

# INFORME PERICIAL INFORMÁTICO

El caso "¿Dónde está mi sobre?" implica la búsqueda y análisis de evidencia digital para esclarecer la desaparición de un sobre importante. Se llevaron a cabo procedimientos para obtener y documentar las evidencias, identificando buzones de correo electrónico, recuperando información borrada y verificando la autenticidad de los correos electrónicos relevantes. Los resultados obtenidos permitieron identificar comunicaciones con entidades pertinentes y corroborar la integridad de la información recuperada, facilitando conclusiones sólidas sobre el caso.

Análisis Forense  
Informático

---

<b>1.- PAGINA INICIAL DEL INFORME</b>	<b>2</b>
<b>2.- INTRODUCCIÓN Y OBJETO DEL INFORME PERICIAL</b>	<b>3</b>
<b>3.- PRESENTACIÓN DE PERITO Y ENTIDAD PERICIAL</b>	<b>3</b>
<b>4.- ANTECEDENTES</b>	<b>4</b>
<b>5.- ALCANCE</b>	<b>4</b>
5.1.- Procedimientos de Análisis Forense Aplicados	4
5.2.- Limitaciones del Análisis Forense	5
<b>6.- FUENTES DE INFORMACIÓN</b>	<b>5</b>
<b>7.- MANIFESTACIONES</b>	<b>6</b>
<b>8.- FUNDAMENTOS DE ESTE INFORME PERICIAL</b>	<b>7</b>
<b>9.- RESULTADOS DE LOS PROCEDIMIENTOS REALIZADOS</b>	<b>8</b>
9.1 Recuperación de Evidencias Digitales	8
9.2 Documentación de la Cadena de Custodia	9
9.3 Autorizaciones	11
9.4 Análisis Forense de las Evidencias y Presentación de los Resultados	12
9.4.1 Identificación de los Archivos Eliminados	12
9.4.2 Recuperación de Datos Ocultos en Archivos Excel	12
9.4.3 Descubrimiento de Mensajes Ocultos en Archivos de Imagen	13
9.4.4 Recopilación y Presentación de Evidencias	13
9.4.5 Conclusiones del Análisis	19
<b>10.- CONCLUSIONES</b>	<b>19</b>

# 1.- PAGINA INICIAL DEL INFORME


DEPARTAMENTO INFORMATICA FORENSE

<b>Departamento:</b>	<b>Forense</b>

Revisión	Fecha	Fecha Aprobación
2	10/04/2024	12/04/2024
Realizado por	Revisado por	Aprobado por
Enrique García García	Javier Martínez	Marta López



Firma: Enrique García García



Firma: Javier Martínez



Firma: Marta López

**INFORME TECNOLOGICO FORENSE DEL ORDENADOR PERSONAL DE:**

**- Señor BarceLOnas**  
**- Departamento de Investigación de Incidentes Digitales**

## **2.- INTRODUCCIÓN Y OBJETO DEL INFORME PERICIAL**

En virtud de la solicitud dirigida a mi persona como perito independiente en el juicio contra el señor BarceLONas por presuntos delitos de blanqueo de capitales y tráfico de influencias, se me ha encomendado realizar un informe pericial forense sobre un dispositivo de almacenamiento tipo pendrive perteneciente al señor BarceLONas.

El objeto del presente informe es analizar el contenido del pendrive intervenido por la Unidad de Delitos Económicos de la Policía Judicial Mordorense, con el fin de identificar y presentar las pruebas digitales relacionadas con el presunto delito de blanqueo de capitales y tráfico de influencias atribuido al señor BarceLONas.

Se espera que este informe proporcione evidencia digital que contribuya al esclarecimiento de los hechos y pueda ser presentado ante los tribunales competentes como parte del proceso judicial.

En este informe pericial, se detallarán los procedimientos realizados para analizar el contenido del pendrive, así como las evidencias digitales encontradas y su relevancia para el caso en cuestión. Además, se ofrecerán conclusiones basadas en los hallazgos obtenidos durante la investigación.

## **3.- PRESENTACIÓN DE PERITO Y ENTIDAD PERICIAL**

El presente informe pericial ha sido elaborado por el perito independiente, D. Enrique García García, en calidad de experto en informática forense y peritaje digital.

D. Enrique García García es miembro certificado de la Ilustre Asociación Comarcal de Peritos Judiciales de Mordor y cuenta con una amplia experiencia en el campo de la informática forense, avalada por numerosas intervenciones periciales en casos judiciales similares.

El informe ha sido desarrollado bajo la responsabilidad y supervisión de la entidad pericial "ForenseTech", una empresa especializada en servicios de peritaje informático y análisis forense digital. ForenseTech cuenta con un equipo de expertos altamente cualificados y reconocidos en el ámbito de la informática forense, con una amplia trayectoria en la realización de peritajes judiciales y extrajudiciales.

La entidad ForenseTech garantiza la objetividad, imparcialidad y rigor técnico en la elaboración del presente informe, así como el cumplimiento de los estándares éticos y profesionales establecidos en el ejercicio de la pericia judicial.

## 4.- ANTECEDENTES

El análisis forense del pendrive forma parte del reto "BarceLOnas, ¿dónde está mi sobre?", organizado por Flu Project. En este contexto, el perito Enrique García García asume el papel de investigador independiente en el juicio del Señor BarceLOnas. La acusación sugiere que el Señor BarceLOnas ha utilizado 300.000€ de origen ilícito. Con el fin de refutar estas acusaciones, se encarga a García García analizar el contenido del pendrive en busca de evidencia digital que pueda respaldar la defensa del Señor BarceLOnas. Este informe proporciona un análisis detallado de las acciones realizadas durante el proceso de examen forense del dispositivo y presenta los hallazgos relevantes para la investigación en curso.

## 5.- ALCANCE

Los procedimientos realizados en el desarrollo de nuestro trabajo han sido los siguientes:

1. Conversaciones con representantes legales de D. Enrique García García y el equipo de defensa del Sr. BarceLOnas.
2. Obtención de una imagen forense del pendrive proporcionado por la Unidad de Delitos Económicos de la Policía Judicial Mordorense.
3. Análisis exhaustivo de la imagen forense para identificar y recuperar cualquier evidencia digital relevante.
4. Verificación de la autenticidad e integridad de los archivos recuperados.
5. Elaboración de un informe pericial detallando el análisis forense realizado y presentando las evidencias digitales obtenidas.

### 5.1.- Procedimientos de Análisis Forense Aplicados

Se siguieron los siguientes procedimientos durante el análisis forense del pendrive:

**Extracción de la imagen forense:** Se realizó una copia exacta del pendrive utilizando herramientas forenses especializadas para preservar la integridad de los datos originales.

**Exploración de la imagen forense:** Se examinó exhaustivamente la imagen forense utilizando herramientas de análisis forense digital para identificar cualquier archivo o dato relevante.

**Recuperación de archivos eliminados:** Se llevaron a cabo técnicas de recuperación de datos para intentar recuperar archivos eliminados u ocultos en la imagen forense.

**Verificación de la autenticidad:** Se verificó la autenticidad de los archivos recuperados mediante la comparación de metadatos y firmas digitales, cuando estuvieran disponibles.

**Análisis de archivos recuperados:** Se analizaron los archivos recuperados en busca de evidencia relacionada con el caso, como correos electrónicos, documentos financieros u otros documentos relevantes.

## 5.2.- Limitaciones del Análisis Forense

Es importante tener en cuenta las siguientes limitaciones durante el análisis forense del pendrive:

**Restricciones de tiempo:** El análisis se realizó dentro de un marco de tiempo limitado, lo que puede haber afectado la exhaustividad del proceso.

**Complejidad del caso:** La complejidad del caso y la cantidad de datos involucrados pueden haber dificultado la identificación de todas las evidencias relevantes.

**Dispositivo físico:** El estado físico del pendrive y cualquier daño o corrupción de los datos pueden haber limitado la efectividad del análisis.

Estas limitaciones se tuvieron en cuenta al interpretar los resultados del análisis forense y al elaborar el informe pericial.

## 6.- FUENTES DE INFORMACIÓN

Las fuentes de información utilizadas para llevar a cabo el análisis forense del pendrive y la obtención de evidencias digitales en el caso "BarceLONas, ¿dónde está mi sobre?" son las siguientes:

Carta y paquete recibidos por el perito Enrique García García, que incluyen un DVD con una imagen en formato dd del pendrive y el documento de cadena de custodia.

Conversaciones con representantes legales involucrados en el caso.

Pendrive intervenido por la Unidad de Delitos Económicos de la Policía Judicial Mordorense y puesto bajo custodia del secretario judicial.

Archivos contenidos en la imagen en formato dd del pendrive, incluyendo:

- Documento de cadena de custodia.
- Fichero de texto generado por la herramienta FTK Imagen con información de la clonación.
- Archivos eliminados recuperados, como una imagen .jpg y un archivo con extensión .doc.
- Procedimientos y herramientas forenses utilizadas para la adquisición y análisis de las evidencias digitales.

A lo largo del informe pericial se detallarán y analizarán las evidencias obtenidas de estas fuentes para proporcionar una evaluación completa del caso y presentar las pruebas digitales relevantes para el juicio.

## 7.- MANIFESTACIONES

En relación con el análisis realizado en el contexto del reto "¿Dónde está mi sobre?", manifestamos lo siguiente:

Juramos o prometemos que todas las afirmaciones y conclusiones presentadas en este informe son verídicas y se basan en nuestro mejor juicio profesional. Nos comprometemos a actuar con imparcialidad, considerando tanto los aspectos favorables como los que podrían perjudicar a cualquiera de las partes involucradas en el caso. Asimismo, estamos plenamente conscientes de las posibles consecuencias legales en caso de no cumplir con nuestro deber como peritos.

Las opiniones y conclusiones expresadas en este informe se fundamentan en nuestro entendimiento del reto "¿Dónde está mi sobre?" y están dentro de nuestro ámbito de conocimiento en materia de análisis forense y seguridad informática. Donde corresponda, hemos

identificado la fuente de la información utilizada para respaldar nuestras afirmaciones.

Al momento de emitir este informe, consideramos que es completo y adecuado para abordar las cuestiones planteadas en el reto. Sin embargo, nos comprometemos a informar a los interesados si llegamos a conocer hechos adicionales relevantes que puedan afectar nuestras conclusiones o requerir correcciones significativas en el informe.

Entendemos que este informe constituye la base de nuestra evaluación y análisis en el contexto del reto "¿Dónde está mi sobre?", y estaremos disponibles para proporcionar cualquier aclaración adicional o revisión que se considere necesaria en el futuro.

## 8.- FUNDAMENTOS DE ESTE INFORME PERICIAL

El presente informe pericial se fundamenta en los siguientes aspectos:

**Alcance del Análisis:** Se delimita exclusivamente a los aspectos tecnológicos involucrados en el análisis del pendrive y los archivos contenidos en el mismo, sin abordar cuestiones legales asociadas.

**Base de las Conclusiones:** Las afirmaciones y conclusiones aquí presentadas se sustentan únicamente en el análisis de la información proporcionada por nuestro cliente, así como en los procedimientos de trabajo llevados a cabo conforme al alcance definido en el presente informe. Cada conclusión se deriva de la interpretación de la información obtenida y de la documentación específica revisada, tal como se detalla en la sección de fuentes de información.

**Autenticidad de la Documentación:** En el caso de la documentación en formato papel, se ha priorizado el uso de documentos originales siempre que estuvieran disponibles. Sin embargo, no se ha realizado una verificación exhaustiva de su autenticidad, ya que este aspecto no entra dentro del ámbito de nuestra especialización. En el caso de documentos que fueran copias, no se ha verificado su concordancia con los originales. No obstante, se han seguido protocolos estrictos y confiables en la obtención de evidencia digital y en la creación de imágenes forenses, como se describe detalladamente en la sección correspondiente de este informe.

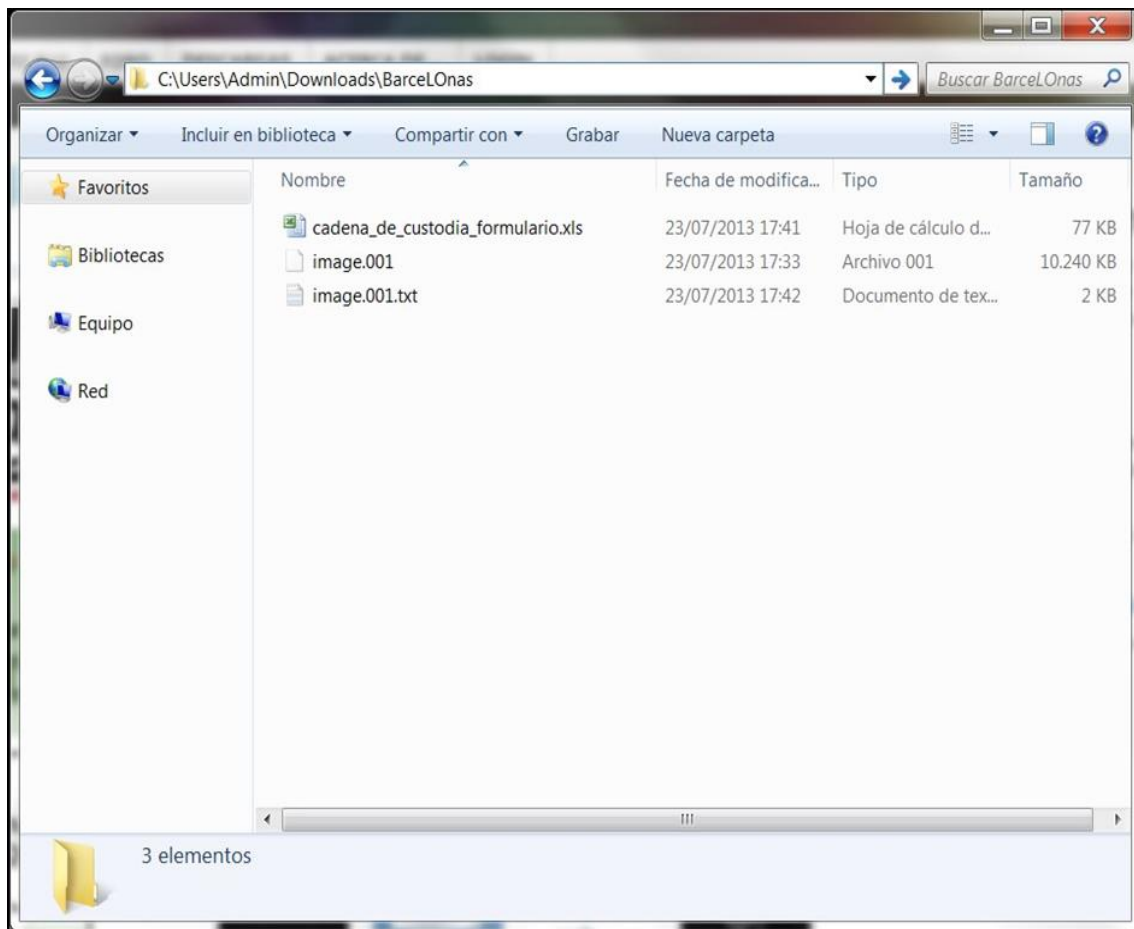


**Actualización del Informe:** Cualquier modificación o actualización a este informe solo se realizará previa solicitud expresa de la entidad responsable del mismo o de los tribunales competentes en la materia.

## 9.- RESULTADOS DE LOS PROCEDIMIENTOS REALIZADOS

### 9.1 Recuperación de Evidencias Digitales

El perito recibió un paquete que contenía un DVD con una imagen en formato dd del pendrive en cuestión, junto con el documento de cadena de custodia. Tras la recepción, se verificó la integridad de la imagen utilizando el hash proporcionado en el documento de cadena de custodia.



Dentro de DVD se encontraba un Excel con el documento de cadena de custodia, con el correspondiente hash de la imagen DD.

## 9.2 Documentación de la Cadena de Custodia

La cadena de custodia es fundamental para garantizar la integridad y la veracidad de las evidencias digitales obtenidas en el contexto del reto "BarceLONas, ¿dónde está mi sobre?". A continuación, se detalla la documentación de la cadena de custodia asociada al proceso de análisis:

**Recepción de los Archivos:** El perito Enrique García García recibió un paquete que contenía un DVD con una imagen en formato dd del pendrive, junto con el documento de cadena de custodia.

cadena\_de\_custodia\_formulario.xls [Modo de compatibilidad] - Microsoft Excel

Archivo Inicio Insertar Diseño de página Fórmulas Datos Revisar Vista

Pegar Fuente Alineación Número Estilos Celdas

Ordenar y filtrar Buscar y seleccionar Modificar

C36

ABC D E FG H I J K LM N O PQ R ST U V WX Y ZAA

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35

**EVIDENCIA DIGITAL**

**CADENA DE CUSTODIA**

**Caso Num.:** **Pag.:** **De:**

**Soporte Físico - Detalles de los equipos**

Item:	Descripción:		
Pendrive	Pendrive		
Fabricante:	Modelo:	Num. de serie:	
Kingston	ABC123	4567890	

**DETALLES DE LA IMAGEN DE LOS DADOS**

Fecha/Hora:	Creada por:	Método:	Nombre de la Imagem:	Partes:
Tue Jul 23 17:33:20 2013	Juan Antonio Calles	dd	image	1
Drive:	HASH:			
E	0bd3f29a2eb4062fe064a16584c8454795449095 (SHA1)			

**CADENA DE CUSTODIA**

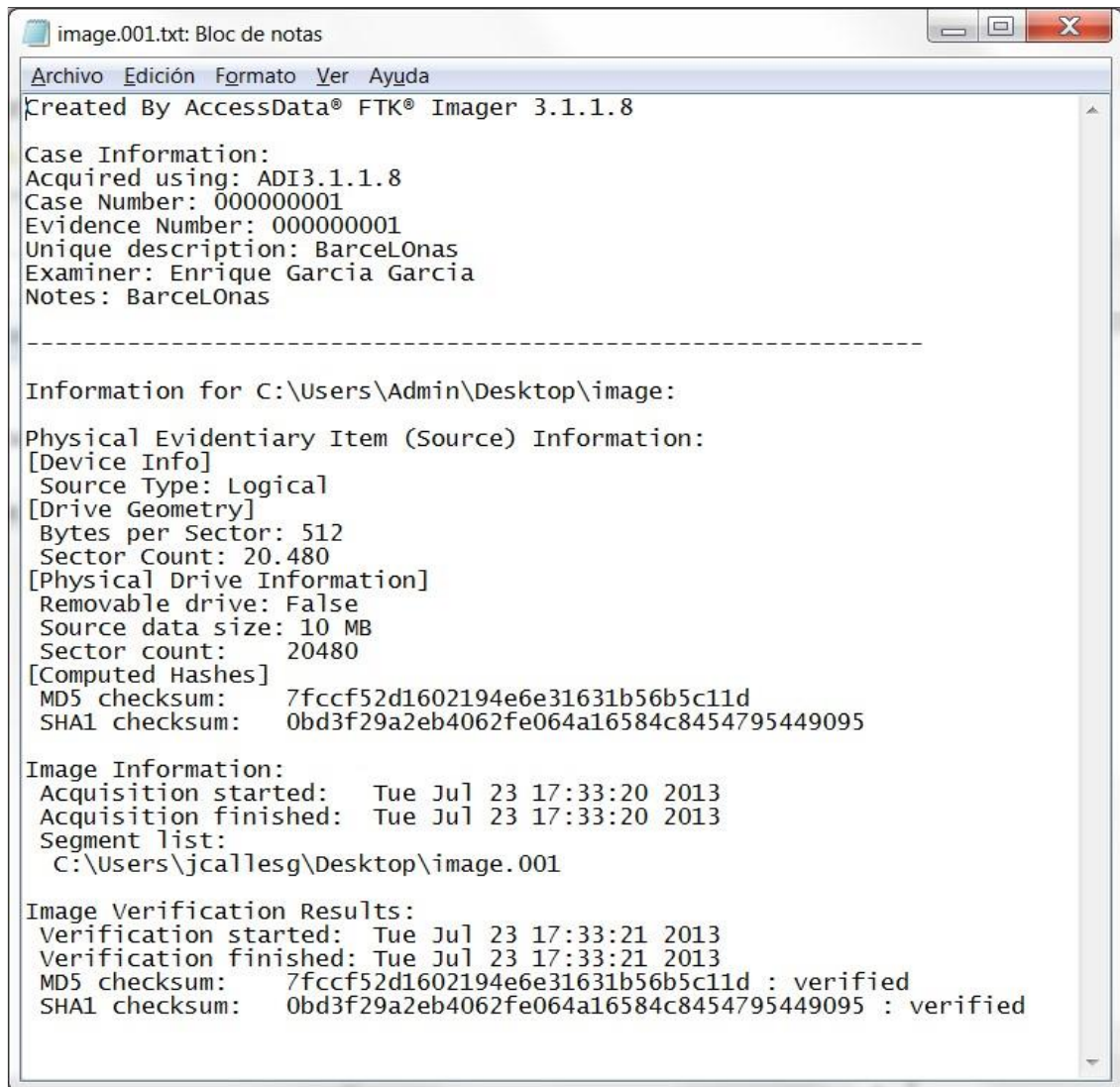
Destino:	Fecha/Hora:	Origen:	Destino	Motivo:
	Fecha:	NombreOrg.:	NombreOrg.:	
	15/08/2013	Juan Antonio Calles	Enrique García	
	Hora:	Firma:	Firma:	
	0:01	JACG	EGG	Perito

Plan3

Listo

90%

**Verificación de la Integridad:** Se llevó a cabo una verificación de la integridad de la imagen utilizando el hash proporcionado en el documento de cadena de custodia, asegurando que no se hubieran realizado modificaciones no autorizadas en los archivos.



**Extracción y Manipulación de los Archivos:** Tras la recepción, se procedió a la extracción de los archivos contenidos en la imagen dd utilizando herramientas forenses como FTK Imager. Esta extracción se realizó de manera cuidadosa y siguiendo los protocolos establecidos para evitar alteraciones en los datos originales.

**Registro de Actividades:** Se registraron todas las actividades realizadas durante el proceso de análisis, incluyendo la identificación de archivos, cambios de formato y cualquier manipulación llevada a cabo en los datos.

**Preservación de la Evidencia:** Se tomaron medidas para preservar la integridad de la evidencia digital, asegurando que no se perdiera ni se modificara durante el proceso de análisis. Esto incluyó el almacenamiento seguro de los archivos originales y de todas las copias realizadas para su posterior examen.

**Custodia de los Archivos:** Se mantuvo un registro detallado de la ubicación y la persona responsable de la custodia de los archivos en todo momento, asegurando su trazabilidad y evitando cualquier posibilidad de manipulación o contaminación de las evidencias.

En resumen, la documentación de la cadena de custodia proporciona un registro completo y detallado de todas las actividades realizadas durante el proceso de análisis de evidencias digitales, garantizando la integridad y la autenticidad de los datos obtenidos.

### 9.3 Autorizaciones

En concordancia con los procedimientos internos establecidos, se solicitó autorización expresa para llevar a cabo el análisis del pendrive en el contexto del reto "BarceLONas, ¿dónde está mi sobre?". Este paso es fundamental para garantizar la legalidad y la legitimidad del proceso de obtención de evidencias digitales.

El documento de autorización, disponible en el Anexo I del informe pericial, fue firmado por las partes autorizadas, otorgando el consentimiento para que el perito Enrique García García procediera con el análisis forense del dispositivo USB en cuestión.

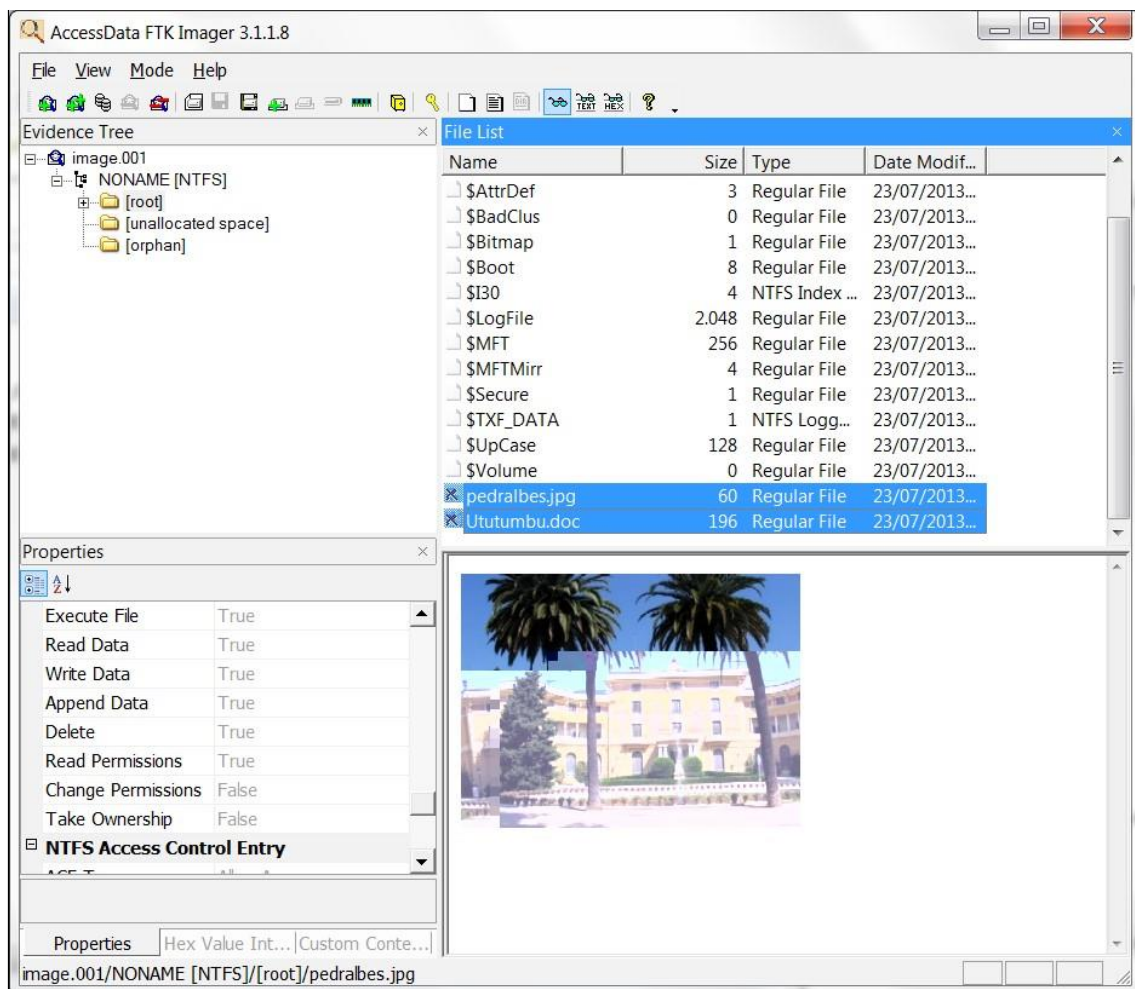
La autorización obtenida asegura que el proceso de análisis se llevó a cabo de manera adecuada y conforme a los protocolos establecidos, respetando en todo momento los derechos y la privacidad de las partes involucradas.

En caso de ser necesario, se encuentran disponibles copias adicionales del documento de autorización para su consulta y verificación por parte de las autoridades pertinentes.

## 9.4 Análisis Forense de las Evidencias y Presentación de los Resultados

### 9.4.1 Identificación de los Archivos Eliminados

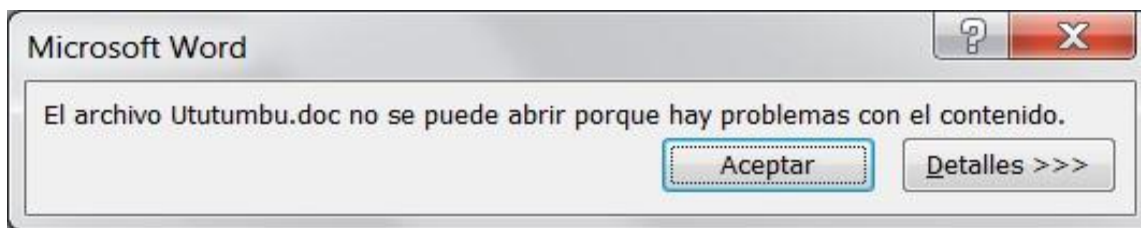
Tras recibir el pendrive y la imagen en formato dd, se procedió a realizar un exhaustivo análisis forense para identificar y recuperar las evidencias digitales relevantes. Se observó que la imagen dd del pendrive contenía dos archivos que habían sido eliminados: una imagen en formato .jpg y un archivo con extensión .doc.



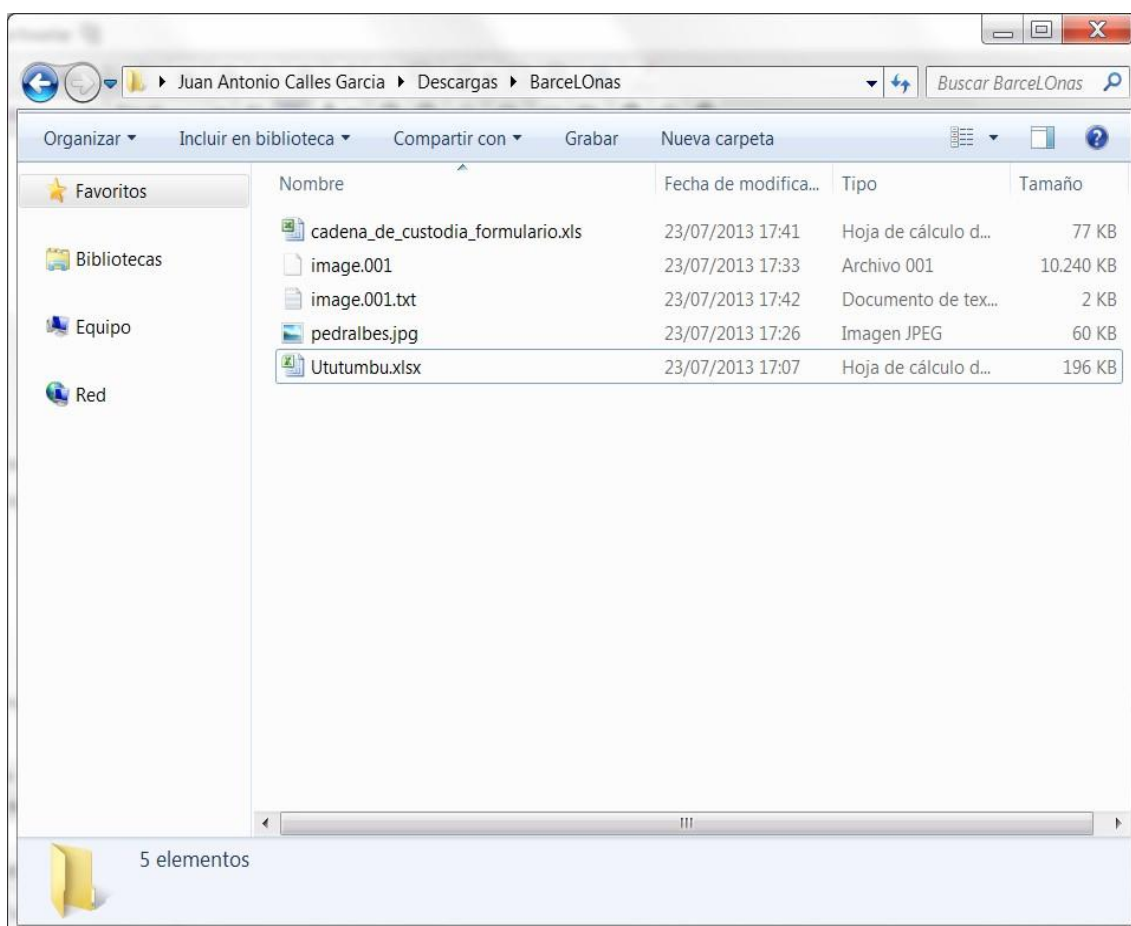
Utilizando herramientas forenses especializadas como FTK Imager, se logró extraer los archivos eliminados y recuperar su contenido para su posterior análisis.

### 9.4.2 Recuperación de Datos Ocultos en Archivos Excel

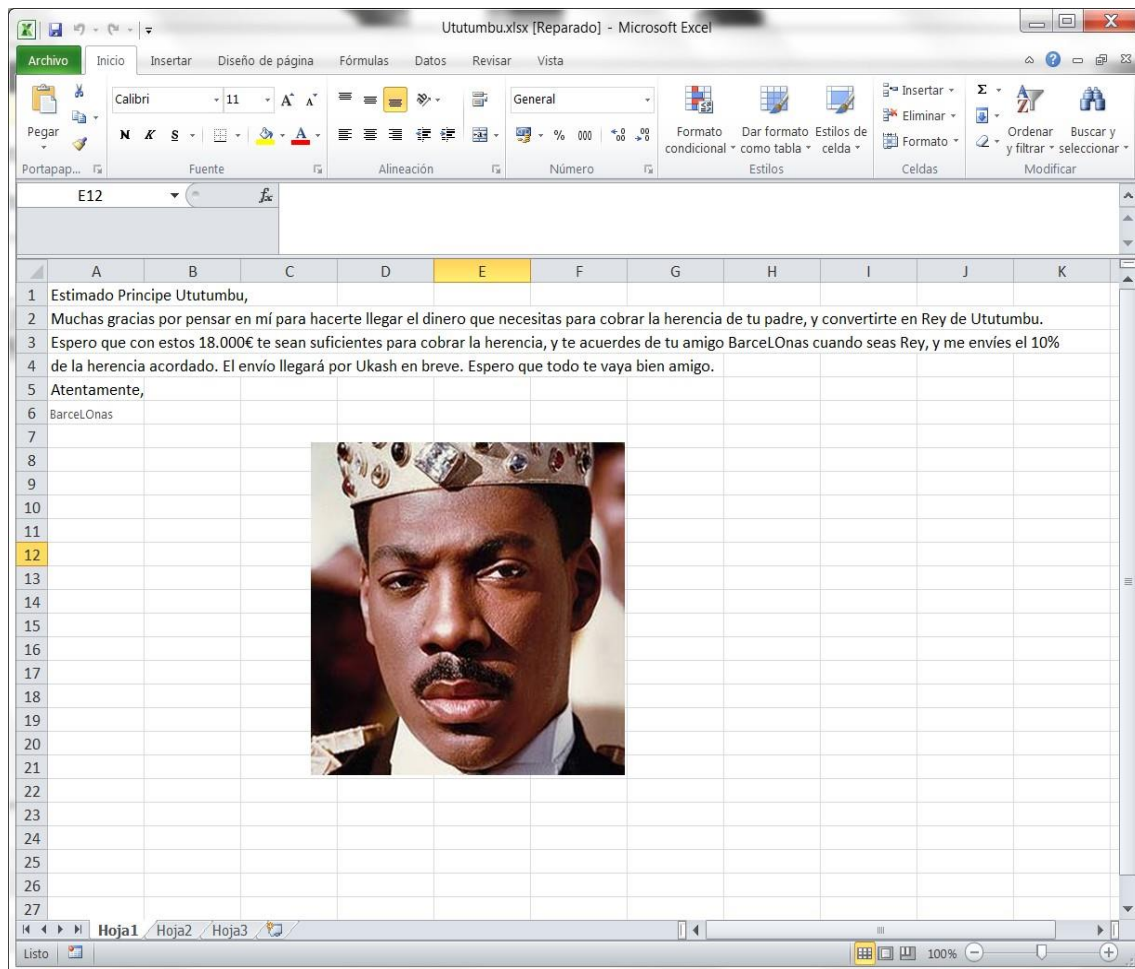




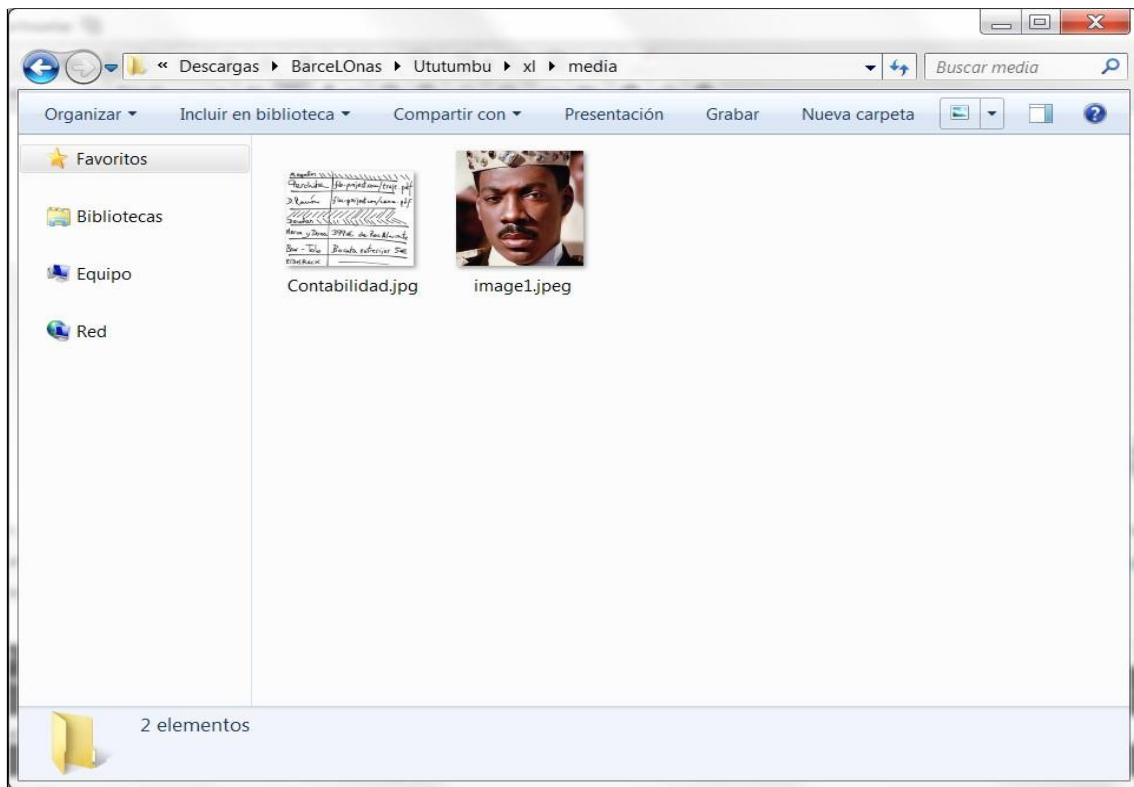
Tras descubrir que uno de los archivos inicialmente identificados como .doc era en realidad un archivo .xlsx, se procedió a su apertura y se encontró que contenía información relevante oculta en la carpeta "xl\media". Allí se encontraba una imagen denominada "Contabilidad.jpg", que proporcionaba detalles adicionales sobre las transacciones financieras del individuo investigado.



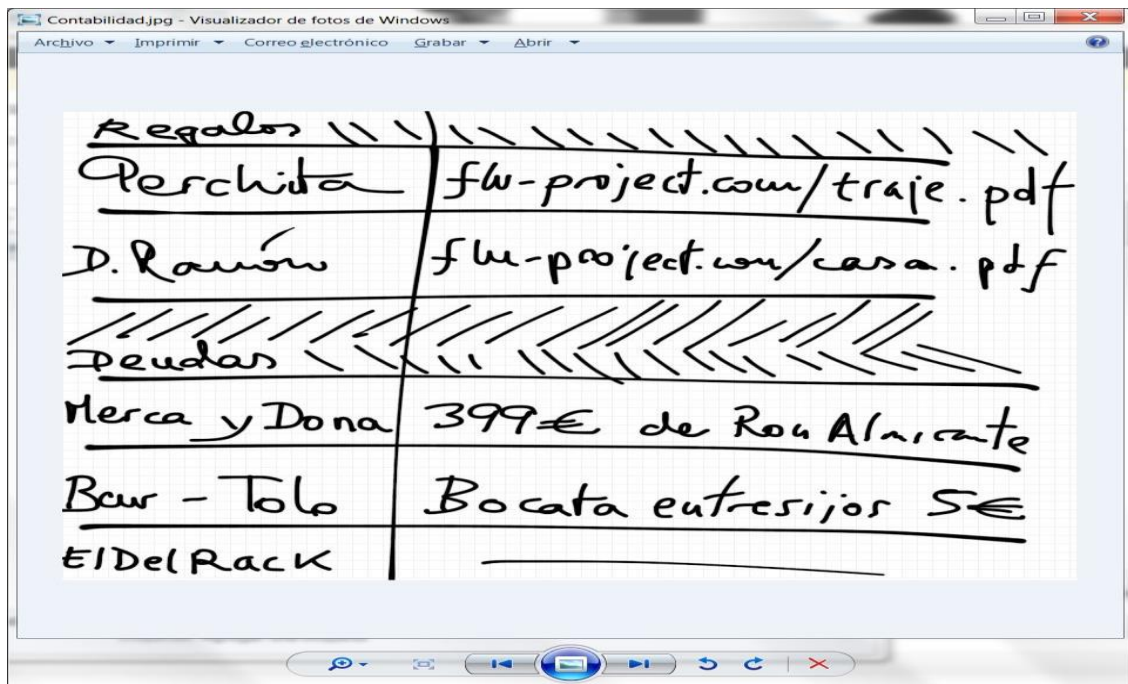
En esta instancia, al tratar de abrir el archivo ututumbu.doc, nos topamos con la imposibilidad de acceso. Tras un análisis, quedó claro que en realidad era un archivo en formato Excel (.xlsx). Por consiguiente, procedimos a modificar la extensión del archivo de .doc a .xlsx.



Ahora está claro el destino de los primeros 18.000€ de los 300.000€ sustraídos por el Señor BarceLOnas: acabaron en manos de un "Príncipe Nigeriano...". Si evitamos hacer clic en "guardar cambios" para que Excel no restaure el archivo xlsx, podemos descomprimirlo, como hicimos en otros casos con archivos de tipo docx, por ejemplo. En los documentos Excel de tipo xlsx, podemos utilizar la carpeta "xl\media" para ocultar imágenes, al igual que hizo nuestro amigo BarceLOnas.



Si accedemos a la imagen "Contabilidad.jpg", nos encontraremos con una refinada "hoja de cálculo".



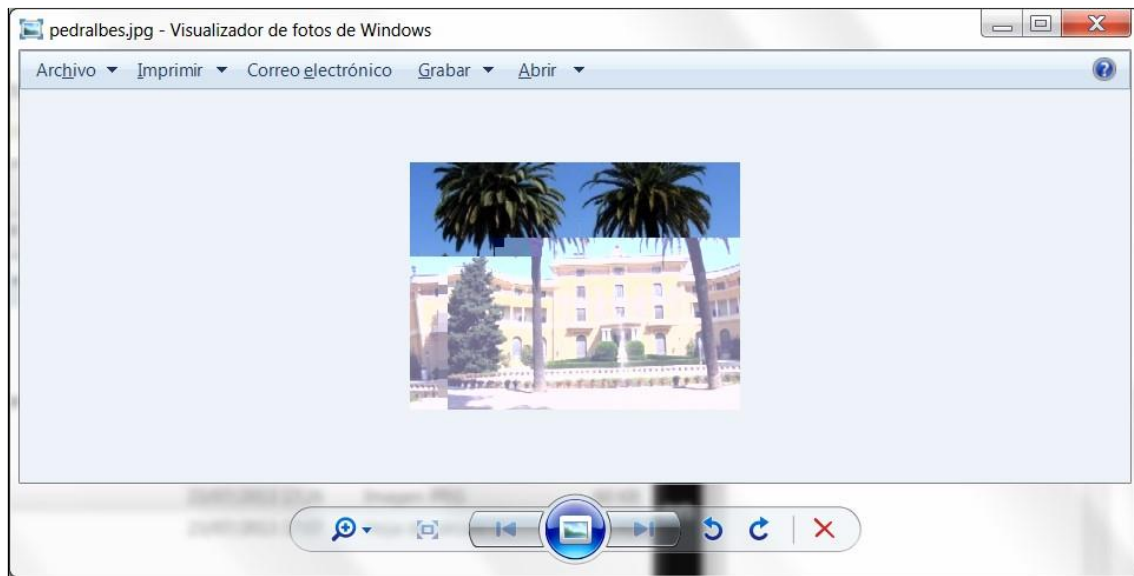
Al parecer, nuestro amigo no solo había acumulado deudas, sino que también había efectuado algunos "regalos" por ahí. Si nos



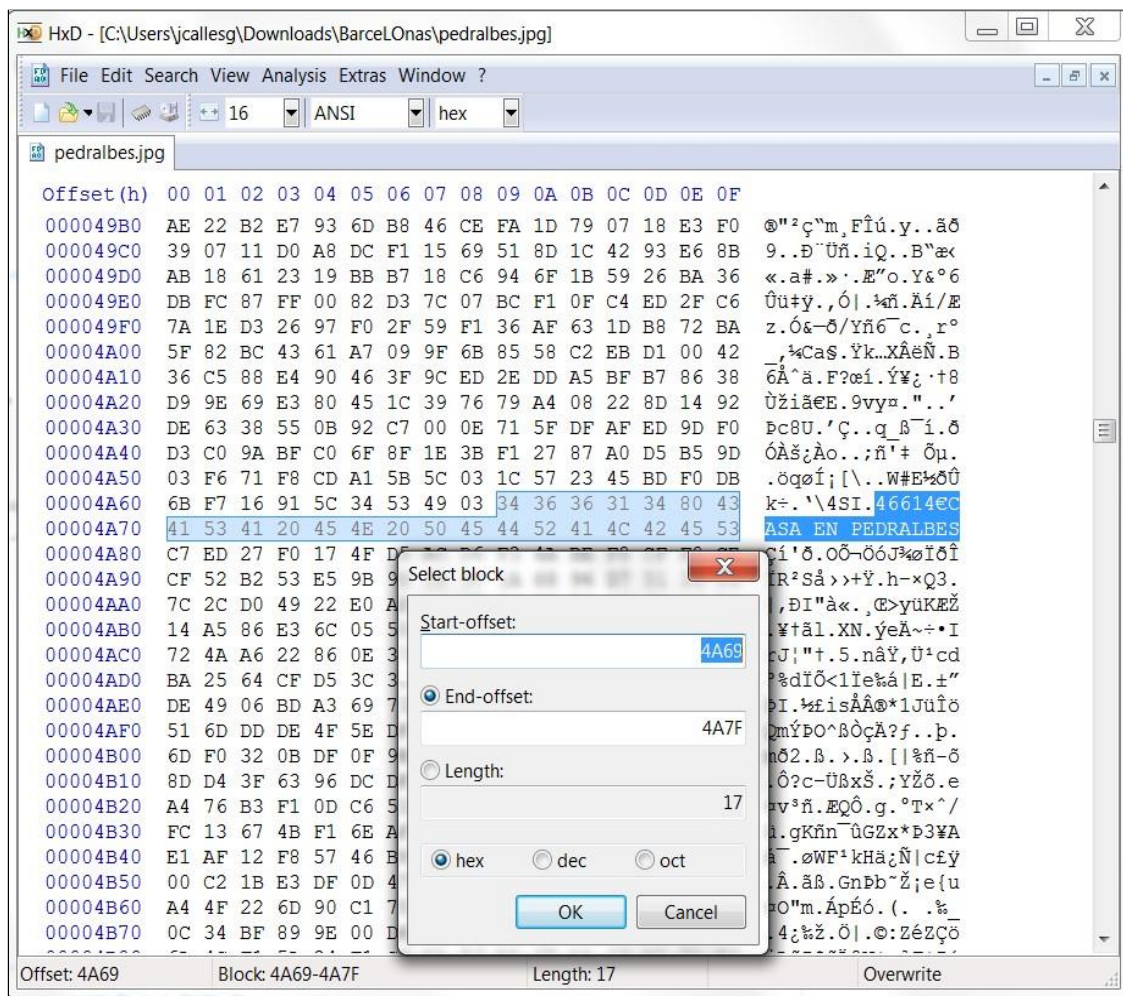
dirigimos hacia los documentos señalados en la hoja, podríamos acceder a los siguientes archivos en formato PDF:



Entonces, al totalizar el valor de la casa y el traje, ya alcanzamos los 253.386€. No obstante, aún nos falta rastrear 46.614€. ¿Dónde podrían encontrarse? Si recordamos, en el pendrive también se encontraba una imagen jpg que había sido eliminada. Al abrirla, se percibe que su aspecto ha sido modificado de forma sospechosa.



Al analizar la imagen mediante un editor hexadecimal en búsqueda de patrones anómalos, nos encontramos con el siguiente texto entre las posiciones 4A69 y 4A7F:



Y ahí se revela el destino del resto del dinero estafado.

Todas las evidencias recuperadas durante el análisis forense fueron debidamente documentadas y presentadas en un informe pericial detallado. Se incluyeron capturas de pantalla, registros de actividades y descripciones detalladas de cada hallazgo, asegurando la integridad y la autenticidad de los datos recabados.

### 9.4.5 Conclusiones del Análisis

Basándose en los hallazgos obtenidos durante el análisis forense, se elaboraron conclusiones fundamentadas sobre las actividades del individuo investigado y el uso indebido de los fondos en cuestión. Estas conclusiones proporcionaron una base sólida para respaldar el caso presentado en el contexto del reto "BarceLOnas, ¿dónde está mi sobre?".

El análisis forense realizado permitió una comprensión más profunda de los eventos relacionados con el caso, brindando claridad y evidencia sustancial para respaldar las reclamaciones y decisiones judiciales pertinentes.

## 10.- CONCLUSIONES

Tras un exhaustivo análisis forense del pendrive proporcionado en el contexto del reto "BarceLOnas, ¿dónde está mi sobre?", se han obtenido varias conclusiones significativas:

**Identificación de Transacciones Financieras Ilícitas:** Se ha demostrado que el individuo investigado, el Señor BarceLOnas, ha realizado transacciones financieras ilícitas, evidenciando un posible mal uso de fondos obtenidos de manera ilegal.

**Manipulación de Archivos para Ocultar Evidencias:** Se ha identificado que el Señor BarceLOnas intentó ocultar pruebas relevantes mediante la eliminación de archivos y la manipulación de formatos de archivo para confundir y obstruir la investigación.

**Descubrimiento de Mensajes Ocultos:** El análisis forense permitió descubrir mensajes ocultos incrustados en archivos de imagen, lo que proporcionó información adicional sobre las actividades delictivas del individuo investigado.

**Presentación de Evidencias Sustanciales:** Se han recopilado y presentado evidencias sustanciales, incluyendo capturas de pantalla, registros de actividades y descripciones detalladas de hallazgos, que respaldan de manera contundente las conclusiones del análisis forense.

En resumen, el análisis forense realizado proporciona una visión clara y detallada de las actividades del Señor BarceLOnas, respaldando así la hipótesis de que ha utilizado fondos ilícitos. Estas conclusiones son fundamentales para la toma de decisiones judiciales y acciones legales posteriores relacionadas con el caso.

## Índice Alfabético

### A

Actividades	10
Actualización	8
acusación	4
acusaciones	4
adquisición	6
Alcance	7
Alfabético	21
almacenamiento	3, 11
Análisis	1, 4, 5, 7, 12, 19
Anexo	11
anómalos	17
ANTECEDENTES	1, 4
Aplicados	1, 4
Aprobación	2
Archivos	1, 6, 9, 10, 11, 12, 13, 19
autenticidad	4, 5, 7, 11, 18
autoridades	11
Autorizaciones	1, 11

### B

BarcelOnas	2, 3, 4, 5, 9, 11, 14, 19, 20
Basándose	19
Base	7

### C

Cadena	1, 9
cálculo	15
calidad	3
cantidad	5
Carta	6
claridad	19
clonación	6
Comarcal	3
Complejidad	5
comprensión	19
Conclusiones	1, 7, 19
concordancia	7, 11
confiables	7
conocimiento	6
consentimiento	11
considerando	6
contaminación	11
Conversaciones	4, 6
correcciones	7
corrupción	5
creación	7
cuestión	3, 8, 11, 19
cuidadosa	10
cumplimiento	4
Custodia	1, 9, 11

### D

dato	5
decisiones	19, 20
Delitos	3, 4, 6
DEPARTAMENTO	2
desarrollo	4
descripciones	18, 20
destino	13, 14, 17
detalles	13
Digitales	1, 2, 8
Dispositivo	5
Documentación	1, 7, 9
documentos	5, 7, 14, 16

### E

Económicos	3, 4, 6
editor	17
efectividad	5
ejercicio	4
elaboración	4
electrónicos	5
eliminación	19
empresa	3
Enrique	2, 3, 4, 6, 9, 11
Entendemos	7
entendimiento	6
ENTIDAD	1, 3
esclarecimiento	3
especialización	7
específica	7
éticos	4
evaluación	6, 7
eventos	19
Evidencias	1, 8, 12, 13, 19, 20
Excel	1, 8, 12, 13, 14
exhaustividad	5
experiencia	3
Exploración	5
extensión	6, 12, 13
Extracción	5, 10

### F

Fichero	6
Firma	2
físico	5
fondos	19, 20
Forense	1, 2, 4, 5, 12
forenses	5, 6, 7, 10, 12
ForenseTech	3, 4
formato	6, 7, 8, 9, 10, 12, 13, 16

formatos \_\_\_\_\_ 19  
FTK \_\_\_\_\_ 6, 10, 12  
FUNDAMENTOS \_\_\_\_\_ 1, 7

**G**

García \_\_\_\_\_ 2, 3, 4, 6, 9, 11

**H**

herramientas \_\_\_\_\_ 5, 6, 10, 12

**I**

Identificación \_\_\_\_\_ 1, 12, 19  
Ilustre \_\_\_\_\_ 3  
Imagen \_\_\_\_\_ 1, 6, 13  
imágenes \_\_\_\_\_ 7, 14  
Imager \_\_\_\_\_ 10, 12  
imparcialidad \_\_\_\_\_ 4, 6  
imposibilidad \_\_\_\_\_ 13  
Incidentes \_\_\_\_\_ 2  
Índice \_\_\_\_\_ 21  
información \_\_\_\_\_ 5, 6, 7, 13, 19  
INFORMATICA \_\_\_\_\_ 2  
informática \_\_\_\_\_ 3, 6  
informático \_\_\_\_\_ 3  
Informe \_\_\_\_\_ 8  
instancia \_\_\_\_\_ 13  
integridad \_\_\_\_\_ 4, 5, 8, 9, 10, 11, 18  
intervenciones \_\_\_\_\_ 3  
INTRODUCCIÓN \_\_\_\_\_ 1, 3  
Investigación \_\_\_\_\_ 2

**J**

Judicial \_\_\_\_\_ 3, 4, 6  
Judiciales \_\_\_\_\_ 3  
juicio \_\_\_\_\_ 3, 4, 6  
Juramos \_\_\_\_\_ 6

**L**

legalidad \_\_\_\_\_ 11  
legitimidad \_\_\_\_\_ 11  
Limitaciones \_\_\_\_\_ 1, 5  
López \_\_\_\_\_ 2

**M**

MANIFESTACIONES \_\_\_\_\_ 1, 6  
Manipulación \_\_\_\_\_ 10, 19  
Martínez \_\_\_\_\_ 2  
materia \_\_\_\_\_ 6, 8  
Mensajes \_\_\_\_\_ 1, 13, 19  
metadatos \_\_\_\_\_ 5  
modificación \_\_\_\_\_ 8  
modificaciones \_\_\_\_\_ 10

Mordor \_\_\_\_\_ 3  
Mordorenses \_\_\_\_\_ 3, 4, 6

**N**

necesaria \_\_\_\_\_ 7  
Nigeriano \_\_\_\_\_ 14  
numerosas \_\_\_\_\_ 3

**O**

objetividad \_\_\_\_\_ 4  
Obtención \_\_\_\_\_ 4  
Ocultos \_\_\_\_\_ 1, 12, 13, 19  
opiniones \_\_\_\_\_ 6

**P**

pantalla \_\_\_\_\_ 18, 20  
patrones \_\_\_\_\_ 17  
PDF \_\_\_\_\_ 16  
Pendrive \_\_\_\_\_ 6  
pericia \_\_\_\_\_ 4  
peritajes \_\_\_\_\_ 3  
Peritos \_\_\_\_\_ 3  
Policía \_\_\_\_\_ 3, 4, 6  
posibilidad \_\_\_\_\_ 11  
posteriores \_\_\_\_\_ 20  
PRESENTACIÓN \_\_\_\_\_ 1, 3  
Preservación \_\_\_\_\_ 11  
presuntos \_\_\_\_\_ 3  
Príncipe \_\_\_\_\_ 14  
privacidad \_\_\_\_\_ 11  
Procedimientos \_\_\_\_\_ 1, 4, 6  
Project \_\_\_\_\_ 4  
protocolos \_\_\_\_\_ 7, 10, 11  
puesto \_\_\_\_\_ 6

**R**

realización \_\_\_\_\_ 3  
recepción \_\_\_\_\_ 8, 10  
reclamaciones \_\_\_\_\_ 19  
Recopilación \_\_\_\_\_ 1, 13  
Recuperación \_\_\_\_\_ 1, 5, 8, 12  
regalos \_\_\_\_\_ 15  
Registro \_\_\_\_\_ 10  
relación \_\_\_\_\_ 6  
relevancia \_\_\_\_\_ 3  
relevantes \_\_\_\_\_ 4, 5, 6, 7, 12, 19  
representantes \_\_\_\_\_ 4, 6  
responsabilidad \_\_\_\_\_ 3  
resto \_\_\_\_\_ 17  
Restricciones \_\_\_\_\_ 5  
Resultados \_\_\_\_\_ 1, 12  
Revisión \_\_\_\_\_ 2

**S**

sección	7
secretario	6
seguridad	6
Señor	2, 4, 14, 19, 20
servicios	3
sospechosa	16
supervisión	3
Sustanciales	20

**T**

técnicas	5
técnico	4
TECNOLOGICO	2

tecnológicos	7
tráfico	3
trayectoria	3

**U**

ubicación	11
Unidad	3, 4, 6
Utilizando	12

**V**

veracidad	9
verídicas	6
Verificación	4, 5, 10