

Forensic Case 1 - Caso GEO

Caso GEO

Un archivo de imagen se ha encontrado en un dispositivo digital secuestrado durante una investigación de delitos ciberneticos. La fotografía puede ser crucial para entender el contexto de un incidente. Tu tarea es determinar dónde y cuándo se tomó esta fotografía.

¿Dónde fue tomada la fotografía?

FORMATO: CTF{NAME_ADDRESS}

Ejemplo:

30° 63' 43.80" N, 21° 37' 10.02" W > CTF{30_63_43_80_N_21_37_10_02_W}

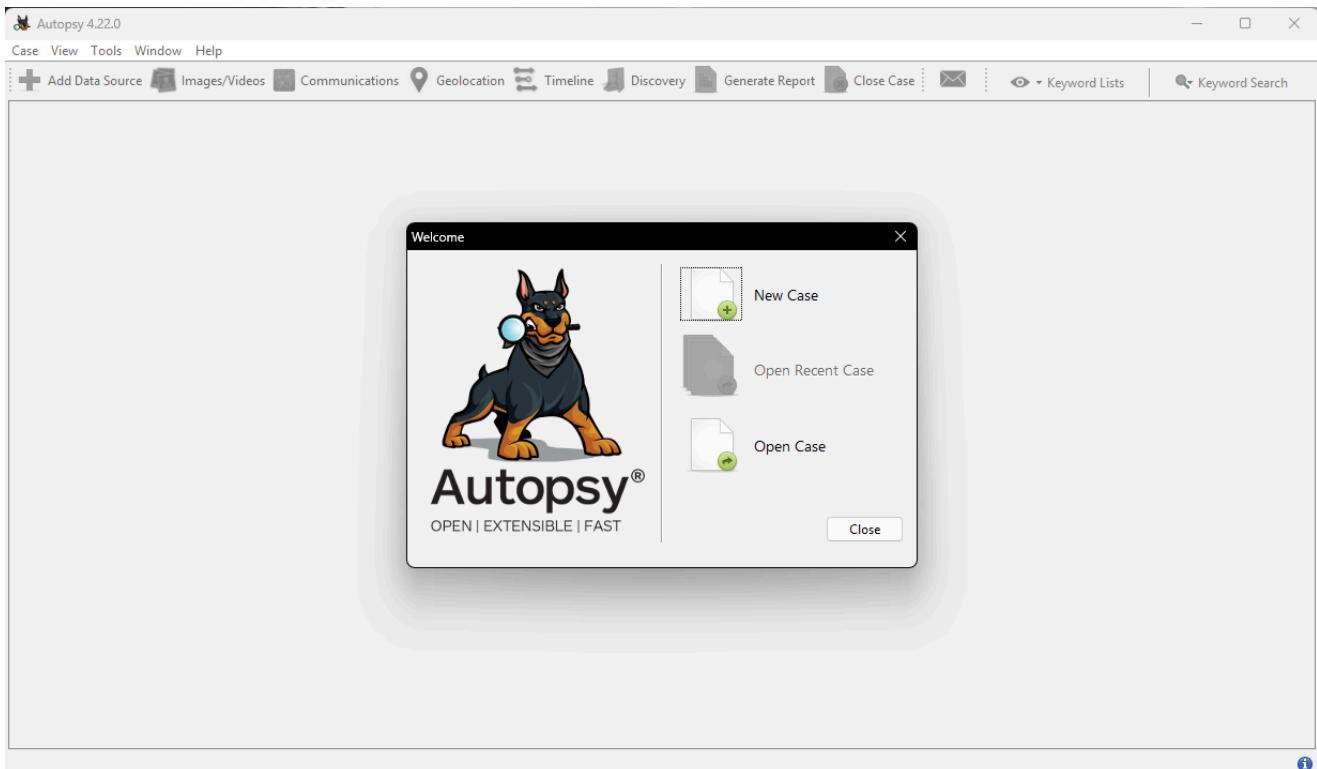
Can you find the password? Enter the password as flag in the following form:
CTF{passwordhere}

Procederemos a Descargar el archivo y guardarlo en una carpeta donde podamos localizarlo de manera ordenada, haciendo *hovering* vemos que se trata de una imagen .jpg

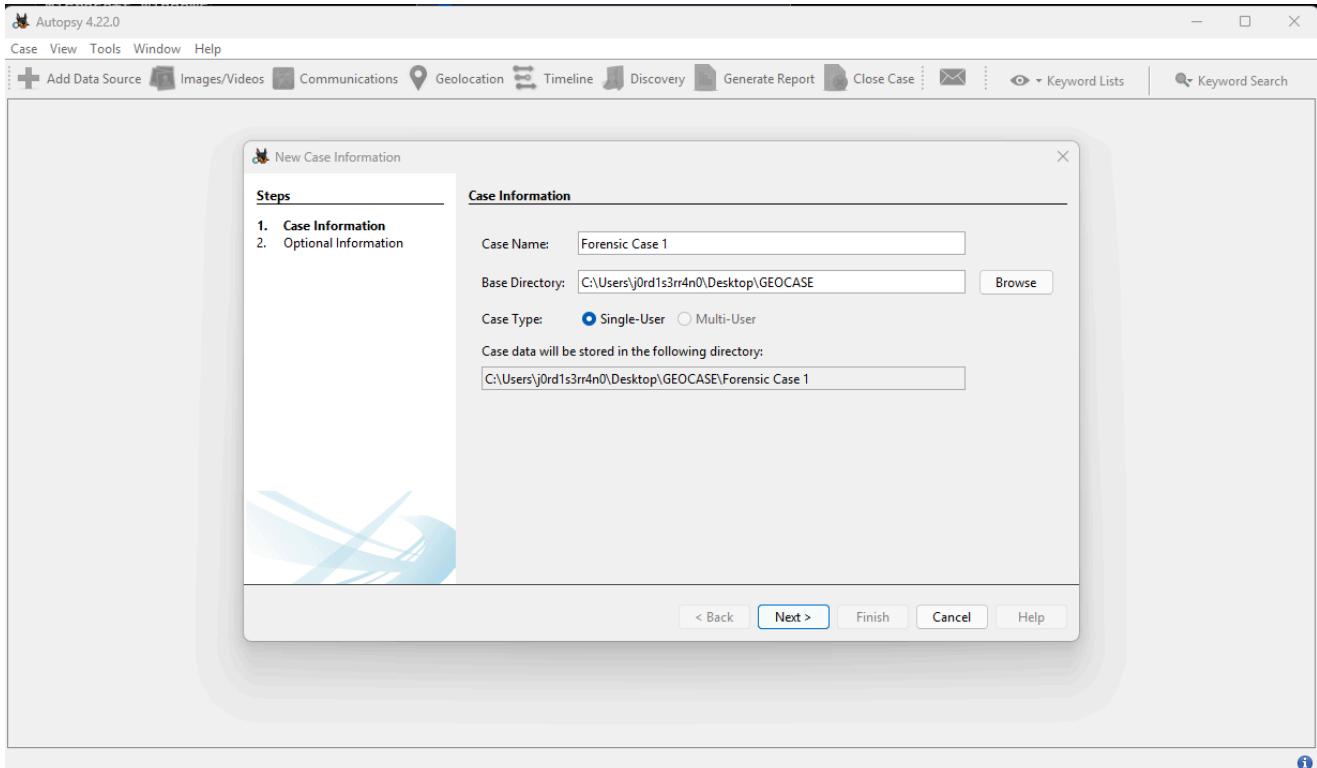


Download

raw.githubusercontent.com/j0rd1s3rr4n0/ForensTech-Challenges/refs/heads/.../picture.jpg



A continuación abrimos Autopsy: esta plataforma forense gráfica integra extracción de metadatos EXIF, análisis hexadecimal y mapeo geolocalizado en un único entorno visual. Aunque podríamos optar por `exiftool` para una extracción rápida de metadatos en línea de comandos, Autopsy agiliza el flujo de trabajo al combinar estas funciones con un visor de contenido y módulos de ingestión configurables.



Procederemos a Generar el espacio de trabajo donde vamos a realizar el análisis del archivo.

Formulario de creación de caso: definimos `Forensic Case 1` y establecemos el directorio raíz.

New Case Information X

Steps	Optional Information
1. Case Information 2. Optional Information	Case Number: <input type="text"/> Examiner Name: <input type="text"/> Phone: <input type="text"/> Email: <input type="text"/> Notes: <input type="text"/> Organization Organization analysis is being done for: <input type="text"/> Not Specified <input type="button" value="Manage Organizations"/>

< Back

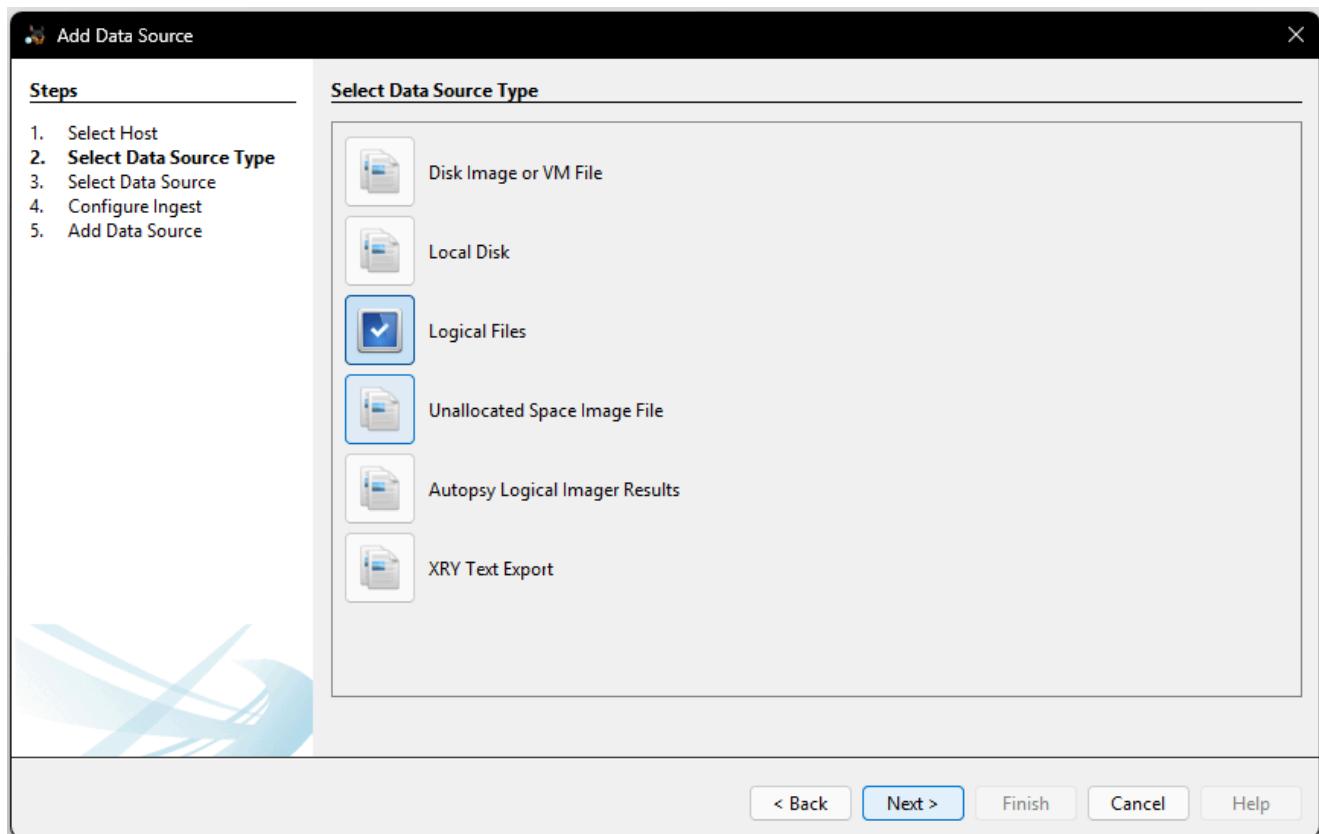
Nota: en este análisis omitimos intencionadamente los campos opcionales de Autopsy como número de caso, nombre del examinador, teléfono, correo electrónico, notas adicionales y organización, porque no se generará un reporte formal.

Add Data Source X

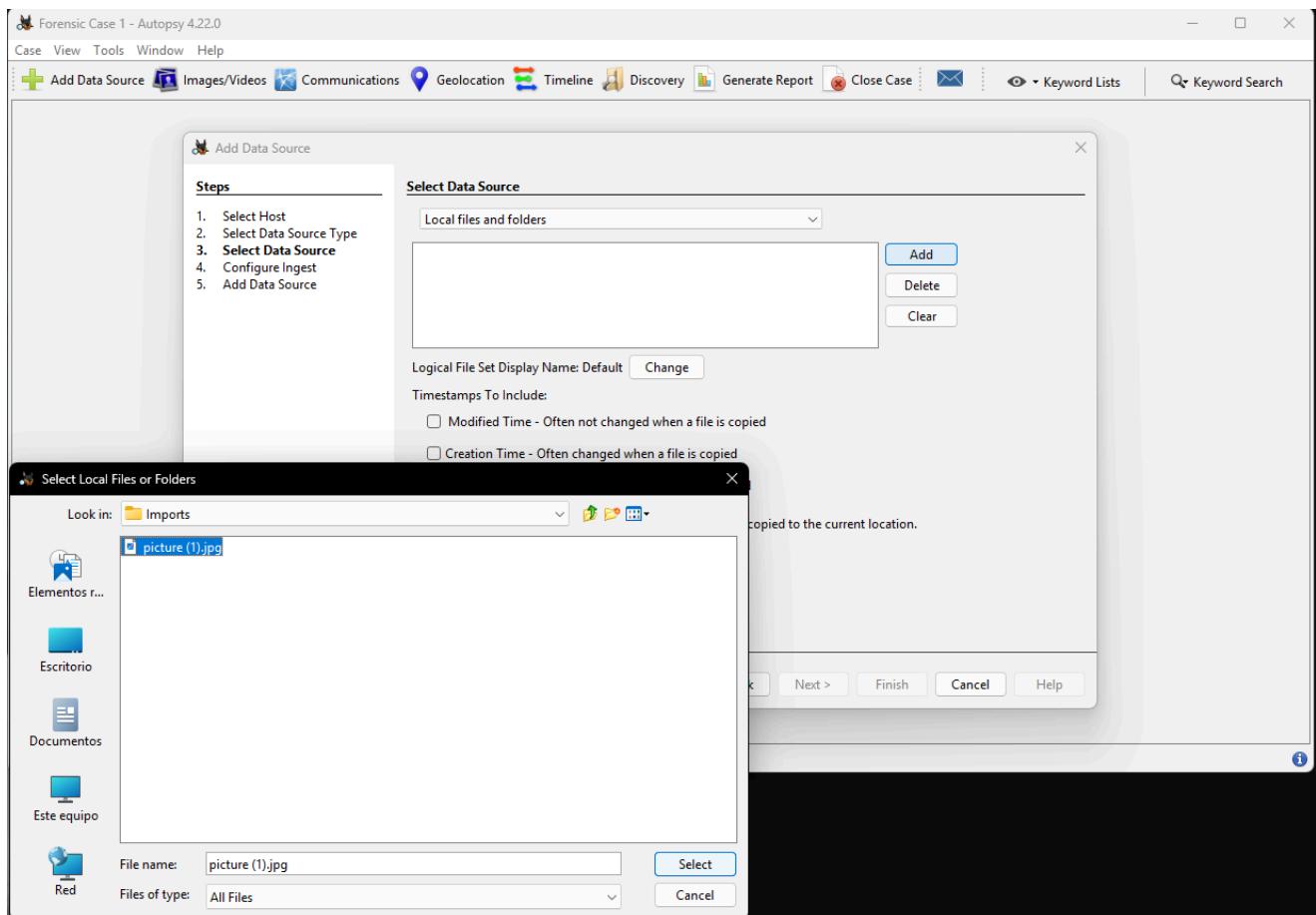
Steps	Select Host
1. Select Host 2. Select Data Source Type 3. Select Data Source 4. Configure Ingest 5. Add Data Source	Select Host Hosts are used to organize data sources and other data. <input checked="" type="radio"/> Generate new host name based on data source name <input type="radio"/> Specify new host name <input type="text"/> <input type="radio"/> Use existing host <input type="text"/> < Back <input type="button" value="Next >"/> <input type="button" value="Finish"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>

Opción Generate new host name based on data source name : genera un alias único a partir del nombre del archivo. Esto facilita el mapeo de resultados cuando se importan múltiples fuentes con nombres similares. Al automatizar la generación del nombre de host, evitamos colisiones manuales y garantizamos consistencia en los registros. Cada artefacto

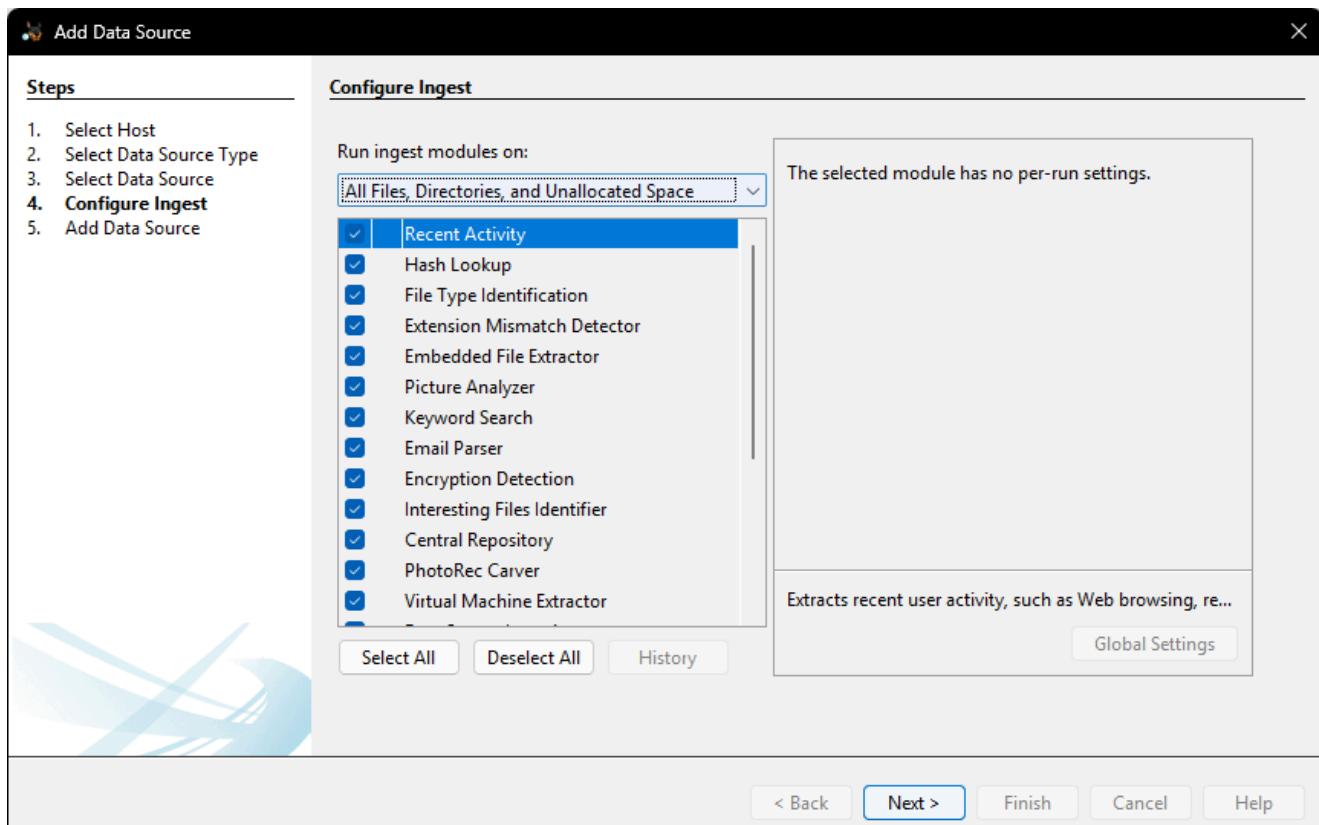
importado se asocia inequívocamente con su fuente original, lo que mejora la trazabilidad, simplifica la auditoría y reduce errores humanos en entornos multi-caso.



En este menú de ingestión deseleccionamos otros módulos de análisis de disco completo y dejamos marcada únicamente la opción **Logical Files**. De esta forma, Autopsy se enfocará exclusivamente en los archivos lógicos dentro de la imagen importada —en nuestro caso, picture.jpg— lo que reduce el tiempo de procesamiento y evita cargar artefactos innecesarios como registros de sistema o particiones completas.



Ventana de "**Add Data Source**": al hacer clic en **Add**, vinculamos el archivo físico al caso forense. Seleccionar **picture.jpg** aquí es crucial pues define el alcance de los módulos de ingestión posteriores. Esta acción asegura que Autopsy indexe y procese exclusivamente los datos de interés, evitando la inclusión involuntaria de archivos no relacionados.

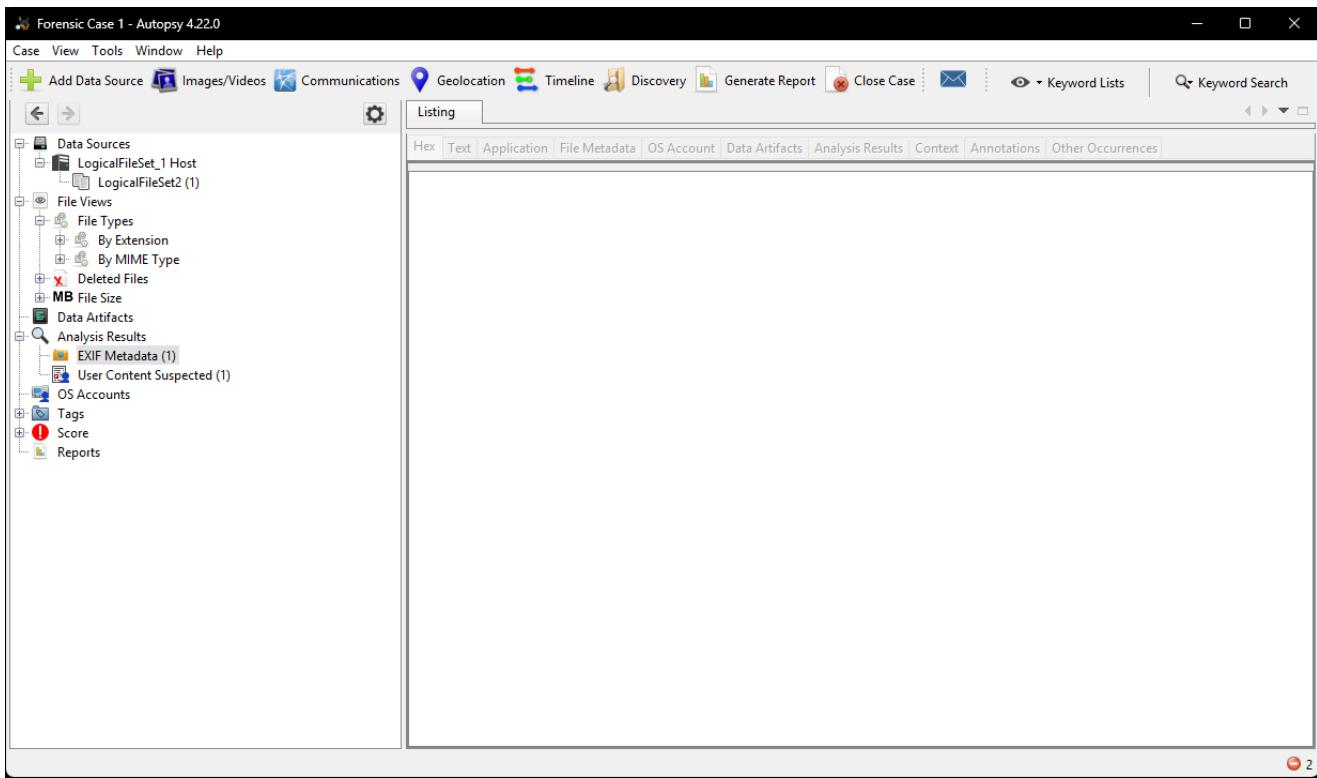


Opciones de ingestión configuradas al 100%: dejamos todas las casillas marcadas. Mantener todos los módulos activos garantiza que no perdamos ningún artefacto forense

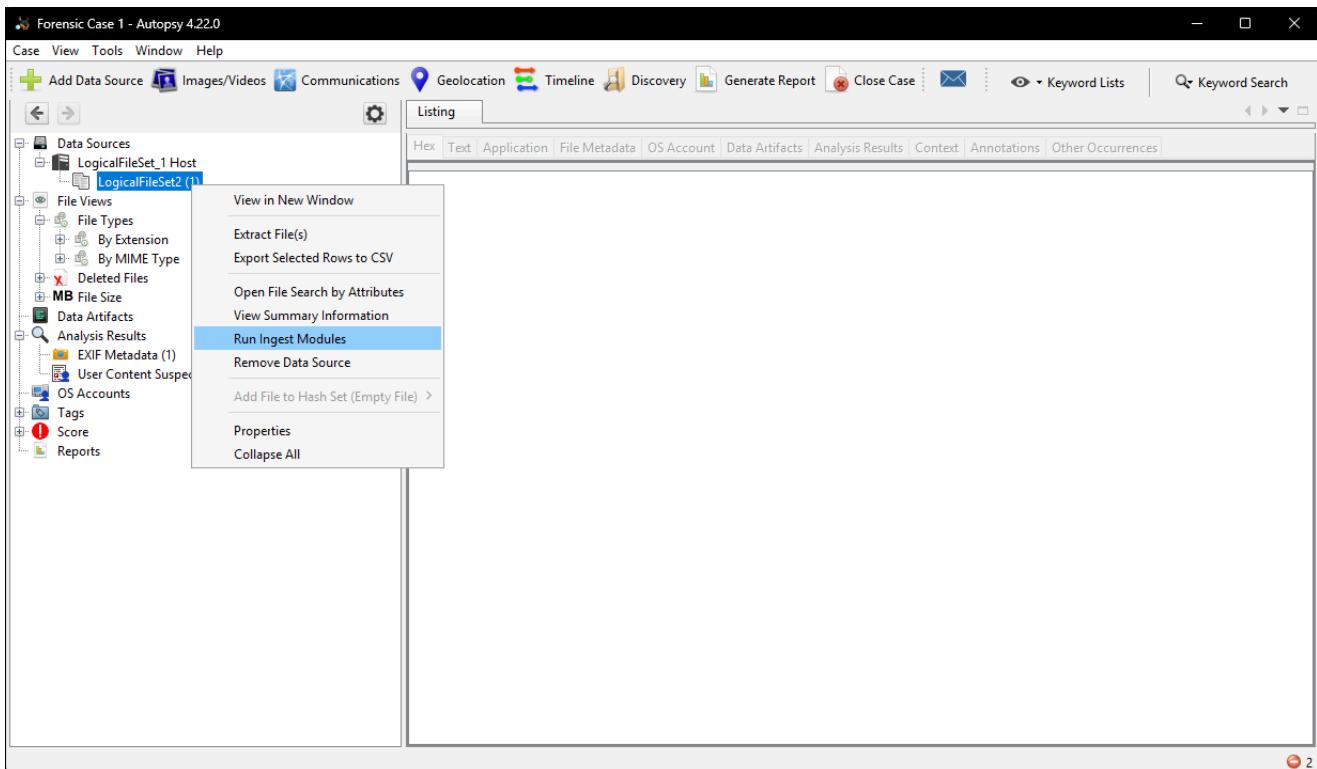
relevante, aunque incrementa el tiempo de procesamiento. En entornos de alto volumen se pueden desactivar módulos secundarios para optimizar rendimiento, pero en un caso puntual como este, la exhaustividad es prioritaria.

The screenshot shows a software window titled "Add Data Source". On the left, there's a sidebar with a blue icon and the title "Add Data Source". Below it is a list of steps: 1. Select Host, 2. Select Data Source Type, 3. Select Data Source, 4. Configure Ingest, and 5. Add Data Source. Step 5 is highlighted with a blue background. The main panel is titled "Add Data Source" and contains the message: "Data source has been added to the local database. Files are being analyzed." At the bottom right, there are buttons for "< Back", "Next >", "Finish" (which is highlighted in blue), "Cancel", and "Help".

Confirmación y lanzamiento del proceso haciendo clic en **Finish**: este paso envía todas las configuraciones de ingestión al motor de Autopsy, iniciando el análisis automático. Autopsy comenzará a escanear el archivo, ejecutar cada módulo seleccionado y almacenar los resultados en la base de datos del caso. Es crucial no interrumpir esta fase para garantizar que todos los artefactos se indexen correctamente.



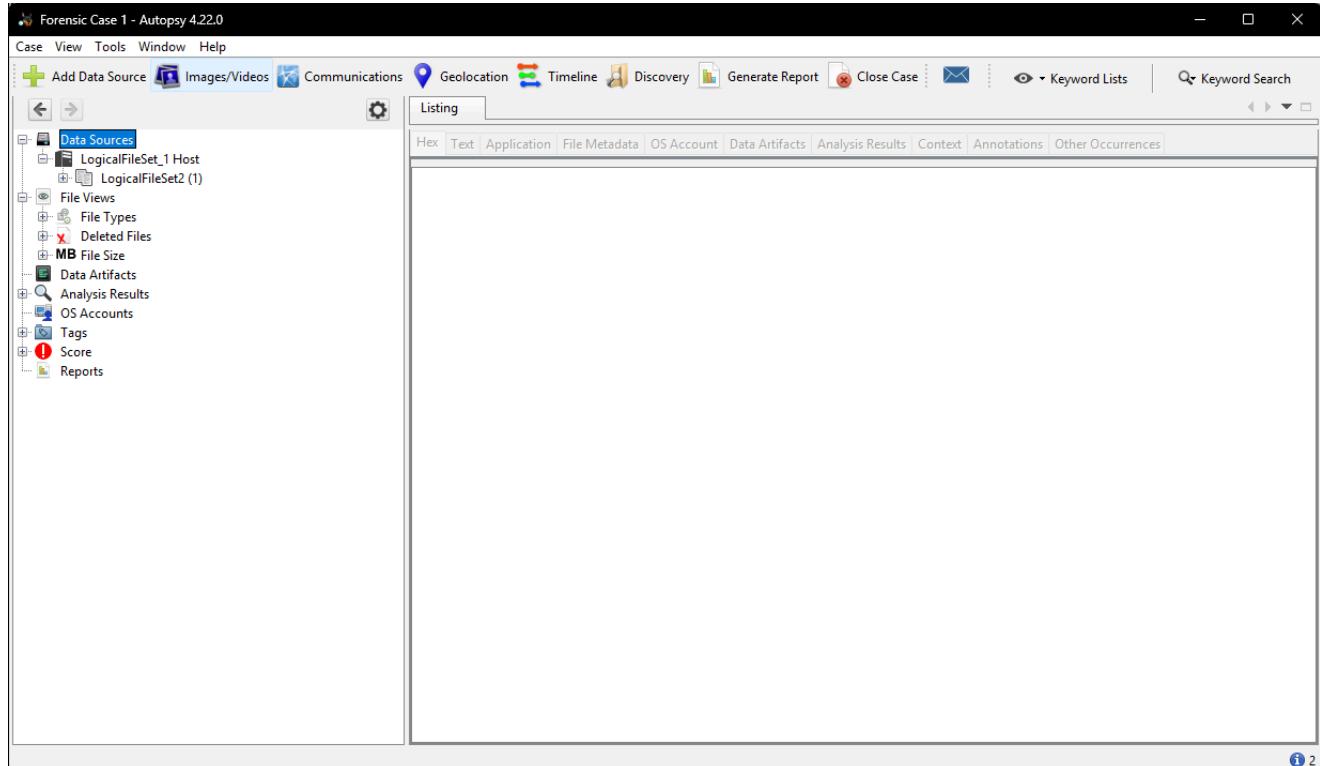
En el caso en que no este listando nada, como a mi. Será necesario Expandir en la parte izquierda de Autopsy el Menu de Data Sources ir al LogicalFileSet y una vez nos salga eso tendremos que presionar clic derecho y presionar la opción de Run Ingest Modules , quizás puede dar error de licencia en Cyber Triage Malware Scanner así que en este caso vamos a desactivarlo. Una vez pasado el menú Autopsy procedera a realizar la ingestión de datos



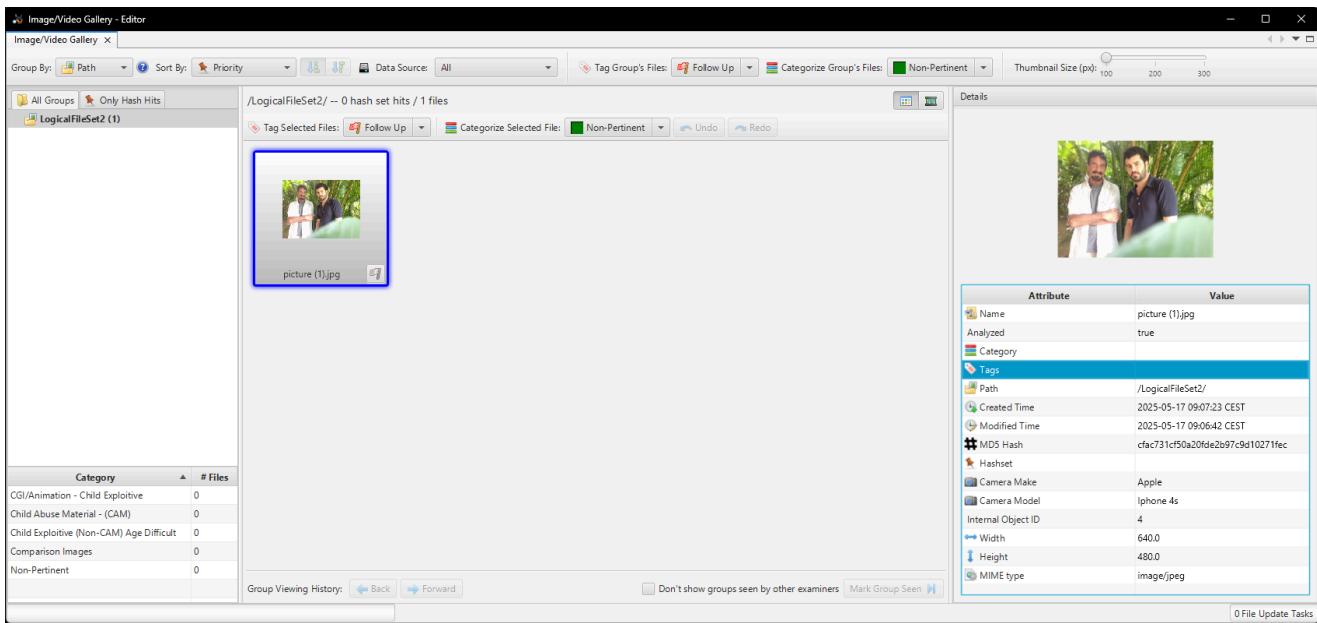
Si Autopsy no lista ningún artefacto tras la ingestión inicial, abrimos el panel izquierdo en Data Sources y expandimos el nodo LogicalFileSet . A continuación, hacemos clic derecho sobre LogicalFileSet y seleccionamos Run Ingest Modules . Este paso fuerza la re-ejecución de todos los módulos configurados.

En la esquina inferior derecha de la interfaz aparece un indicador de estado: un ícono **rojo** señala un error, uno **amarillo** indica que aún se está procesando o indexando, y uno **azul** refleja que el proceso ha finalizado correctamente. Al hacer clic en ese círculo se despliega información detallada sobre el módulo que generó el estado.

En mi caso, el ícono se volvió rojo y, al expandirlo, identifiqué un error de licencia en el módulo **Cyber Triage Malware Scanner**. Desactivamos dicho módulo desde el diálogo de configuración y reejecutamos los restantes, asegurando que la extracción de metadatos y el análisis de archivos se completaran sin bloqueos.



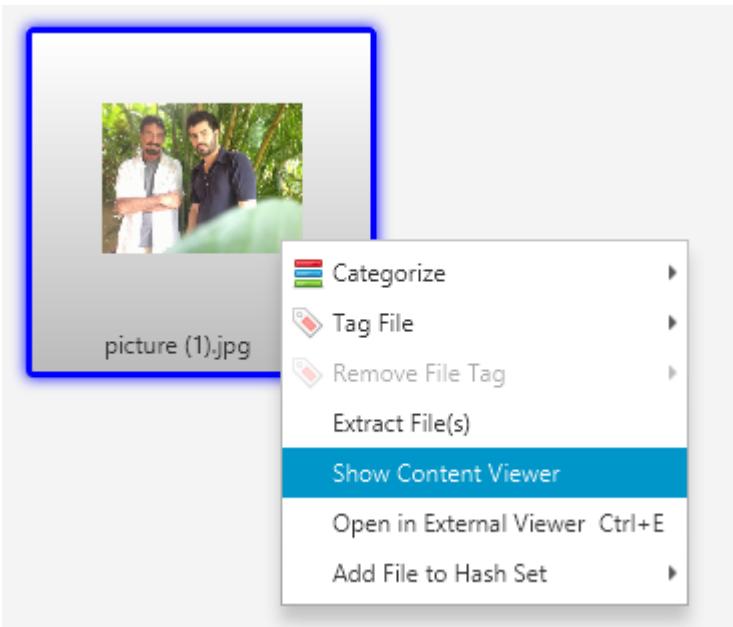
Tras completarse la ingestión de datos, navegamos a la sección **Images/Videos** en el panel izquierdo. Aquí Autopsy muestra en una vista central todas las miniaturas de los archivos multimedia extraídos, permitiéndonos filtrar por tipo (imagen, vídeo), ordenar por fecha de creación o tamaño, y acceder rápidamente a metadatos resumidos sin abrir cada archivo individualmente.



Una vez en **Images/Videos**, Autopsy muestra la miniatura de `picture.jpg` junto a un panel de detalles (derecha) con atributos clave:

- **MD5 Hash (cfc731cf50a20fde2b97c9d10271fec)**: permite verificar integridad y detectar modificaciones o duplicados.
- **Camera Make y Model**: indica que la imagen fue capturada con un Apple iPhone 4s, lo cual aporta contexto al dispositivo involucrado.
- **Created Time / Modified Time**: fechas de procesamiento por Autopsy, no confundir con la fecha EXIF de captura.
- **Path**: confirma la fuente (`/LogicalFileSet2`), útil al correlacionar artefactos en casos con múltiples data sources.
- **Tags & Categorías**: en la parte inferior izquierda, Autopsy propone estas categorías predeterminadas para clasificar imágenes:
 - CGI/Animation – Child Exploitive
 - Child Abuse Material (CAM)
 - Child Exploitive (Non-CAM) Age Difficult
 - Comparison Images
 - Non-Pertinent

*Este menú nos permite no solo visualizar información esencial de un vistazo (hash, origen, tipo de archivo), sino también asignar **Tags** y **Categorías** para organizar el análisis de manera estructurada.*



Si hacemos clic derecho sobre la miniatura y seleccionamos **Show Content Viewer**, se despliega un conjunto de pestañas para examinar la imagen desde varias perspectivas:

- **Hex:** inspección hexadecimal para confirmar firmas (FF D8 FF), ubicar segmentos EXIF y detectar posibles datos ocultos o incrustaciones maliciosas.

LogicalFileSet2/picture (1).jpg - Editor

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Other Occurrences

Page: 1 of 9 Page Go to Page: | Jump to Offset Launch in Hd

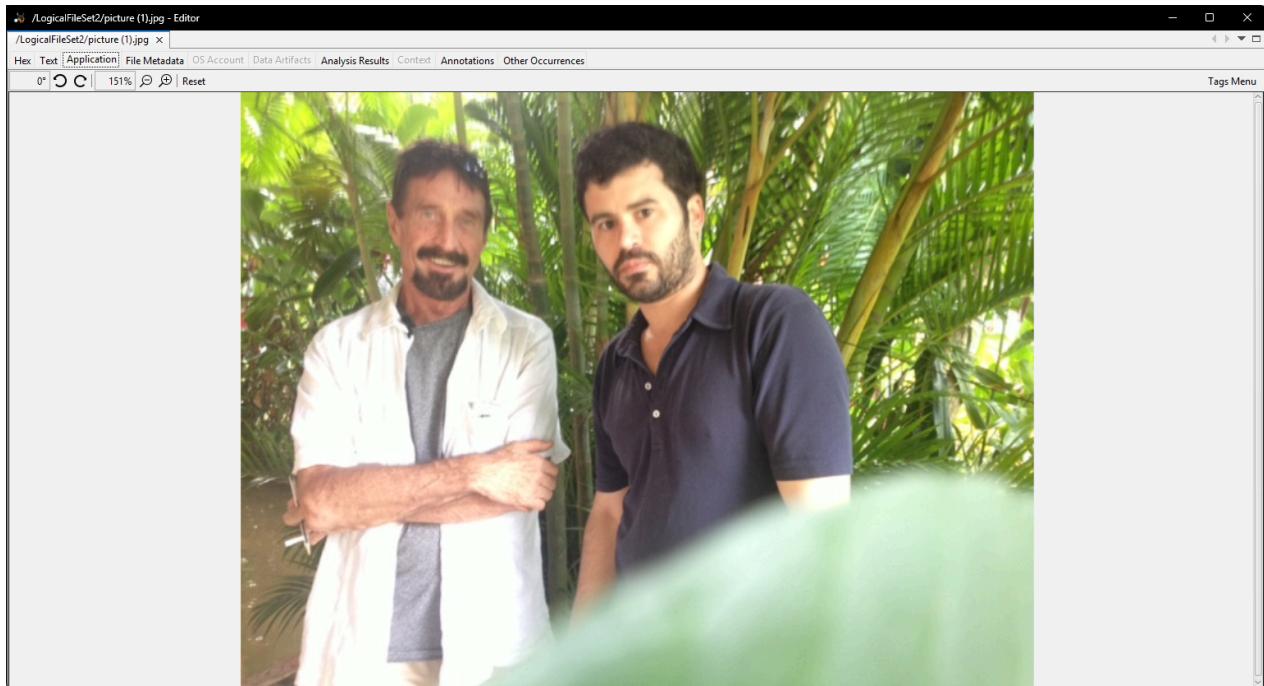
```

FF D8 FF E1 03 26 45 79 E9 E6 00 00 4D 4D 00 2A .....Exif..NM.
0x00000010: 00 00 00 08 00 0B 01 0F 00 02 00 00 00 06 00 00 ..... .
0x00000020: 00 S2 01 10 00 02 00 00 00 08 00 00 00 98 01 12 ..... .
0x00000030: 00 03 00 00 00 01 00 01 00 00 00 01 1A 00 05 00 00 ..... .
0x00000040: 00 01 00 00 00 A1 01 1B 00 05 00 00 00 01 00 00 ..... .
0x00000050: 00 AA 01 28 00 00 00 00 00 01 00 02 00 00 01 31 .....1
0x00000060: 00 02 00 00 00 00 00 00 B2 01 32 00 02 00 00 .....2
0x00000070: 00 14 00 00 00 B8 02 13 00 03 00 00 00 01 00 01 ..... .
0x00000080: 00 00 87 E5 00 00 00 00 00 01 00 00 00 CC 88 25 .....1.....4
0x00000090: 00 04 00 00 00 01 00 00 02 52 00 00 00 00 41 70 .....R...Ap
0x000000a0: 70 EC E6 00 E9 51 E8 EF EE E6 20 34 53 00 00 ple.iPhone 4S...
0x000000b0: 00 49 00 00 00 00 00 00 00 40 00 00 00 00 01 3E 2E .H.....H...6.
0x000000c0: 30 2E 31 00 32 30 31 32 3A 31 32 3A 30 33 20 31 01.1.2012:12:03 1
0x000000d0: 32 3A 32 36 3A 30 30 00 00 18 82 8A 00 05 00 00 2:26:00.....
0x000000e0: 00 01 00 00 01 F2 82 5D 00 00 00 00 00 00 00 01 00 00 ..... .
0x000000f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0x00000100: 00 03 00 00 00 01 00 7D 00 00 50 00 00 07 00 00 .....1.....
0x00000110: 00 04 00 32 32 31 00 03 00 02 00 00 00 14 00 00 ..0221.....
0x00000120: 02 02 90 04 00 02 00 00 00 14 00 00 02 16 91 01 ..... .
0x00000130: 00 07 00 00 00 04 00 00 00 01 52 01 00 0A 00 00 ..... .
0x00000140: 00 01 00 00 02 2A 92 02 00 05 00 00 00 01 00 00 ..... .
0x00000150: 02 32 92 03 00 00 00 00 00 01 00 00 00 03 92 07 .2.....1.
0x00000160: 00 03 00 00 00 01 00 03 00 00 00 00 52 09 00 03 00 00 ..... .
0x00000170: 00 01 00 10 00 01 92 0A 00 00 00 00 00 01 00 00 ..... .
0x00000180: 02 42 92 14 00 03 00 00 00 04 00 00 02 4A A0 00 .B.....J..
0x00000190: 00 07 00 00 00 03 31 30 30 A0 01 00 03 00 00 .....0100.....
0x000001a0: 00 01 00 01 00 0A 02 00 04 00 00 00 01 00 00 ..... .
0x000001b0: 0C C0 A0 03 00 00 00 00 01 00 00 00 00 A2 17 ..... .
0x000001c0: 00 03 00 00 00 01 00 02 00 00 A4 02 00 03 00 00 ..... .
0x000001d0: 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0x000001e0: 00 00 04 05 00 03 00 00 00 00 00 00 00 00 00 00 .....$..
0x000001f0: 00 03 00 00 00 01 00 00 00 00 00 00 00 00 00 00 ..... .
0x00000200: 00 01 00 00 00 14 00 00 00 00 00 00 05 32 30 .....20
0x00000210: 31 32 3A 31 32 3A 30 33 20 31 32 3A 32 36 3A 30 12:12:03 12:26:0
0x00000220: 30 00 32 31 31 32 3A 31 32 3A 30 33 20 31 32 3A 0.2012:12:03 12:
0x00000230: 32 36 3A 30 30 00 00 00 0A DB 00 00 02 83 00 00 26:00.....
0x00000240: 10 D8 00 00 04 AB 00 00 0D 62 00 00 05 5D 00 00 .....1....
0x00000250: 00 6B 00 00 00 19 09 74 03 00 02 E2 05 64 00 09 .k.....t...b.d..
0x00000260: 00 01 00 02 00 00 00 02 4E 00 00 00 02 00 00 00 .....N.....
0x00000270: 00 00 03 00 00 02 C4 00 03 00 02 00 00 00 00 02 ..... .
0x00000280: 57 00 00 00 00 05 00 00 03 00 00 02 DC W..... .
0x00000290: 00 05 00 01 00 00 00 01 00 00 00 00 00 00 06 00 05 ..... .
0x000002a0: 00 00 00 01 00 02 F4 00 07 00 05 00 00 00 03 ..... .
0x000002b0: 00 00 02 FC 00 10 00 02 00 00 00 02 54 00 00 00 .....T...
0x000002c0: ..11 00 05 ..00 00 01 ..00 00 02 14 ..00 00 00 ..00

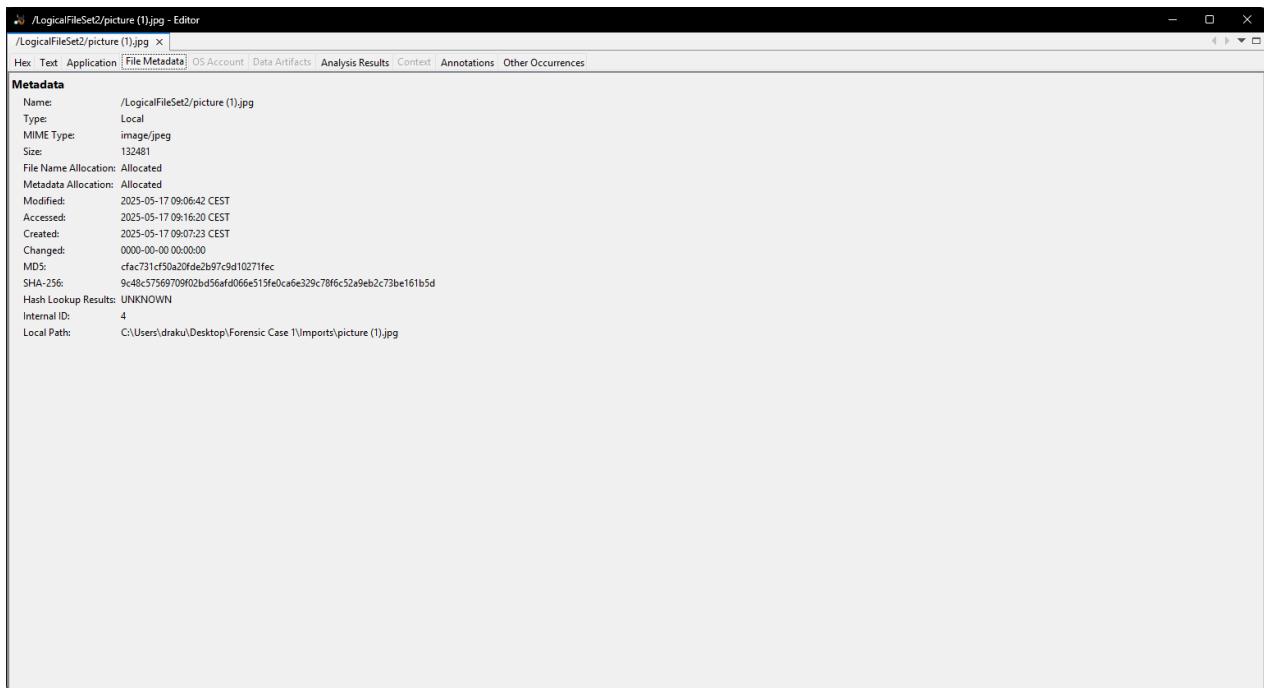
```

- **Text:** ejecución de strings para extraer fragmentos legibles (rutas, URLs, etiquetas XMP), ideal para hallar referencias internas.

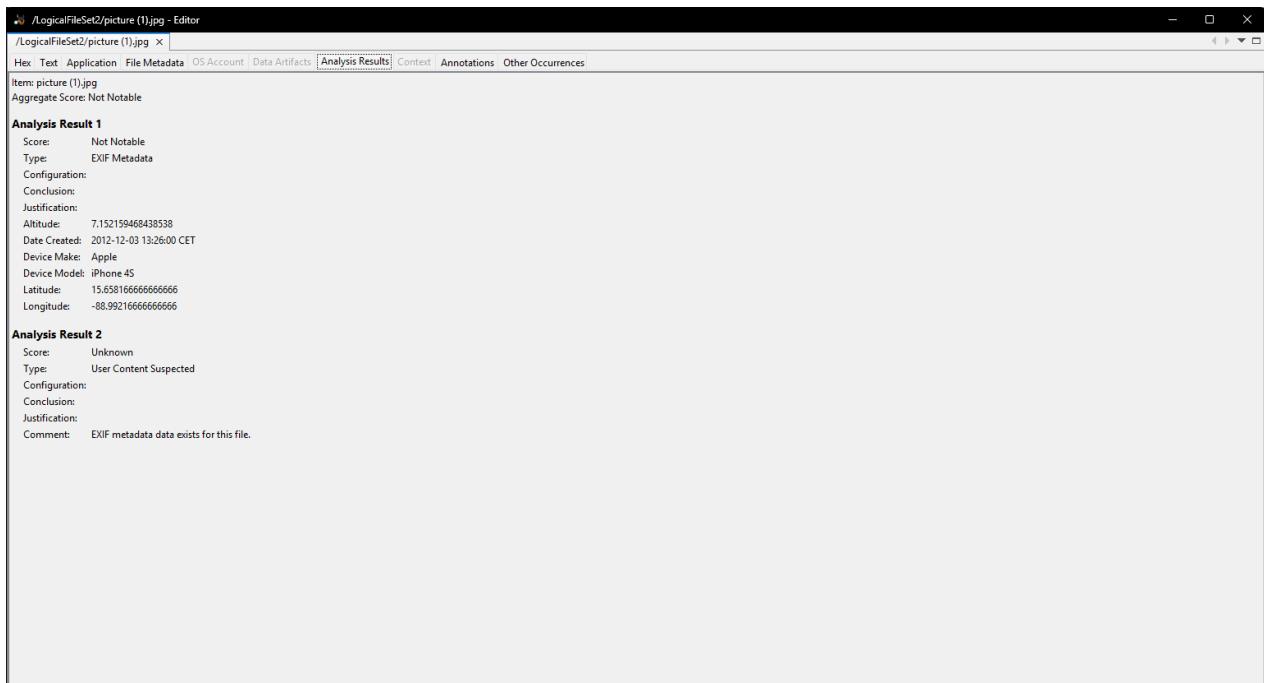
- **Application:** información sobre el dispositivo o software creador (modelo de cámara, versión de firmware), que aporta contexto sobre el origen del archivo.



- **File Metadata:** metadatos del sistema de archivos (tamaño, fechas de creación/modificación por Autopsy, ruta local), distintos de los EXIF originales.

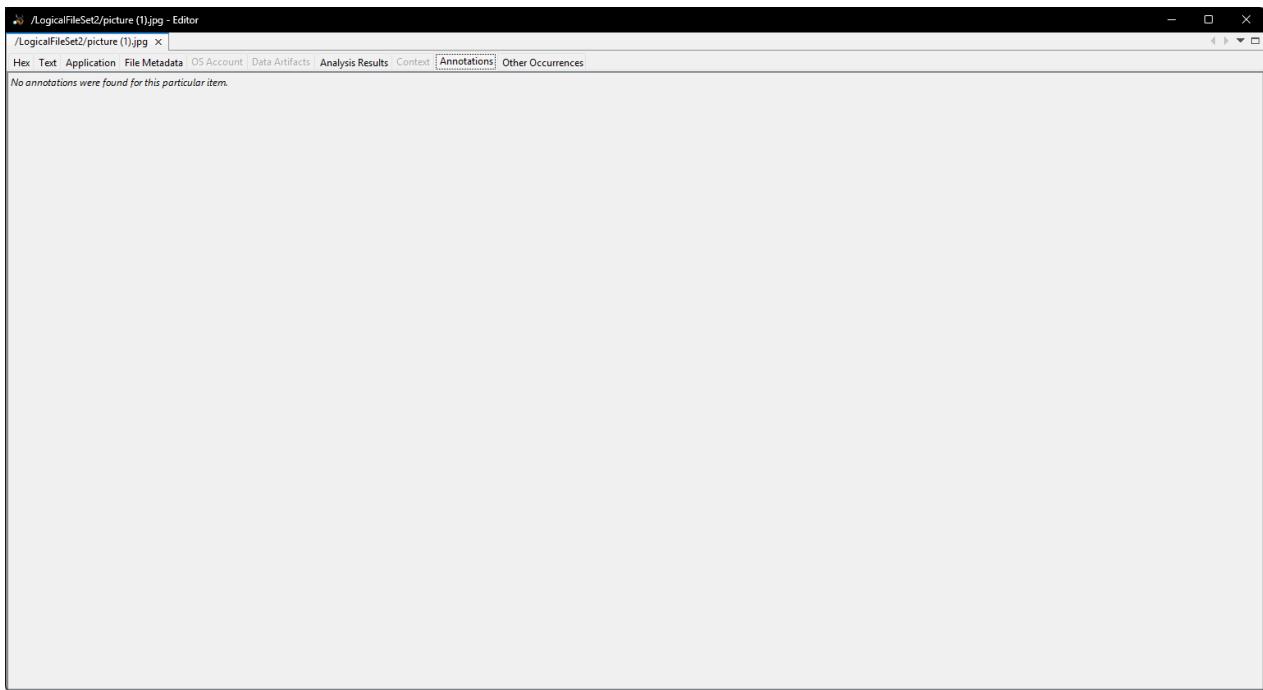


- **Analysis Results:** consolidación de metadatos EXIF más críticos, como fecha y hora de captura, coordenadas GPS y altitud.



Ejemplo: fecha de captura 2012-12-03 13:26:00 y GPS Lat 15.658166667 , Lon -88.992166667 .

- **Annotations:** espacio para notas del investigador; en este caso ninguna anotación previa.



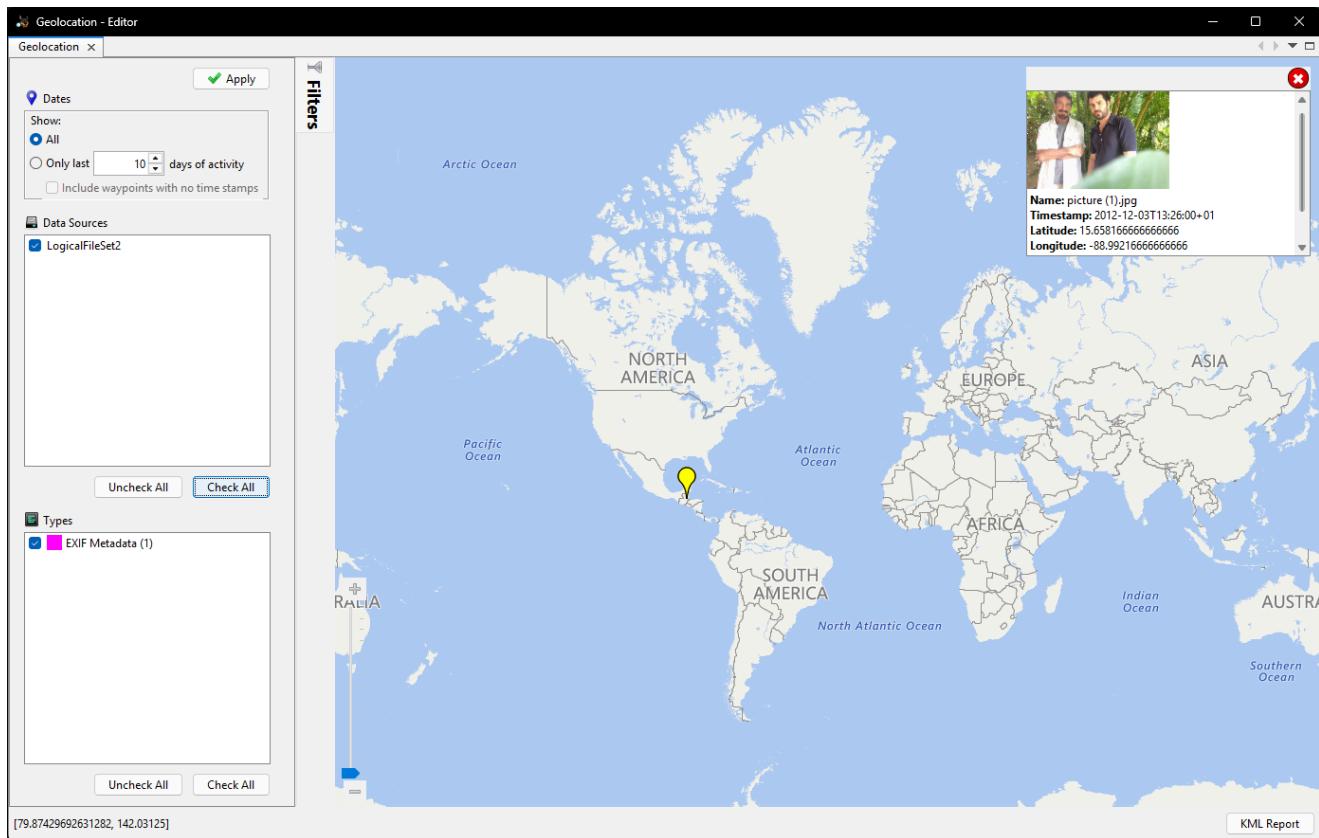
- **Other Occurrences:** lista todas las instancias detectadas de este archivo en otros data sources o casos, facilitando la trazabilidad de duplicados.

A screenshot of the same software interface, but now showing the 'Other Occurrences' tab. The window title is 'LogicalFileSet2/picture (1).jpg - Editor'. The tabs at the top are: Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The 'Other Occurrences' tab is selected. The main area displays a table with three columns: 'Case', 'Data Source Name', and 'File Name'. There is one row of data: 'JJ' under Case, 'LogicalFileSet2' under Data Source Name, and 'picture.jpg' under File Name. To the right of the table, there are several sections of detailed information:

- Common Properties**:
 - Type: File MD5
 - Value: cfac731cf50a20fd2b97c9d10271fec
 - Known Status: unknown
- File Details**:
 - File Path: /picture.jpg
- Data Source Details**:
 - Name: LogicalFileSet2
- Case Details**:
 - Name: JJ
 - Created Date: 2024/11/29 09:21:17 (CET)

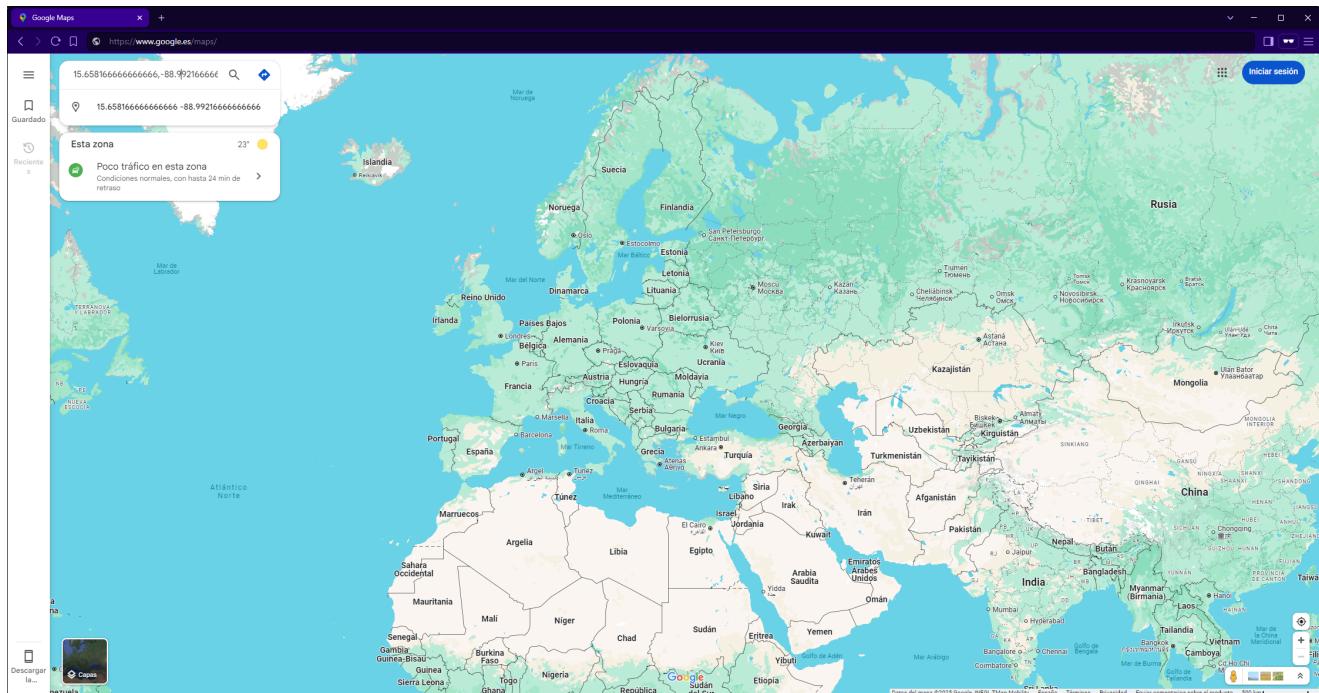
At the bottom left of the window, it says 'Central Repository Starting Date: 2024/11/29 09:21:17 (CET)'. At the bottom right, it says 'Found 1 instances in 1 cases and 1 data sources.'

Cada pestaña complementa las demás, proporcionando desde datos en crudo hasta metadatos estructurados que agilizan el análisis forense.



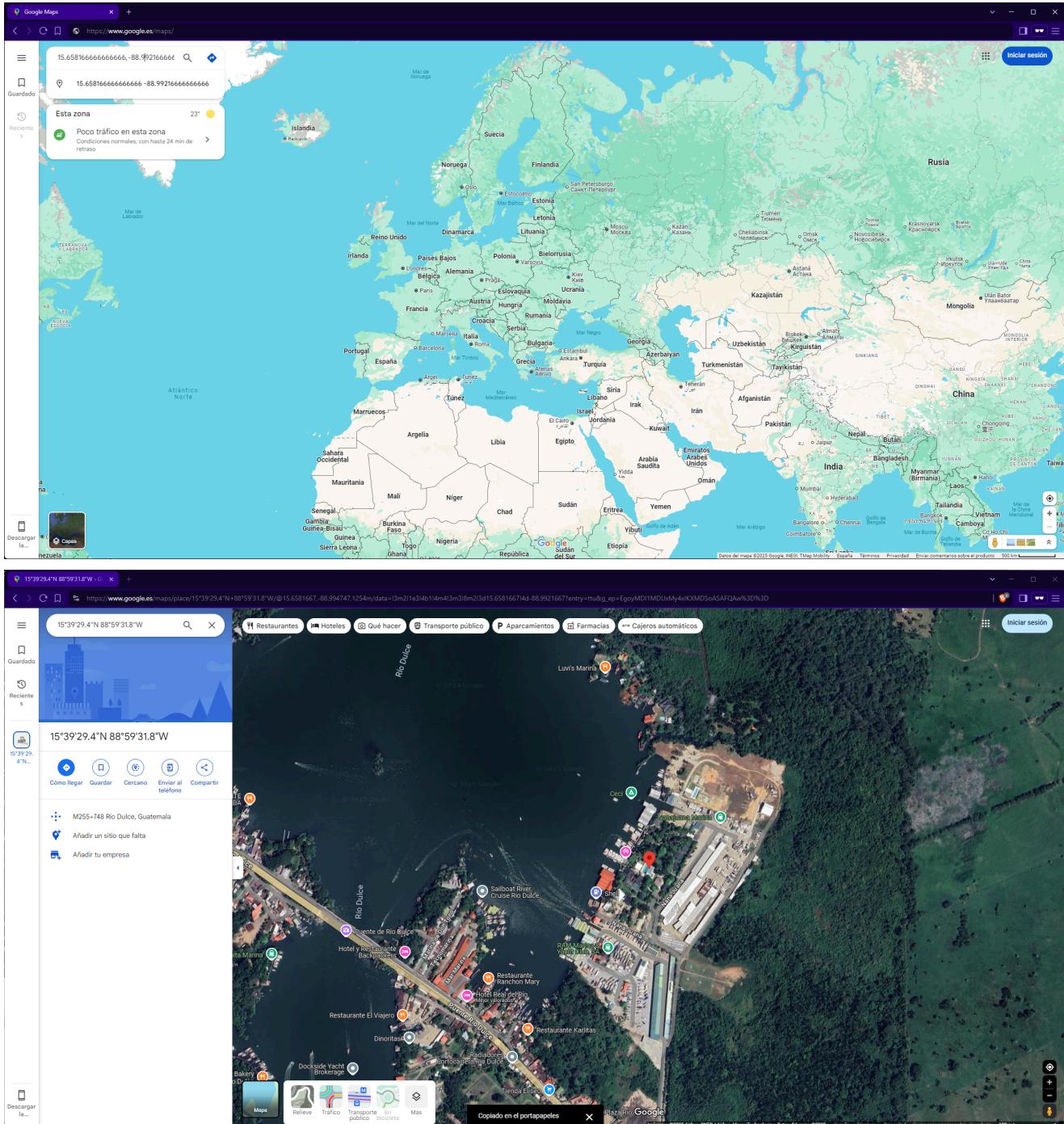
Al acceder al menú **Geolocation**, Autopsy renderiza un globo terráqueo interactivo con un pin en la ubicación aproximada basada en los metadatos GPS extraídos. En esta vista podemos rotar y acercar el globo para comprobar si las coordenadas apuntan a una zona terrestre, costera o marítima, lo que ayuda a validar la fiabilidad de los datos.

Copiar las coordenadas decimales: 15.658166666666666, -88.99216666666666 .



En la esquina superior derecha aparece un panel con los detalles de **Latitude** y **Longitude** en formato decimal. Desde aquí copiamos cómodamente los valores para usarlos en herramientas externas como Google Maps o scripts de conversión. Además, se muestran otros metadatos de geolocalización (altitud, precisión, datum) que permiten evaluar la exactitud de la posición.

Verificación en Google Maps



El panel inferior revela el Plus Code (*M255+748 Río Dulce, Guatemala*), que actúa como un identificador de ubicación preciso incluso en zonas sin direcciones formales. La conversión a DMS proporcionada por Google (visible junto al buscador) se puede usar directamente para el reto o como comprobación antes de usar scripts de conversión. Además, la vista de calle (Street View) ayuda a validar visualmente características del entorno captado.

Google maps nos ayuda a pasar de Formato **grados decimales** DD a DMS pero en el caso de que no disponamos de Google Maps nos podríamos montar un script como el siguiente:

```
# Coordenadas decimales proporcionadas
lat_decimal = 15.658166666666666 # Latitud en formato decimal
lon_decimal = -88.99216666666666 # Longitud en formato decimal
```

```

# Función para convertir coordenadas decimales a grados, minutos y segundos
(DMS)

def decimal_to_dms(decimal):
    degrees = int(decimal)
    minutes_decimal = abs(decimal - degrees) * 60
    minutes = int(minutes_decimal)
    seconds = (minutes_decimal - minutes) * 60
    return degrees, minutes, seconds

# Convertir la latitud y longitud de decimal a DMS
lat_dms = decimal_to_dms(lat_decimal) # Convertir latitud
lon_dms = decimal_to_dms(lon_decimal) # Convertir longitud

# Determinar la dirección para la latitud (N o S) y longitud (E o W)
lat_direction = "N" if lat_decimal >= 0 else "S"
lon_direction = "E" if lon_decimal >= 0 else "W"

# Crear una función para alinear y mostrar la tabla
def print_table():

    # Definir los datos de la tabla
    headers = ["Coordenada", "Grados", "Minutos", "Segundos", "Dirección"]
    lat_data = ["Latitud", f"{lat_dms[0]}", f"{lat_dms[1]}", f"{lat_dms[2]:.1f}", lat_direction]
    lon_data = ["Longitud", f"{lon_dms[0]}", f"{lon_dms[1]}", f"{lon_dms[2]:.1f}", lon_direction]

    # Calcular el ancho máximo de cada columna
    column_widths = [max(len(str(item))) for item in col] for col in
zip(headers, lat_data, lon_data)]

    # Función para imprimir una fila de la tabla
    def print_row(row):
        print("| " + " | ".join([str(item).ljust(column_widths[i]) for i,
item in enumerate(row)]) + " |")

    # Calcular la línea de separación
    separator = "+" + "+".join(["-" * (width + 2) for width in
column_widths]) + "+"

    # Imprimir la tabla
    print(separator)
    print_row(headers)
    print(separator)
    print_row(lat_data)
    print_row(lon_data)
    print(separator)

# Llamar a la función para mostrar la tabla
print_table()

```

```

# Construir el formato de coordenadas: 15°39'29.4"N 88°59'31.8"W
lat_formatted = f"{lat_dms[0]}{lat_dms[1]}{lat_dms[2]:.2f}{lat_direction}"
lon_formatted = f"{lon_dms[0]}{lon_dms[1]}{lon_dms[2]:.2f}{lon_direction}"

# Imprimir el resultado final con las coordenadas en formato adecuado
print(f"\nCoordenadas: {lat_formatted} {lon_formatted}\n")

```

Output:

Coordenada	Grados	Minutos	Segundos	Dirección
Latitud	15	39	29.4	N
Longitud	-88	59	31.8	W

Coordenadas: 15°39'29.40"N 88°59'31.80"W

Comentario: Obsérvese que en el resultado final **los segundos pasan a dos decimales** (29.40" y 31.80") y las coordenadas negativas se transforman en direcciones cardinales (**W** para longitud). Estas transformaciones son necesarias para cumplir con el formato del reto.

Formateo Final de la Flag

Una vez obtenidos los valores DMS con dos decimales y direcciones cardinales:

1. Eliminamos los símbolos (° , ' , ") y las comas, reemplazándolos por guiones bajos – .
2. Aseguramos que cada componente (grados, minutos, segundos con dos decimales, dirección) esté separado por un único guión bajo.
3. Construimos la cadena bajo el formato CTF{...} .

```

15°39'29.40"N 88°59'31.80"W → 15_39_29_40_N_88_59_31_80_W
15_39_29_40_N_88_59_31_80_W → CTF{15_39_29_40_N_88_59_31_80_W}

```

Nota:

No incluimos signos negativos; la dirección cardinal sustituye al signo. Cada número debe ocupar al menos dos dígitos si es posible (00–59 para minutos/segundos). El orden exacto es:

lat_grados_lat_min_lat_seg_lat_dir_lon_grados_lon_min_lon_seg_lon_dir.

Flag final: CTF{15_39_29_40_N_88_59_31_80_W} *(29.40" y 31.80") y las coordenadas negativas se transforman en direcciones cardinales (W para longitud). Estas transformaciones son necesarias para cumplir con el formato del reto.