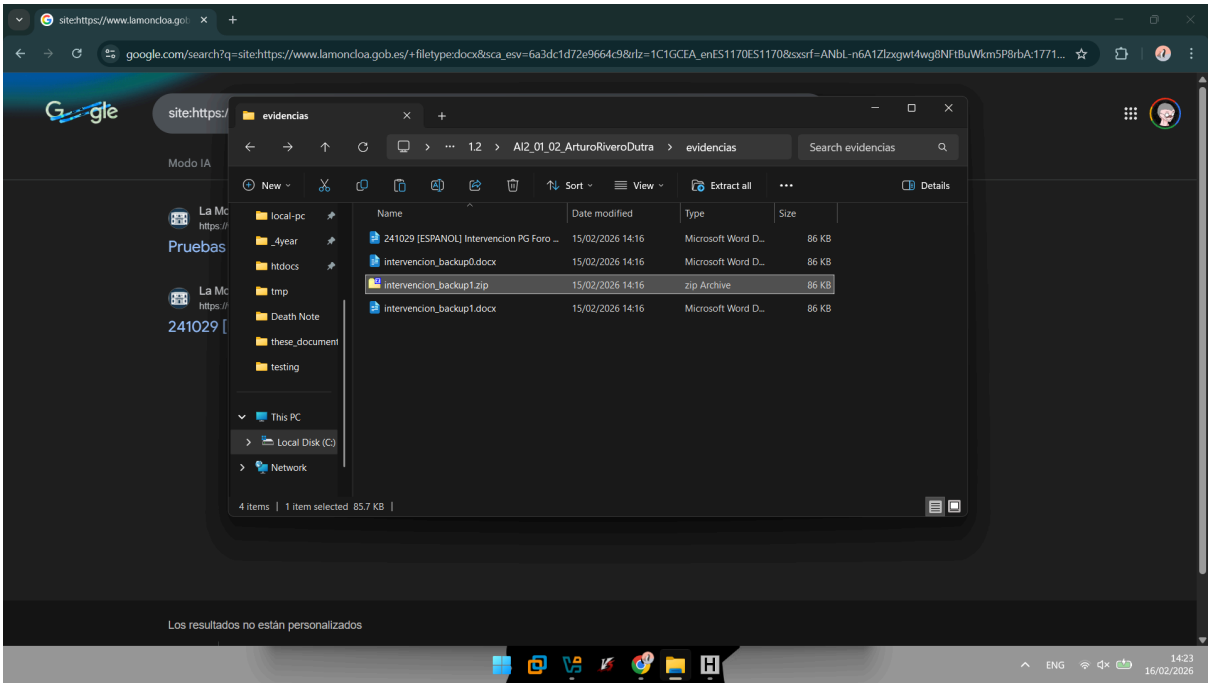
      Ya que éste comienza con el identificador *241029* muy seguramente indicando la fecha de emisión a 29 de octubre de 2024.

      Además, el hecho de que se haya impreso unos 7 minutos después de su creación sugiere que se trabajó sobre una plantilla o que se requería una copia física inmediata.

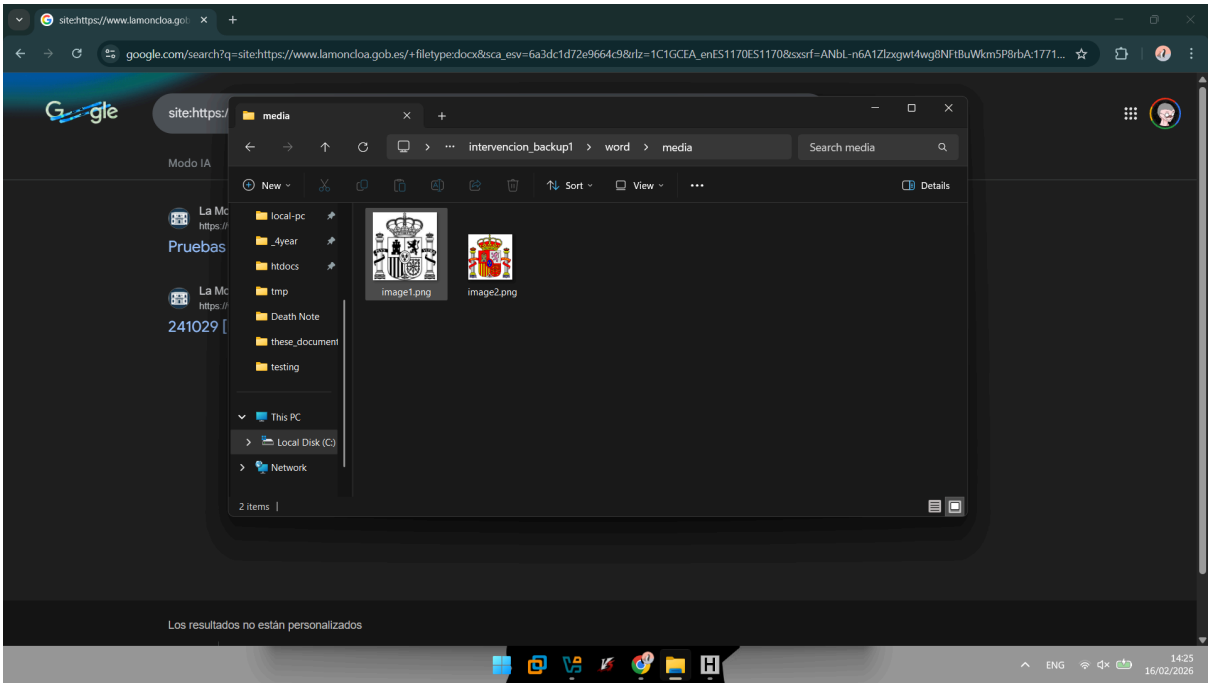
- Software:
    - Microsoft Office

      Esto nos indica el software utilizado lo cual nos da una idea de las herramientas que manejan en la organización.

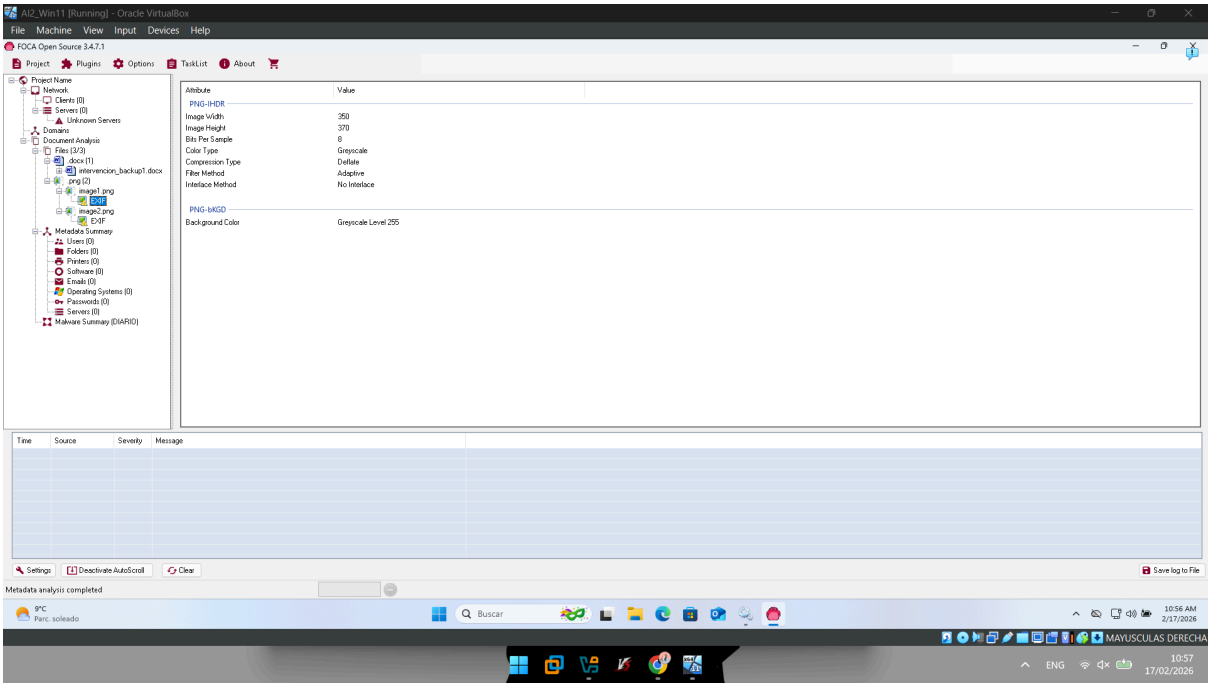
Además de lo anterior, también se puede observar que el documento cuenta con 2 imágenes las cuales son susceptibles de contener metadatos EXIF potencialmente relevantes. Para obtener esta información se creó una copia del documento pero cambiándole la extensión a *.zip*.

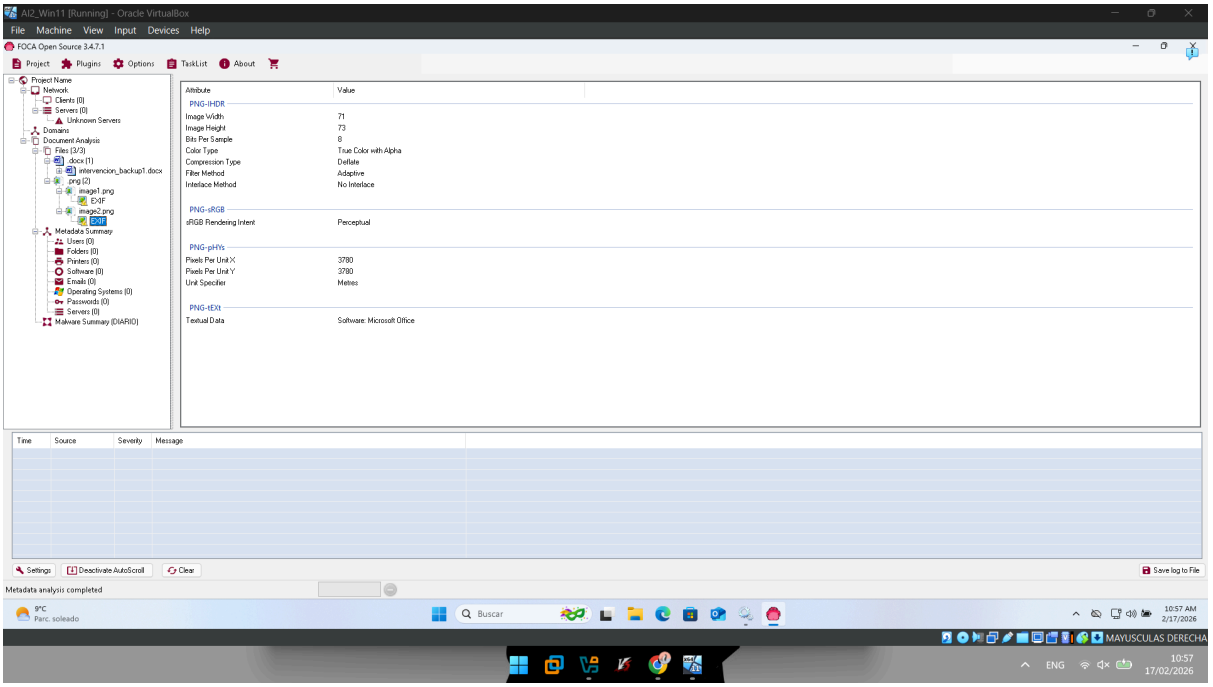


De esta manera se pudo extraer las imágenes correspondientes dentro del directorio */word/media*:



Acto seguido se procedió a analizar los metadatos EXIF de ambas imágenes dentro de la misma herramienta FOCA:

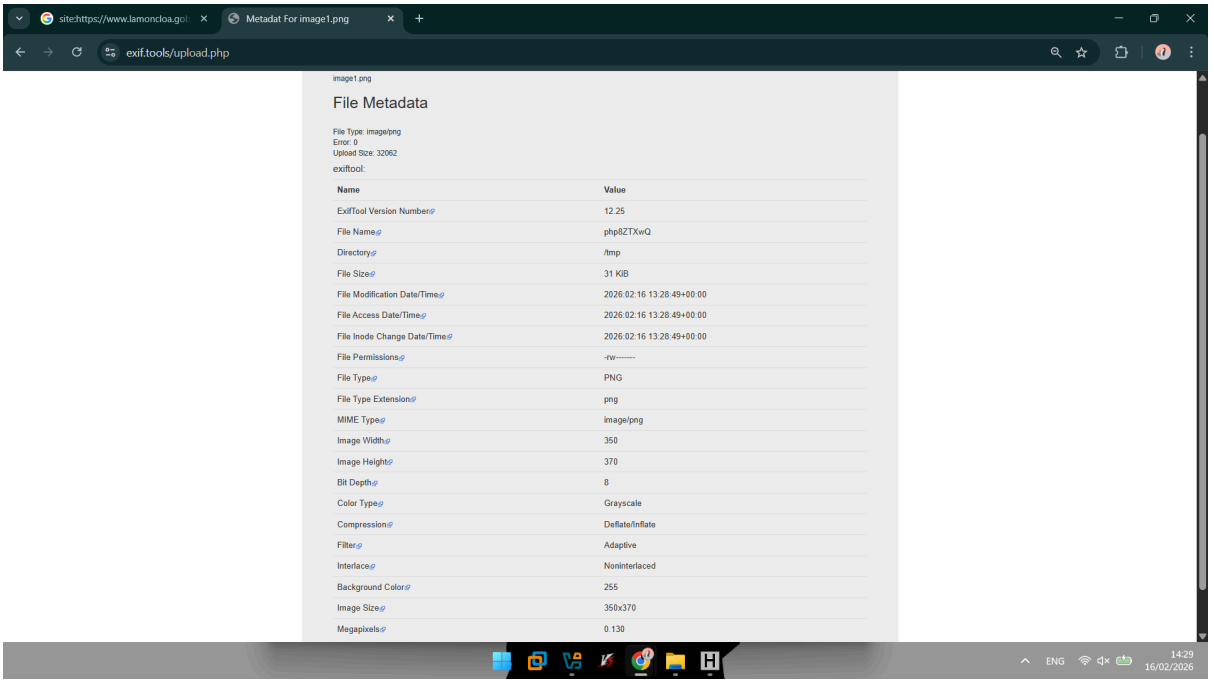




Aunque no se obtuvo información de gran relevancia más allá del *Software: Microsoft Office* en la segunda imagen.

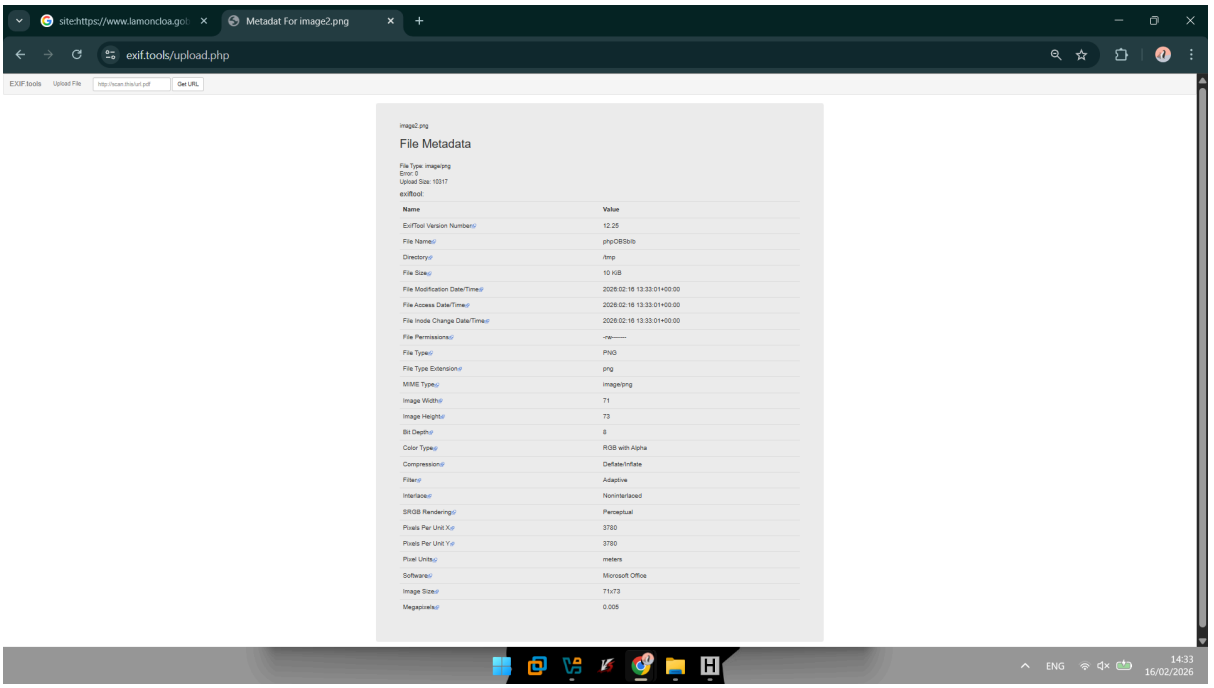
Por tanto, se optó por utilizar una herramienta más especializada en analizar los metadatos EXIF de las imágenes, exif.tools, para contrastar los resultados con los anteriores y potencialmente encontrar más información relevante:

1. *image1.png*:



Aunque para este caso, no existía información de especial relevancia en los metadatos de la imagen más allá de los datos técnicos de la misma.

2. *image2.png*:



Aquí, el único dato de cierta relevancia es el de *Software: Microsoft Office*, el cual refuerza la coherencia con lo encontrado anteriormente.

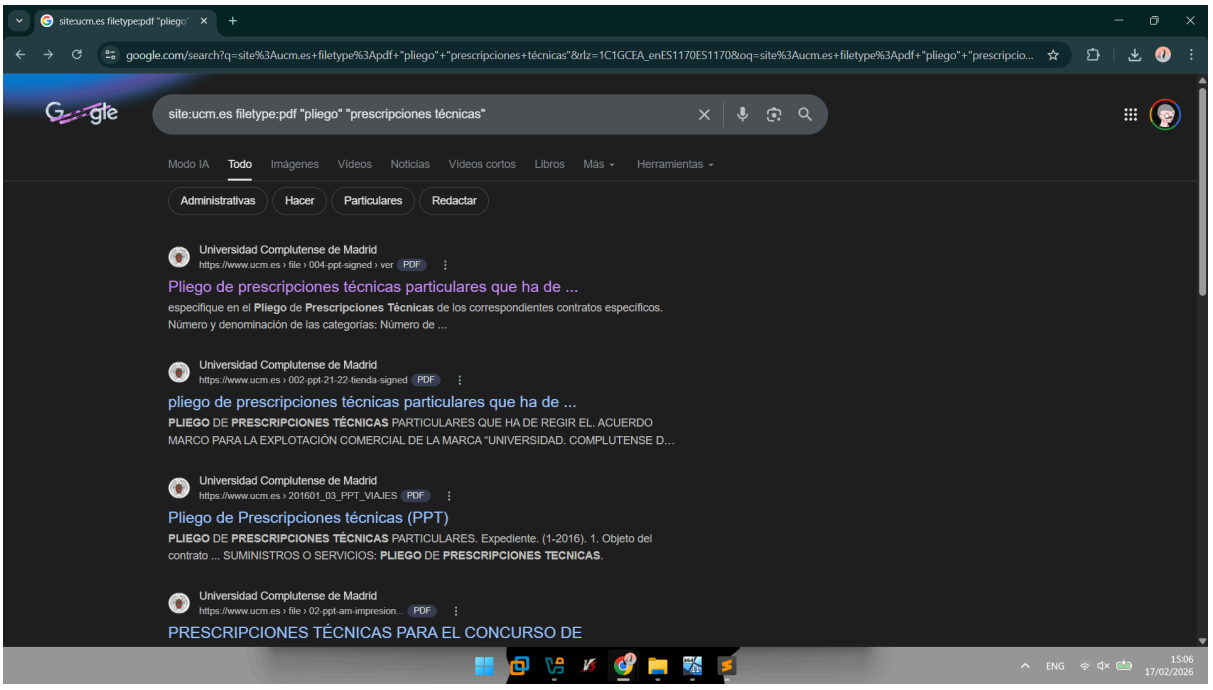
Así, tras la verificación cruzada de los metadatos EXIF con dos herramientas diferentes, se pudo concluir con buena seguridad que no existían metadatos potencialmente omitidos.

2. Documento “.pdf”

Adquisición de la Evidencia

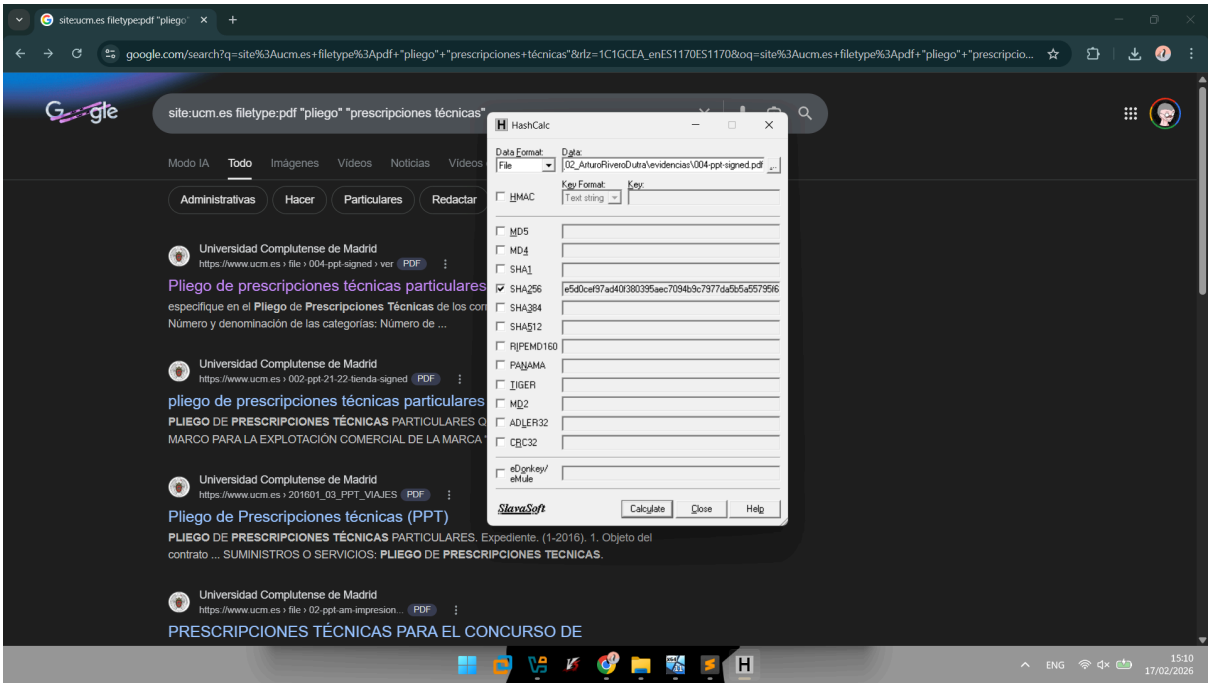
Para la obtención de esta evidencia se tenía como objetivo un archivo *.pdf*, concretamente algún Pliego de Prescripciones Técnicas (PPT), el cual es un documento que con frecuencia presenta buena cantidad de metadatos. Se optó por la utilización de Google Dorks especificando la web oficial de Universidad Complutense de Madrid como objetivo, el tipo de fichero *.pdf*, y la inclusión estricta de las palabras referentes al documento descrito de acuerdo a la siguiente búsqueda:

> *site:ucm.es filetype:pdf "pliego" "prescripciones técnicas"*



Se seleccionó el primer resultado y se procedió a descargarlo.

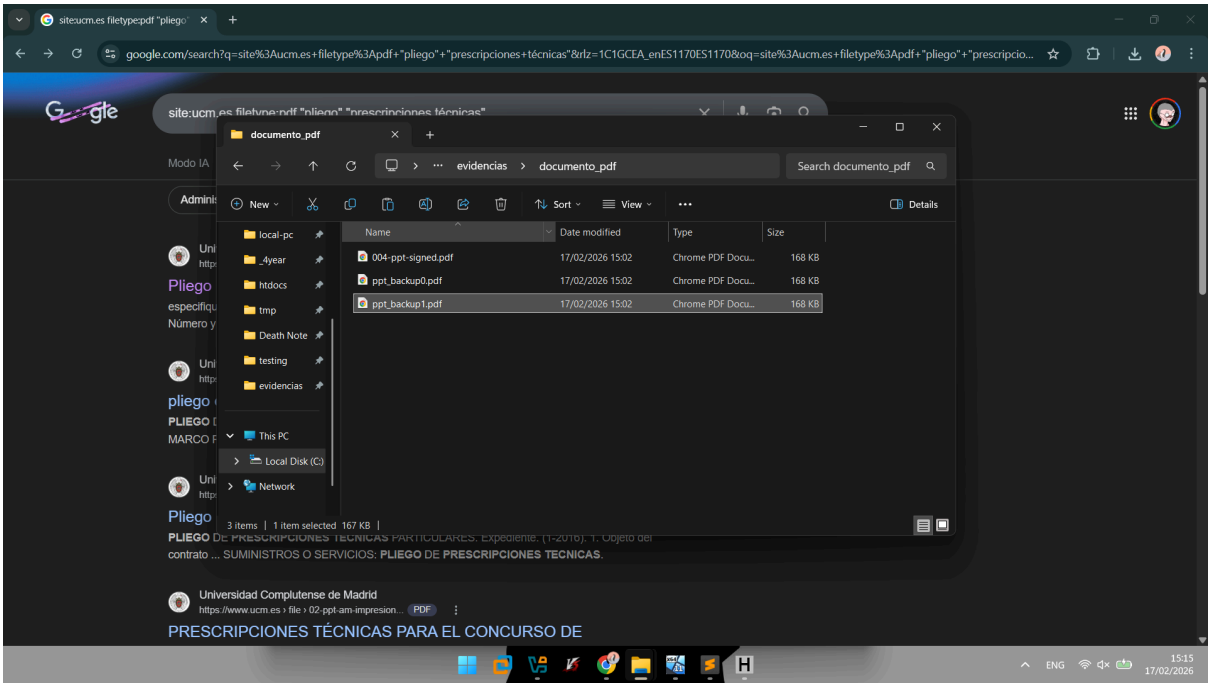
Una vez obtenido el fichero *004-ppt-signed.pdf*, la primera acción tomada fue calcular su *hash SHA-256* para capturar la integridad de la evidencia original. Para ello, se empleó el programa HashCalc:



Obteniendo así el siguiente *hash*:

> *5262560777b1a26bbe5d0cef97ad40f380395aec7094b9c7977da5b5a55795f6*

Después, con tal de asegurar la calidad en el análisis forense cumpliendo con las buenas prácticas descritas en la *ISO/IEC 27037*, se procedió a realizar una primera copia de la evidencia bajo el nombre de *ppt_backup0.pdf* la cual fue debidamente resguardada en un entorno aislado. Posteriormente se realizó una segunda copia nombrada *ppt_backup1.pdf* en la cual fue donde se procedió a continuación con el análisis.



Análisis de la Evidencia

Se empezó el análisis subiendo el documento a la plataforma Metadata2Go para extraer sus metadatos, entre los cuales se encontraron como más relevantes los siguientes:

1. Software utilizado para su creación

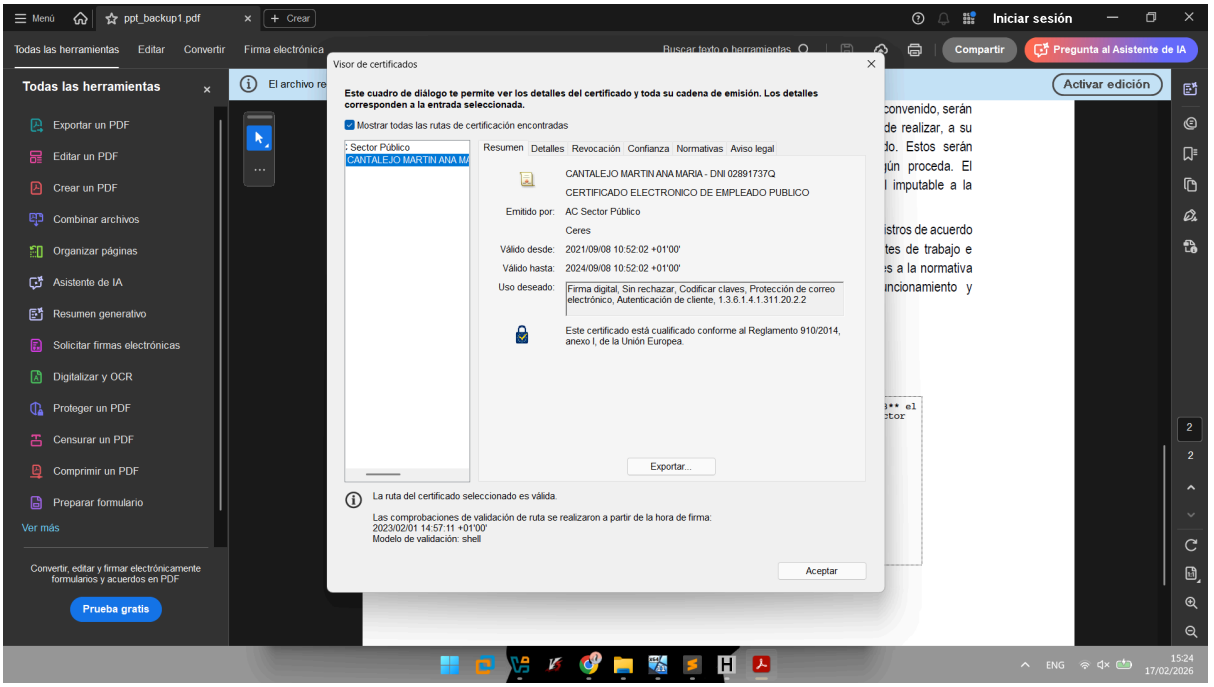
creator_tool	Microsoft® Word 2019

   Microsoft Word 2019. Esto nos indica el software utilizado lo cual nos da una idea de las herramientas que manejan en la organización.

2. Creador y Autor

creator	MARGARITA BARRIO MOZO
author	MARGARITA BARRIO MOZO

   Margarita Barrio Mozo. Esto es interesante porque el documento se encuentra firmado por otra persona, Ana María Cantalejo Martín, como se puede comprobar en Adobe Acrobat:



Lo cual indica que la persona que firmó el documento no fue la encargada de generarlo.

Además, se puede ver que el Software utilizado para firmar fue @firma, el estándar en administraciones públicas españolas:

history_parameters	Firmado por el Cliente @firma
history_software_agent	Cliente @firma

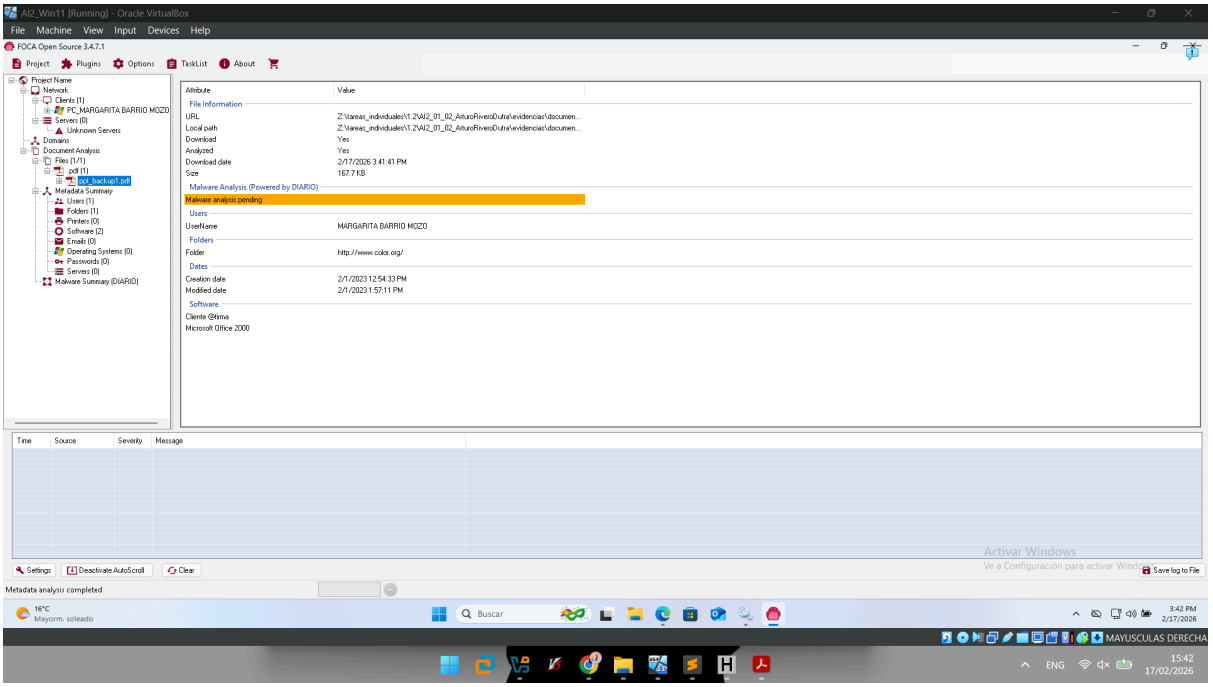
3. Fechas y horas de modificación y creación

create_date	2023:02:01 13:54:33+01:00
modify_date	2023:02:01 14:57:11+01:00

Coherentes con el contenido del documento y la fecha en la que se firmó digitalmente (el mismo día).

Nota: se han omitido en el presente informe los demás metadatos proporcionados por la herramienta Metadata2Go puesto que correspondían mayoritariamente a información técnica sobre la infraestructura gráfica del PDF que no fueron de especial relevancia para el presente análisis.

Adicionalmente, para complementar el análisis, se decidió contrastar los resultados proporcionados por Metadata2Go con aquellos arrojados por FOCA:



De los cuales la única discrepancia remarcable es la versión del Software utilizado que indica FOCA: Microsoft Office 2000. Esta versión es bastante antigua y por tanto está repleta de vulnerabilidades conocidas. Si fuera cierto que se utiliza esta versión en lugar de la de 2019 indicada por Metadata2Go esto supondría un riesgo gravísimo para la organización.

Por tanto, aunque es poco probable que se utilice la versión antigua por el riesgo descrito, no es descartable, de modo que no se pudo concluir con exactitud qué versión del Software se utilizó realmente.

3. Imagen “.jpg”

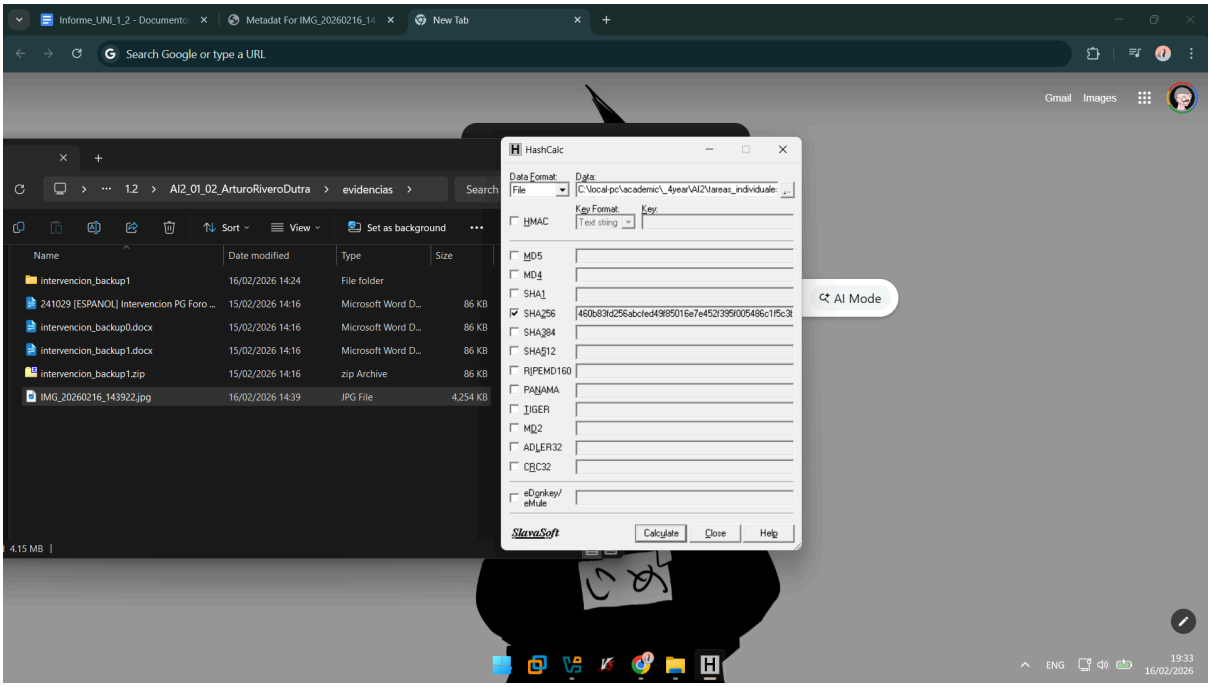
Generación de la Evidencia

Esta evidencia se trata de una imagen *.jpg* la cual fue generada mediante la aplicación de cámara del dispositivo móvil mencionado en el análisis del laboratorio forense.

Adquisición de la Evidencia

Tras la generación, se transfirió la imagen a la máquina designada para su análisis descrita también en la misma sección. Para conservar la integridad del archivo original no se hizo uso de ninguna plataforma de mensajería estándar ya que éstas suelen “limpiar” los metadatos o comprimir la información, por lo que se transfirió el archivo directamente mediante un cable USB desde el dispositivo móvil hasta la máquina del análisis.

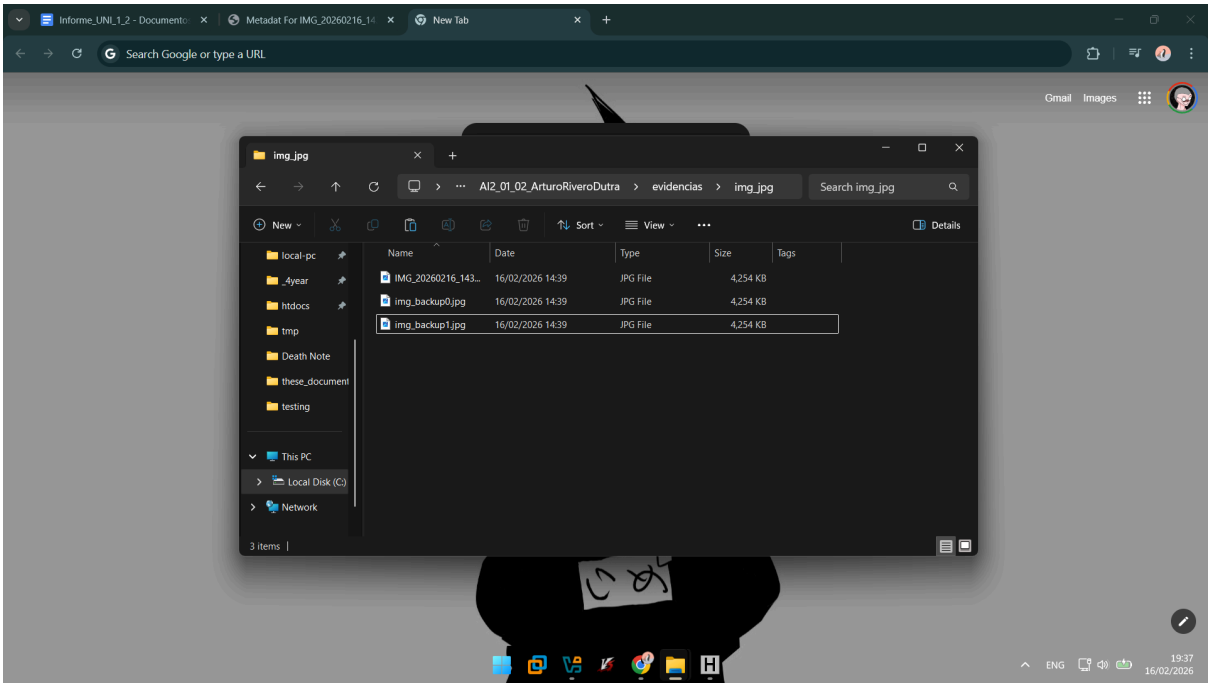
Una vez en la máquina, la primera acción tomada fue calcular el *hash SHA-256* de la imagen para capturar la integridad de la evidencia original. Para ello, se empleó el programa HashCalc:



Obteniendo así el siguiente *hash*:

> *460b83fd256abcfed49f85016e7e452f395f005486c1f5c3b4bb2a607a031edc*

Después, con tal de asegurar la calidad en el análisis forense cumpliendo con las buenas prácticas descritas en la ISO/IEC 27037, se procedió a realizar una primera copia de la evidencia bajo el nombre de *img_backup0.jpg* la cual fue debidamente resguardada en un entorno aislado. Posteriormente se realizó una segunda copia nombrada *img_backup1.jpg* en la cual fue donde se procedió a continuación con el análisis.



Análisis de la Evidencia

Se comenzó el análisis de esta evidencia subiendo la imagen a la plataforma exif.tools con tal de extraer sus metadatos EXIF, obteniendo así la siguiente información de especial relevancia:

1. Modelo y marca del dispositivo móvil utilizado para sacar la foto

Camera Model Name	AC2001
Make	OnePlus

Con esto se supo que se trataba de un móvil *OnePlus AC2001*, lo cual podría llegar a reforzar la posible evidencia física que pudiéramos encontrar o ayudar en el perfilado financiero de su dueño con el fin de identificarlo.

2. La fecha y hora en la que se tomó la foto

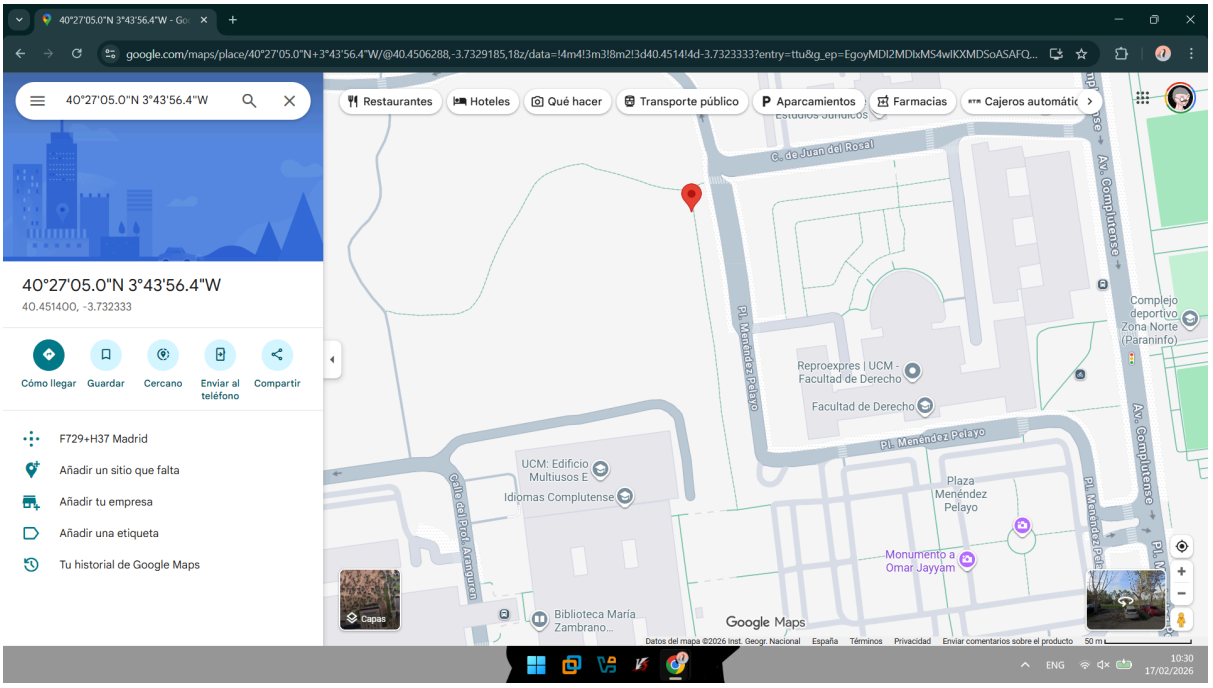
Date/Time Original	2026:02:16 14:39:22

16 de febrero de 2026 a las 14:39:22. Esta información fue de crucial relevancia para establecer una línea cronológica con los eventos sucedidos que se estaban investigando.

3. La ubicación proporcionada por el GPS

GPS Altitude	704.6 m Above Sea Level
GPS Date/Time	2026:02:16 13:39:22Z
GPS Latitude	40° 27' 5.04" N
GPS Longitude	3° 43' 56.40" W
Focal Length	4.7 mm
GPS Position	40° 27' 5.04" N, 3° 43' 56.40" W

Esta información también fue de vital importancia puesto que nos indicó el lugar aproximado (con un ligero margen de error) donde se tomó la foto. Con ella se pudo mapear las coordenadas con una ubicación real introduciéndolas en Google Maps:



Con esta información, sumada al propio contenido de la imagen, que parece ser una biblioteca, se pudo reducir el espacio de búsqueda a bibliotecas cercanas a la zona de las coordenadas (por Ciudad Universitaria). Esto dio lugar a una investigación in situ de la que se pudo concluir que la ubicación exacta donde se había tomado la foto era en la sala de filología de la biblioteca María Zambrano.

Nota: se han omitido en el presente informe los demás metadatos proporcionados por la herramienta exif.tools puesto que correspondían mayoritariamente a información técnica sobre la cámara que no fueron de especial relevancia para el presente análisis. Sin embargo, en otro caso con otras condiciones, podrían llegar a ser útiles por ejemplo para identificar el modelo del dispositivo móvil por las características técnicas de su cámara si esta información no estuviera disponible.

Descripción de las Evidencias Capturadas

Relación detallada del elemento capturado:

Nombre Evidencia	Hash SHA-256	Fecha Adquisición	Analista	Fecha Análisis
241029 [ESPAÑOL] Intervención PG Foro Empresarial España-India .docx	cdc28f47b163695d1bb107b210f2639018fa947de631526b58a32efe2e637fc5	16/02/2026	Arturo Rivero	16-17/02/2026
004-ppt-signed.pdf	5262560777b1a26bbe5d0cef97ad40f380395aec7094b9c7977da5b5a55795f6	17/02/2026	Arturo Rivero	17/02/2026
IMG_20260216_143922.jpg	460b83fd256abcfed49f85016e7e452f395f005486c1f5c3b4bb2a607a031edc	16/02/2026	Arturo Rivero	17/02/2026

Nota: Los análisis se realizaron sobre las respectivas copias de trabajo de cada evidencia.

Herramientas Utilizadas

En esta sección se recopila el glosario de las herramientas utilizadas junto a una breve descripción de su funcionalidad:

- HashCalc: Utilidad con interfaz gráfica de usuario que permite computar el *hash* para una entrada sea esta una cadena de texto o un archivo con una selección de algoritmos disponibles.
- FOCA: Herramienta con interfaz gráfica de usuario enfocada a la extracción y análisis de una variedad de metadatos de grandes volúmenes de ficheros.

- Google Dorks: Conjunto de operadores integrados en el buscador de Google que permiten filtrar los resultados y obtener aquellos cuyas características más nos interesen.
- exif.tools: Plataforma web que corre por detrás la herramienta exiftool la cual extrae todos los metadatos EXIF de un fichero apropiado.
- Metadata2Go: Herramienta online que extrae una gran variedad de metadatos de una gran selección de formatos de fichero.
- Adobe Acrobat: Software de manipulación de documentos PDF muy completo.
- Google Maps: Plataforma online para consultar mapas del mundo por excelencia.

Conclusiones

Como se ha demostrado en el análisis forense descrito en el presente informe, los ficheros poseen una serie de metadatos, además de los datos propios del fichero, que a menudo contienen información relevante para la investigación y que pueden ser extraídos y analizados con herramientas como las descritas anteriormente. Entre esta información relevante se pueden destacar datos como los *timestamps*, el autor y creador del fichero, el *software* empleado, el modelo del dispositivo usado, la organización y empresa que emitió el fichero, coordenadas GPS y la presencia de firmas digitales. Toda esta información es de especial utilidad para establecer una línea cronológica con los sucesos, identificar a los involucrados y conocer las herramientas que se utilizan en una organización.

Por último, es importante mencionar que la información que pueden proporcionar los metadatos, aunque útil en muchas ocasiones, no es necesariamente concluyente ya que puede ser alterada con fines ofuscantes disponiendo de las herramientas adecuadas.

Firmado digitalmente por:

Arturo Rivero Dutra,
a 17 de febrero de 2026