

INFORME PERICIAL INFORMÁTICO

Autenticidad e integridad de una conversación de WhatsApp
Documento de ejemplo con datos ficticios

N.º de expediente	IP-2026-0147
Fecha de emisión	5 de junio de 2026
Procedimiento	Juicio ordinario por reclamación de cantidad
Órgano	Juzgado de Primera Instancia de Madrid
Solicitante	D.ª Laura Gómez Ferrer, a través de su letrada, D.ª Marta Sanz Olivares
Perito	D. Nombre Apellidos (perito de ejemplo), Máster en Informática Forense y Delitos Informáticos
Entidad	IP Peritos Judiciales, S.L. (IP Peritos Informáticos), C/ General Pardiñas 108, 28006 Madrid

Aviso. Este documento muestra la estructura y el nivel de detalle de un informe pericial informático. Todos los nombres, números de teléfono, identificadores, fechas y valores hash son ficticios. No tiene validez probatoria ni puede usarse como modelo para presentar ante un juzgado: un informe pericial solo es válido si lo elabora, firma y ratifica un perito.

Índice

1. Juramento y declaración de tachas	2
2. Objeto y alcance	2
3. Antecedentes	2
4. Evidencias y cadena de custodia	3
5. Metodología, normas y herramientas	3
6. Análisis y resultados	4
7. Limitaciones	5
8. Conclusiones	5
9. Firma y anexos	5

1. Juramento y declaración de tachas

Juramento o promesa (art. 335.2 LEC). El perito que suscribe manifiesta, bajo juramento o promesa de decir verdad, que ha actuado y, en su caso, actuará con la mayor objetividad posible, tomando en consideración tanto lo que pueda favorecer como lo que sea susceptible de causar perjuicio a cualquiera de las partes, y que conoce las sanciones penales en las que podría incurrir si incumpliere su deber como perito.

Declaración de tachas (art. 343 LEC). El perito declara que no concurre en él ninguna de las causas de tacha previstas en la ley: no tiene parentesco con las partes ni con sus abogados, no tiene interés directo o indirecto en el asunto y no mantiene relación de dependencia, amistad íntima o enemistad con ninguno de ellos.

Independencia. Los honorarios de este informe no dependen del resultado del análisis ni del fallo del procedimiento.

2. Objeto y alcance

El objeto de la pericia es determinar si la conversación de WhatsApp aportada por la solicitante es auténtica, íntegra y no ha sido manipulada. En concreto, se pide responder a tres preguntas:

- 1. ¿La conversación existe en la base de datos de WhatsApp del teléfono de la solicitante?
- 2. ¿Los mensajes, sus fechas y sus remitentes coinciden con las capturas de pantalla aportadas?
- 3. ¿Hay indicios de eliminación, edición o alteración de mensajes en el periodo analizado?

El análisis se limita al terminal de la solicitante y a la conversación con el contacto identificado como «Javier Ruiz», entre el 3 de febrero y el 28 de abril de 2026.

3. Antecedentes

La solicitante reclama a D. Javier Ruiz Montes la devolución de un préstamo personal de 4.800 €. Según su letrada, el demandado reconoció la deuda por WhatsApp el 14 de marzo de 2026, y la solicitante conservó capturas de pantalla de esa conversación.

Como la otra parte puede impugnar unas simples capturas, la letrada solicita un análisis forense del teléfono que acredite el origen y la integridad de los mensajes. El 20 de mayo de 2026 se acepta el encargo y se acuerda la entrega del terminal en la sede de IP Peritos Informáticos.

4. Evidencias y cadena de custodia

Se ha analizado una única evidencia: el teléfono móvil de la solicitante, entregado en mano y desbloqueado por ella para la extracción.

Evidencia	EV-01
Dispositivo	Apple iPhone 13 (modelo A2633), color azul
Sistema operativo	iOS 17.5.1
IMEI	35 000000 000000 0 (ficticio)
Número asociado	+34 600 000 112 (ficticio)
Estado	Encendido, sin daños visibles, batería al 64 %

Registro de custodia

Fecha y hora	Actuación	Responsable
22/05/2026 10:05	Recepción del terminal y firma del acta de entrega por la solicitante	Perito
22/05/2026 10:12	Activación del modo avión para aislar el terminal de la red	Perito
22/05/2026 10:20	Inicio de la extracción forense	Perito
22/05/2026 11:47	Fin de la extracción y cálculo del hash de la imagen	Perito
22/05/2026 12:02	Devolución del terminal a la solicitante y firma del acta	Perito

Valores hash (SHA-256)

Elemento	Hash SHA-256
Imagen de la extracción	9f2c4a7e1b3d58c6a0e4f7b2d9c1e8a35b6f0d2c7e4a9b1f3c8d5e2a7b0f6c41
Base de datos ChatStorage.sqlite	4e7a1c9d2f5b8e03c6a9d2f71b4e8c05a3d6f9b2e5c8a1d47f0b3e6a9c2d5f81
Transcripción exportada (Anexo C)	d1e4b7a0c3f6e9b25a8d1c4f7e0a3b6d9c2f5e8a1b4d7c0e3f6a9d2c5e8b1f47

La imagen se conserva en un soporte cifrado bajo custodia del perito. Cualquier copia posterior puede compararse con estos valores para comprobar que no se ha alterado.

5. Metodología, normas y herramientas

El trabajo sigue las fases de identificación, adquisición, preservación, análisis y presentación de evidencias digitales. Se han aplicado estas normas:

- **UNE 197001:2019**, criterios generales para la elaboración de informes periciales.
- **UNE 197010:2015**, criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC).
- **UNE-EN ISO/IEC 27037**, directrices para la identificación, recogida, adquisición y preservación de evidencias digitales.
- **UNE 71506:2013**, metodología para el análisis forense de las evidencias electrónicas.

Herramientas utilizadas

Herramienta	Uso
Cellebrite UFED 4PC	Extracción lógica avanzada del terminal
Cellebrite Physical Analyzer	Decodificación y revisión de la base de datos de WhatsApp
DB Browser for SQLite	Consulta directa de las tablas de mensajes
sha256sum	Cálculo y verificación de los valores hash

La extracción se ha hecho con el terminal en modo avión, para evitar que entren mensajes nuevos o se sincronicen cambios durante el proceso. El análisis se ha realizado siempre sobre una copia de la imagen, nunca sobre el original.

6. Análisis y resultados

6.1 Localización de la conversación

La conversación figura en la base de datos ChatStorage.sqlite, dentro del contenedor de WhatsApp del terminal. Está asociada al identificador 34600000187@s.whatsapp.net, que corresponde al número +34 600 000 187 (ficticio), guardado en la agenda como «Javier Ruiz».

En el periodo analizado constan 47 mensajes: 24 enviados por la solicitante y 23 recibidos del contacto.

6.2 Cotejo con las capturas aportadas

Se han comparado las 6 capturas de pantalla aportadas con los registros de la tabla ZWAMESSAGE. Los tres mensajes clave del 14 de marzo de 2026 son estos:

Hora (Madrid)	Remitente	Texto	Valor ZMESSAGEDATE	Coincide
21:38:02	Solicitante	«Javi, ¿cuándo me puedes devolver los 4.800 € del préstamo?»	795213482	Sí
21:42:17	Contacto	«Lo sé, te debo los 4.800. Te los devuelvo antes del verano, palabra.»	795213737	Sí
21:43:05	Solicitante	«Vale, gracias. Lo dejamos así.»	795213785	Sí

WhatsApp guarda la fecha en segundos desde el 1 de enero de 2001 (UTC). Por ejemplo, el valor 795213737 equivale al 14/03/2026 a las 20:42:17 UTC, es decir, a las 21:42:17 en Madrid (UTC+1, antes del cambio al horario de verano).

Los textos, horas y remitentes de las 6 capturas coinciden con los registros de la base de datos.

6.3 Integridad de la conversación

Se han hecho cuatro comprobaciones para detectar posibles manipulaciones:

- **Orden interno:** el campo de ordenación de la conversación es correlativo del 1 al 47, sin saltos.
- **Mensajes eliminados o editados:** no consta ningún mensaje eliminado para todos ni editado en el periodo.
- **Registros borrados:** el análisis de las páginas libres de la base de datos y del fichero de registro (WAL) no muestra restos de mensajes borrados de esta conversación.
- **Coherencia temporal:** las fechas son consecutivas y coherentes con los estados de entrega y lectura de cada mensaje.

7. Limitaciones

- Solo se ha analizado el terminal de la solicitante. No se ha tenido acceso al teléfono del contacto ni a los servidores de WhatsApp.
- El análisis acredita qué cuenta de WhatsApp envió cada mensaje, no qué persona física lo escribió. La identidad de quien usaba el número es una cuestión que corresponde valorar al tribunal.
- Las conclusiones se refieren al estado del terminal en la fecha de la extracción, el 22 de mayo de 2026.

8. Conclusiones

A la vista del análisis realizado, el perito concluye:

1. **La conversación existe en el terminal.** Los 47 mensajes entre la solicitante y el número +34 600 000 187 figuran en la base de datos original de WhatsApp del iPhone analizado.
2. **Las capturas son fieles.** Los textos, fechas, horas y remitentes de las 6 capturas aportadas coinciden con los registros de la base de datos.
3. **No hay indicios de manipulación.** No constan mensajes eliminados, editados ni insertados, y el orden interno de la conversación es completo y coherente.
4. **El mensaje clave está acreditado.** El 14 de marzo de 2026, a las 21:42:17 (hora de Madrid), el número +34 600 000 187 envió el mensaje: «Lo sé, te debo los 4.800. Te los devuelvo antes del verano, palabra.»

El perito queda a disposición del juzgado para ratificar este informe y aclarar cualquier extremo en el acto del juicio.

9. Firma y anexos

En Madrid, a 5 de junio de 2026.

D. Nombre Apellidos (perito de ejemplo)
Perito informático · IP Peritos Informáticos

Anexos

- **Anexo A.** Actas de entrega y devolución del terminal, firmadas por la solicitante y el perito.
- **Anexo B.** Informe de extracción generado por Cellebrite UFED, con los valores hash.
- **Anexo C.** Transcripción completa de los 47 mensajes, con fecha, hora y remitente.
- **Anexo D.** Capturas de pantalla aportadas por la solicitante, numeradas del 1 al 6.
- **Anexo E.** Consultas SQL ejecutadas sobre la base de datos y sus resultados.
- **Anexo F.** Currículum y acreditación de la formación del perito.

Normativa citada: Ley 1/2000, de Enjuiciamiento Civil (arts. 335, 336 y 343); UNE 197001:2019; UNE 197010:2015; UNE-EN ISO/IEC 27037; UNE 71506:2013.