

INFORME TÉCNICO

ANÁLISIS DE
EVIDENCIA DIGITAL

NÚMERO DE SOLICITUD
47633686

NÚMERO DE LEGAJO
M-005766/2022

UNIDAD FISCAL
UNIDAD FISCAL DE INVESTIGACION Y
ENJUICIAMIENTO ESP EN DELITOS C/LA
PROPIEDAD Y C/LA INTEG FISICA

EXAMINADOR
Gustavo Fabian Luna

DIRECCION
Prosecretario Edgar J. Aranda



MPF

DEPARTAMENTO DE INFORMÁTICA FORENSE
EQUIPO CIENTÍFICO DE INVESTIGACIONES FISCALES
MINISTERIO PÚBLICO FISCAL DE TUCUMÁN

Introducción

Objetivos

Mantener la cadena de custodia de los elementos probatorios, desde su recepción hasta su entrega, garantizando la integridad de los datos adquiridos.

Estandarizar el conjunto de actividades y tareas a desarrollar, estableciendo criterios unificados de trabajo, y mayor seguridad.

Marco legal

El informe técnico tiene como referencia básica el Código Procesal de Tucumán, la ley nacional de protección de datos personales, la ley de propiedad intelectual y la ley de delitos informáticos. Ante la ausencia de regulación específica se ha tenido especialmente en cuenta la normativa constitucional y los aportes provenientes de líneas jurisprudenciales firmes y del derecho comparado.

Roles

El rol del director consiste en realizar el control de calidad de los diferentes informes y procesos llevados a cabo, garantizando que se respeten los objetivos y marco legal del presente informe.

El rol del examinador es el de recolectar, identificar, preparar, adquirir, extraer, analizar y/o presentar la evidencia, según sea necesario. Sin perjuicio de ello, existen examinadores especializados en diferentes áreas.

Técnicas de estudio

El trabajo realizado ha utilizado el modelo PURI (Proceso Unificado de Recuperación de Información), el cual es un proceso teórico de las tareas involucradas en la aplicación de técnicas y herramientas forense disponibles. La extracción de evidencias en esta rama podría diagramarse como una composición de etapas, no necesariamente todas imprescindibles, representado por el siguiente esquema.

Relevamiento e identificación

Identificación de dispositivos, del caso, de la documentación legal y los participantes durante cualquier etapa del desarrollo del informe.

Preparación y adquisición

Preparación del lugar del trabajo, evitando contaminantes digitales y/o físicos; y la posterior adquisición de los datos contenidos en los dispositivos por intermedio de los programas y herramientas disponibles en este Departamento de Informática Forense.

Extracción y análisis

Extracción de los datos adquiridos y su validación, realizando un examen general y específico de acuerdo a los presupuestos indicados por el solicitante. Se realizará una interpretación de la evidencia, dentro del marco de incumbencia y en los términos de los puntos de pericia que hubieren sido indicados.

Presentación

Redacción del informe, la presentación de la evidencia obtenida, la forma de su preservación, entre otros factores. El mismo será generado digitalmente bajo constancia de doble firma electrónica, con el fin de asegurar la integridad de su contenido. Dicha firma electrónica tendrá un cifrado con algoritmo clave RSA 1024-bits, la cual cumple con los requisitos de validez del artículo 1 y 9 de la Ley Nacional n° 25.506.

INFORME TÉCNICO DIGITAL

1. FASE DE RELEVAMIENTO E IDENTIFICACIÓN

1.1. Identificación del caso

Turno	08/02/23 14:00
Lugar	San Miguel de Tucumán, Tucumán, Argentina
Oficina	Departamento de Informática Forense, Equipo Científico de Investigaciones Fiscales, Ministerio Público Fiscal de Tucumán
Director	Lic. Edgar Jesús Aranda, Prosecretario.
Examinador	Gustavo Fabián Luna
Unidad fiscal	UNIDAD FISCAL DE INVESTIGACION Y ENJUICIAMIENTO ESP EN DELITOS C/LA PROPIEDAD Y C/LA INTEG FISICA
Caratula	MACIAS JOSE ALEJANDRO S/ HOMICIDIO CULPOSO AGRAVADO (Art. 84 bis 1° y 2° Párrafo C.P.) VICT GONZALEZ JOHANA ELIZABETH y CRUZ EMILSE ROMINA
Número de legajo	M-005766/2022
Número de gestión	47633686
Objeto	Análisis de evidencia digital
Fases	1.- Relevamiento e identificación 2.- Extracción y análisis 3.- Presentación

1.2. Identificación de documentación (legal y técnica)

Se detallará a continuación la autorización remitida a este Departamento para la realización del presente informe. En caso que la evidencia física o digital recepcionada no coincida con la obrante en dicha autorización, se suspenderá el proceso de adquisición sobre los elementos afectados.

Autorización	Decreto
Fecha	8/2/2023
Firma	García Mónica Andrea
Carácter	Fiscal
Oficina	Unidad Fiscal interviniente

1.3. Participantes

Nombre y apellido	Carácter/Observaciones
Gustavo Fabián Luna	Examinador. Departamento de Informática Forense

1.4. Puntos de análisis

El informe se limitará a lo expresamente establecido por la Unidad Fiscal, siempre que la función y labor de este Departamento este comprendida dentro del marco legal correspondiente.

Punto n°	Descripción
01.-	De la información extraída y recuperada de los teléfonos celulares secuestrados (línea N° 3863455623 y N° 3865564480), elabore informe de análisis de evidencia digital tomando como base los siguientes puntos de pericia: Determine si existieron comunicaciones de dichas líneas telefónicas entre sí (esto es a través de llamadas, SMS, WhatsApp, Facebook, Instagram, Telegram), y a su vez entre esas líneas y los teléfonos N° 3863581588, 3863408975 y 3813536045, entre la fecha 30/10/2022 al 08/11/2022, detallando su contenido.
02.-	Recuperación de datos, imágenes que fueran borradas de los equipos celulares secuestrados.
03.-	Toda otra información de relevancia a la causa, haciéndose constar que se investiga un siniestro vial ocurrido el día 30/10/2022 en la ciudad de Monteros, específicamente en la Ruta 325 e intersección de calle Cabildo.

1.5. Relevamiento de la evidencia

En caso que el objeto del presente informe sea trabajar sobre evidencia física (dispositivos tales como teléfonos celulares, de almacenamiento masivo, etc.) se hará en esta etapa una inspección visual de cada uno, dejándose debida constancia de la forma en que fueron aportados (en sobre, en caja, con firmas, abrochados, etc.) y en el orden como aparecen en el protocolo de identificación y cadena de custodia. Todos los objetos que no se encuentren detallados en la autorización judicial, o que no resultan pertinentes, son considerados no procedentes, y serán devueltos a la Unidad Fiscal en las mismas condiciones que fueron presentados junto al resto de los dispositivos, una vez finalizada la labor forense.

En caso de ser evidencia digital, se procederá a detallar la misma con su correspondiente número de hash.

A continuación, procederemos a analizar los datos adquiridos oportunamente. Para ello, se procederá a descargar la misma del servidor donde se encuentra alojada, y se detallará su nombre, tamaño y hash.

Los datos para analizar corresponden al dispositivo **Teléfono celular, marca Xiaomi, modelo M1903C3EG (Redmi 7A), IMEI físico n° no visible, IMEI electrónico 1 n° 866679049934924, IMEI electrónico 2 n° 866679049934932.**

FIN DE LA FASE DE RELEVAMIENTO E IDENTIFICACION

2. FASE DE EXTRACCIÓN Y ANÁLISIS

En esta fase, se realizará la extracción de la evidencia digital obtenida previamente en los dispositivos objeto de este informe. Se registrará los detalles específicos de la misma, con su número de hash y programas utilizados a tales efectos

2.1 Preparación del lugar de trabajo

Se ha retirado al personal ajeno a este departamento, asegurándose la privacidad en el manejo de los datos sensibles.

El sistema operativo utilizado durante la confección de este informe es Windows 10 Pro, versión 21H1. Los programas que serán utilizados se detallarán a continuación.

N°	Programa	Versión
1	CellebriteReader	7.57.0.51
2	HashMyFiles	V2.42

2.2 Proceso de extracción

Se procedió a verificar el hash de imagen del archivo

Ítem	Nombre del archivo y extensión	Tamaño en bytes	Hash (MD5)
1	Telefono_2022-12-26_Informe.ufdr	23.799.017.181	60e9ea01307e4aafc28a2649c7659787

Se procedió a la apertura del software forense Cellebrite Reader a fin de extraer los datos contenidos en dicha imagen

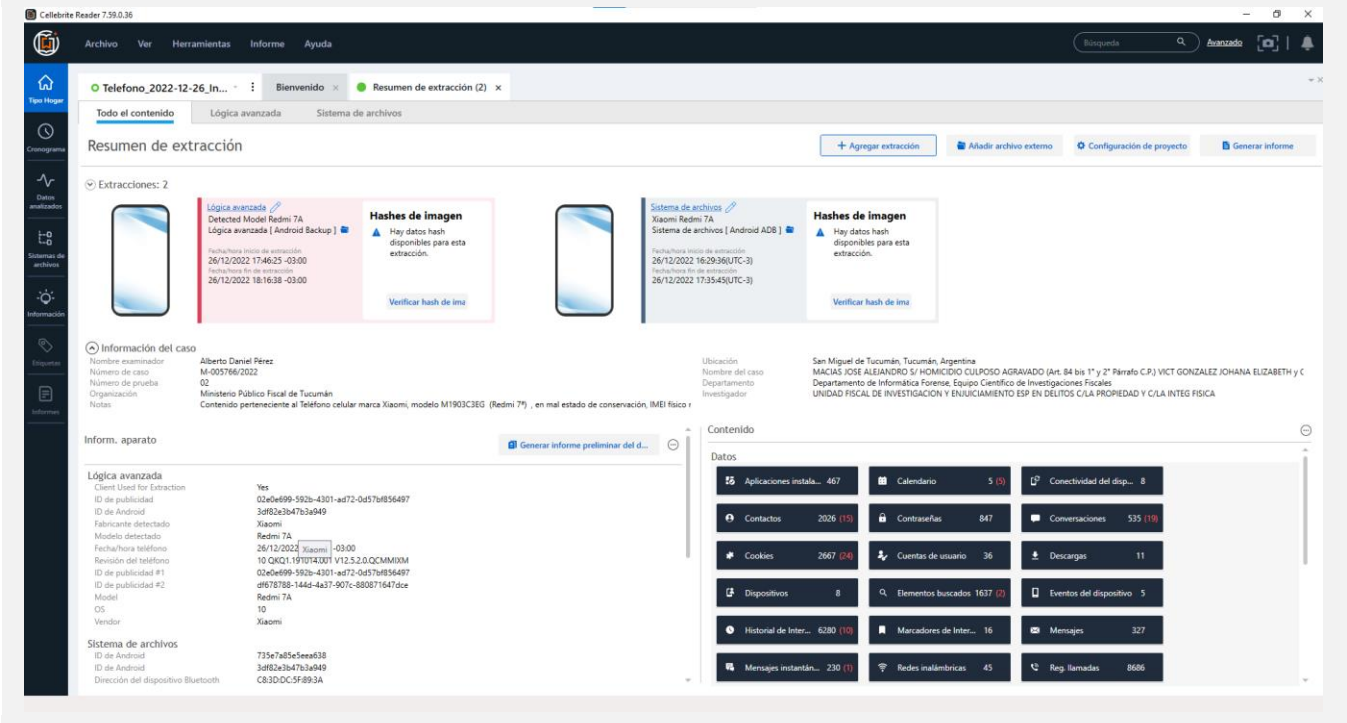


Imagen 1. -

2.3 Proceso de análisis

Cuentas de usuario

De haber ingresado por directorio del software forense, en la carpeta Cuentas de usuario, se establece que cuenta con 36 elementos, destacando los siguientes:

01	José Macías	joo.ale333@gmail.com	
02	José Macías	joo.ale333@gmail.com	104875335561571961642
03	José Macías	joo.ale333@gmail.com	
04	José Macías	543863455623@s.whatsapp.net	Mobile 543863455623 Google Drive Account joo.ale333@gmail.com
05	REGINA EUGENIA MACIAS	macias.regina@colegioconsolacionconcepcion.edu.ar	
06	REGINA EUGENIA MACIAS	macias.regina@colegioconsolacionconcepcion.edu.ar	112828623144680718499
07	REGINA EUGENIA MACIAS	macias.regina@colegioconsolacionconcepcion.edu.ar	



Nombre: José Macías

Nombre de usuario: 543863455623@s.whatsapp.net

Contraseña:

Hora de creación:

Tipo de servicio:

Dirección del servidor:

Origen: WhatsApp

Extracción: Sistema de archivos

Archivo de origen: Xiaomi_Redmi 7A.zip/data/data/com.whatsapp/shared_prefs/registration.RegisterPhone.xml : 0x199 (Tamaño: 708 bytes)
Xiaomi_Redmi 7A.zip/data/data/com.whatsapp/shared_prefs/startup_prefs.xml : 0x1E3 (Tamaño: 616 bytes)
Xiaomi_Redmi 7A.zip/data/data/com.whatsapp/files/

Otras entradas

Mobile 543863455623

Google Drive Account joo.ale333@gmail.com

Organizaciones

Dirección

Notas

Información adicional

Origen

Imágenes

Detalles

Eventos (1)



Guardar

Nombre: me.jpg

Tipo: Imágenes

Tamaño (bytes): 104946

Ruta: Xiaomi_Redmi 7A.zip/data/data/com.whatsapp/files/me.jpg

Creado:

Último acceso:

Modificado: 6/11/2022 13:36:28(UTC+0)

Cambiado:

Eliminado:

Extracción: Sistema de archivos

MD5: f2099d5a78fec00c35ac2ba7e6fe43c5

Archivo de origen: me.jpg

Mapa

Posición:

Dirección:

Dirección del mapa:

Imagen 2. -

Contactos

De haber ingresado por directorio del software forense, en la carpeta Contactos, se establece que cuenta con 2026 elementos. De haber filtrado el abonado 3865564480, se obtuvo lo siguiente:

#					↑ Nombre ▾	Estados de intera	Organizaciones ▾	Teléfonos ▾	Mensajes ▾	Otras entradas ▾
1					carlos Aldonate	Blocked		General +5493865564480		WhatsApp User Id

Imagen 3. -



Nombre: carlos Aldonate

Descripción del dispositivo:

Origen: WhatsApp

Cuenta: 543863455623@s.whatsapp.net

Grupo:

Creado:

Modificado:

Fecha del último contacto:

Número de contactos:

Extracción: Sistema de archivos

Archivo de origen: Xiaomi_Redmi 7A.zip/data/data/com.whatsapp/databases/wa.db : 0x3C660 (Tabla: wa_contacts, wa_block_list; Tamaño: 593920 bytes)
Xiaomi_Redmi 7A.zip/data/data/com.whatsapp/files/Avatars/5493865564480@s.whatsapp.net.j : 0x0 (Tamaño: 3607 bytes)

Estados de interacción

Bloqueado

Información adicional

About

Detalles

General +5493865564480

WhatsApp User Id 5493865564480@s.whatsapp....

Origen

Imágenes

Detalles

Eventos (2)



Guardar

Nombre: 5493865564480@s.whatsapp.net.j

Tipo: Imágenes

Tamaño (bytes): 3607

Ruta: Xiaomi_Redmi 7A.zip/data/data/com.whatsapp/files/Avatars/5493865564480@s.whatsapp.net.j

Creado:

Último acceso:

Modificado: 1/11/2019 01:08:54(UTC+0)

Cambiado:

Eliminado:

Extracción: Sistema de archivos

MD5: 248d22fff7d99082cc6b40d87648c8c

Archivo de origen: 5493865564480@s.whatsapp.net.j

Mapa

Posición:

Dirección:

Dirección del mapa:

Imagen 4. -

De haber filtrado el número de abonado 3863581588, se encontró lo siguiente:

#					↑ Nombre ▾	Estados de intera	Organizaciones ▾	Teléfonos ▾	Mensajes ▾	Otras entradas ▾
1					Acosta Mario			General +5493863581588 General +5493863581588		
2					Mario Acosta			Móvil +54 9 3863 58-1588 Enviar mensaje a +54 9... Móvil +5493863581588		
3					Mario Acosta			General +5493863581588		WhatsApp User Id

Imagen 5. -

» Contacto

Ir a ▾



Nombre:

Mario Acosta

Descripción del dispositivo:

Origen:

WhatsApp

Cuenta:

543863455623@s.whatsapp.net

Grupo:

Creado:

Modificado:

Fecha del último contacto:

Número de contactos:

Extracción:

Sistema de archivos

Archivo de origen:

Xiaomi_Redmi 7A.zip/data/data/com.whatsapp/databases/wa.db : 0x8A9B0 (Tabla: wa_contacts; Tamaño: 593920 bytes)

Xiaomi_Redmi 7A.zip/data/data/com.whatsapp/files/Avatars/5493863581588@s.whatsapp.net.j : 0x0 (Tamaño: 3952 bytes)

Estados de interacción

Información adicional

About

¡Hola! Estoy usando WhatsApp.

Detalles

General

+5493863581588

WhatsApp User Id

5493863581588@s.whatsapp....

Organizaciones

Direcciones

Etiquetas del usuario

Notas

Origen

Imágenes

Ir a ▾

Detalles

Eventos (2)



Guardar

Nombre:

5493863581588@s.whatsapp.net.j

Tipo:

Imágenes

Tamaño (bytes):

3952

Ruta:

Xiaomi_Redmi 7A.zip/data/data/com.whatsapp/files/Avatars/5493863581588@s.whatsapp.net.j

Creado:

Último acceso:

Modificado:

19/11/2021 14:42:22(UTC+0)

Cambiado:

Eliminado:

Extracción:

Sistema de archivos

MD5:

6b847ed8ef378a7e6cf2934a34b21296

Archivo de origen:

5493863581588@s.whatsapp.net.j

Mapa

Posición:

Dirección:

Dirección del mapa:

Imagen 6. -

#					↑ Nombre ▾	Estados de intera	Organizaciones ▾	Teléfonos ▾	Mensajes ▾	Otras entradas ▾
1					Campero Chueco			Mobile +54 9 3863 40-8... Enviar mensaje a +54 9... Mobile +5493863408975		
2					Campero Chueco			General +5493863408975		WhatsApp User Id
3					Chueco Campero			Mobile +5493863408975 Mobile +5493863408975		

Imagen 7. -

» Contacto

Ir a ▾



Nombre:

Campero Chueco

Descripción del dispositivo:

Origen:

WhatsApp

Cuenta:

543863455623@s.whatsapp.net

Grupo:

Creado:

Modificado:

Fecha del último contacto:

Número de contactos:

Extracción:

Sistema de archivos

Archivo de origen:

Xiaomi_Redmi 7A.zip/data/data/com.whatsapp/databases/wa.db : 0x6498D (Tabla: wa_contacts; Tamaño: 593920 bytes)
Xiaomi_Redmi 7A.zip/data/data/com.whatsapp/files/Avatars/5493863408975@s.whatsapp.net.j : 0x0 (Tamaño: 4478 bytes)

Estados de interacción

Información adicional

About

Mi gran tesoro. Mis hijos

Detalles

General

+5493863408975

WhatsApp User Id

5493863408975@s.whatsapp....

Organizaciones

Origen

Imágenes

Ir a

Detalles

Eventos (2)



Guardar

Nombre:

5493863408975@s.whatsapp.net.j

Tipo:

Imágenes

Tamaño (bytes):

4478

Ruta:

Xiaomi_Redmi 7A.zip/data/data/com.whatsapp/files/Avatars/5493863408975@s.whatsapp.net.j

Creado:

Último acceso:

Modificado:

16/5/2022 00:57:29(UTC+0)

Cambiado:

Eliminado:

Extracción:

Sistema de archivos

MD5:

87fe5579070f2bb7008127b73e6b3963

Archivo de origen:

5493863408975@s.whatsapp.net.j

Mapa

Posición:

Dirección:

Dirección del mapa:

Imagen 8. –

#					Nombre	Estados de interacción	Organizaciones	Teléfonos	Mensajes	Otras entradas
1					Zerri Monteros			Mobile 381 353-6045 Enviar mensaje a +54 9... Mobile 3813536045		
2					Zerri Monteros			General 3813536045		WhatsApp User Id

Imagen 9. -

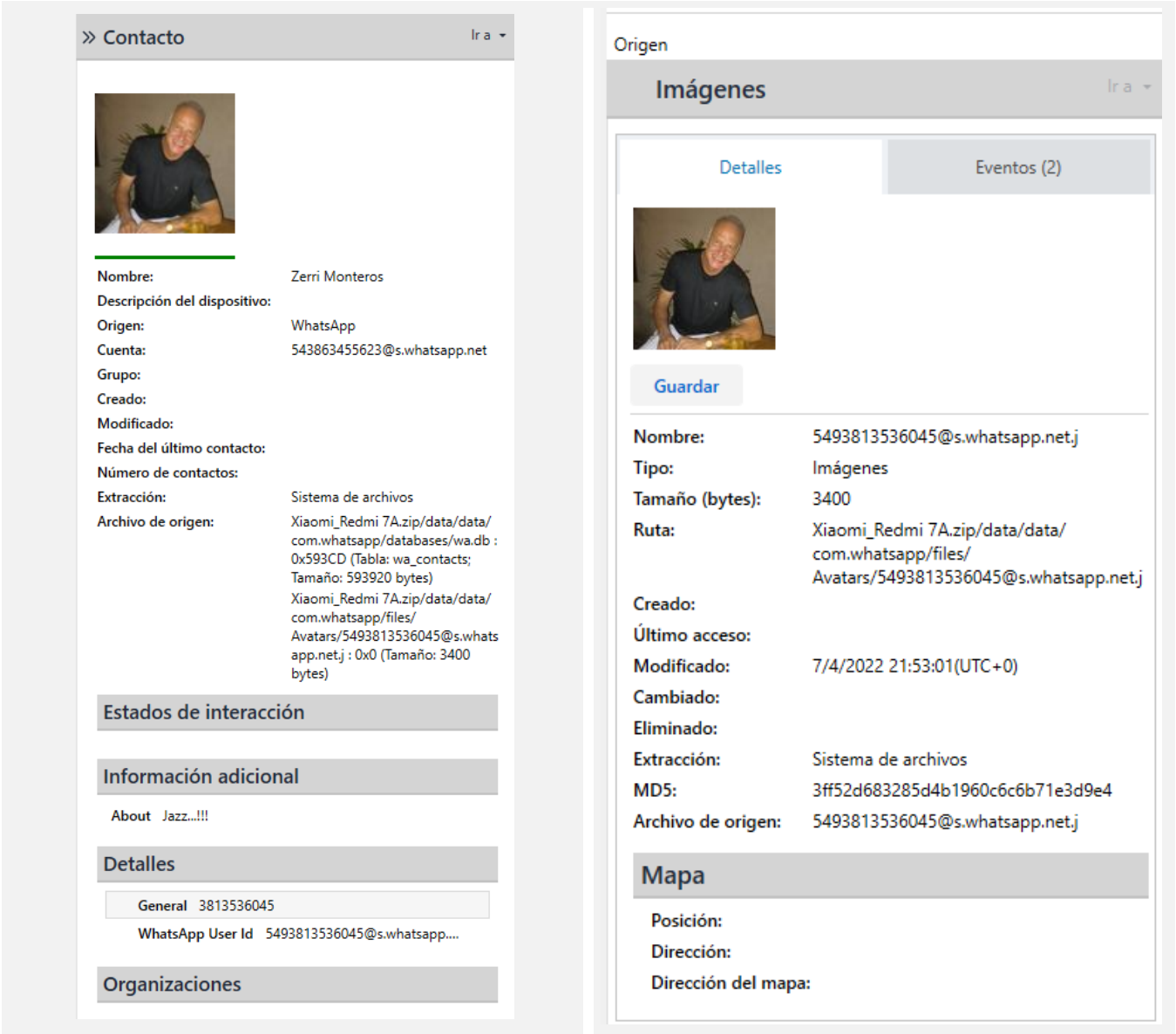


Imagen 10. -

Conversaciones

De haber ingresado por directorio del software forense, en la carpeta Conversaciones, se establece que cuenta con 535 elementos, destacando lo siguiente:

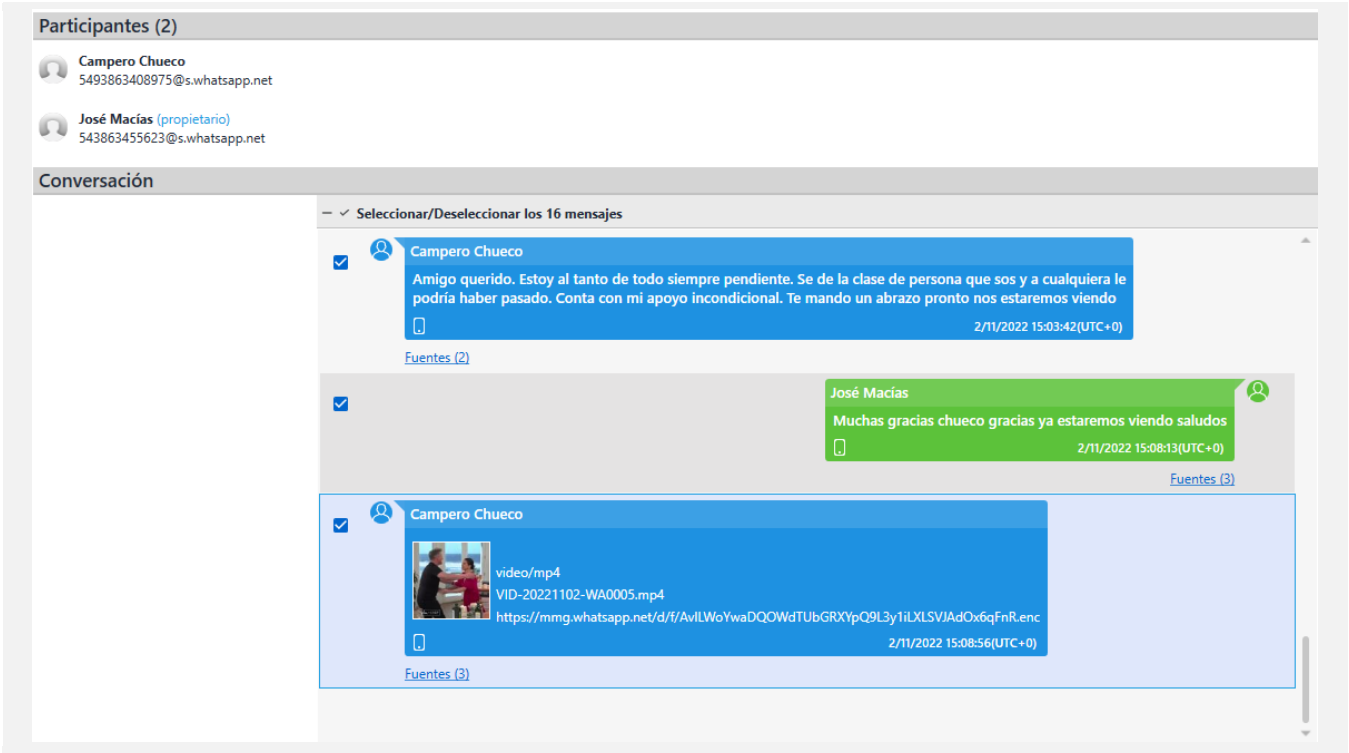


Imagen 11. -

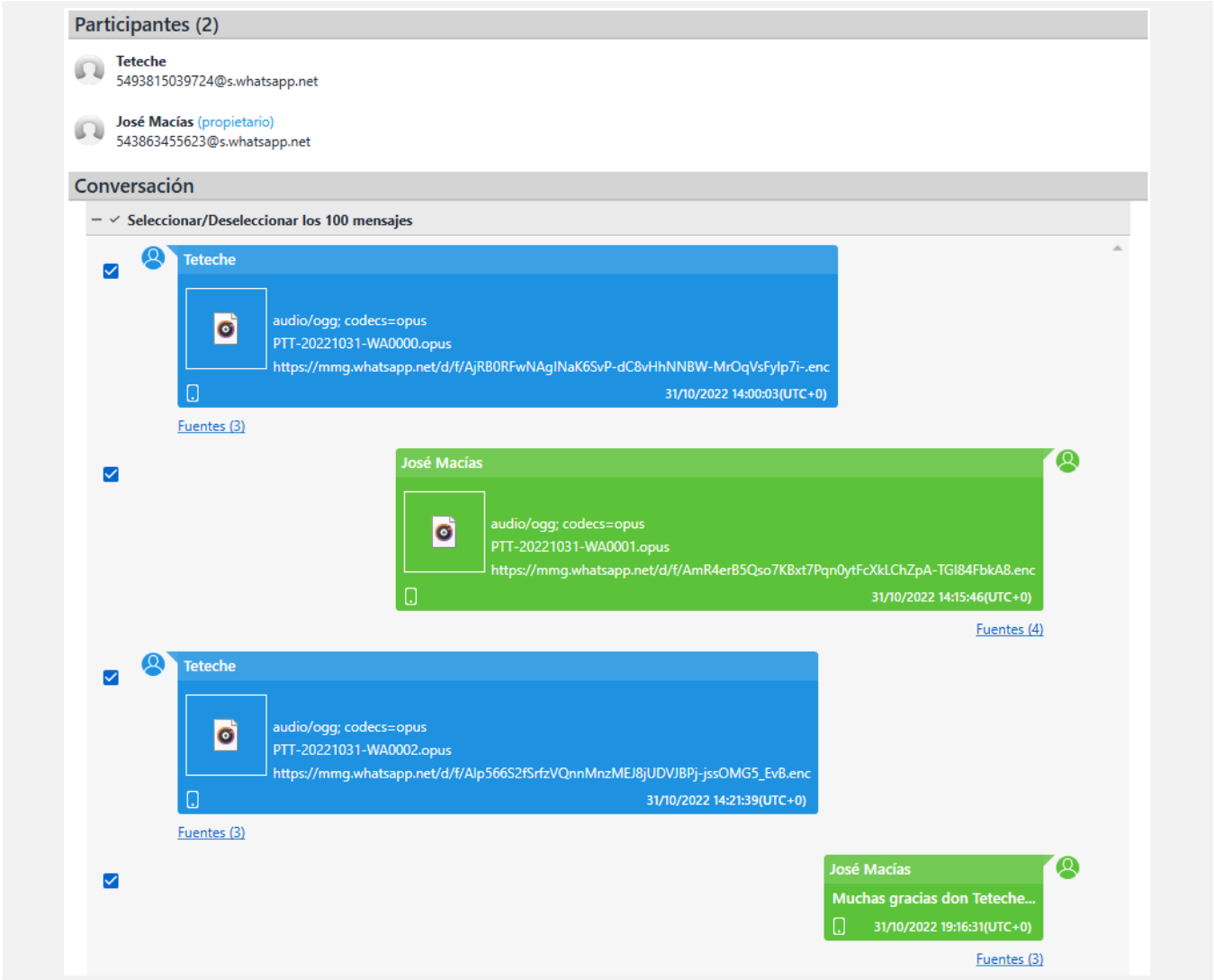


Imagen 12. -

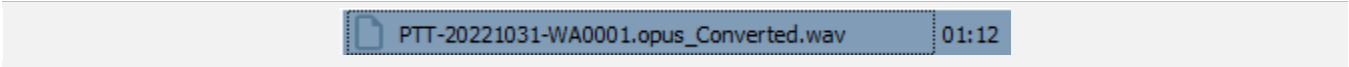


Imagen 13. -

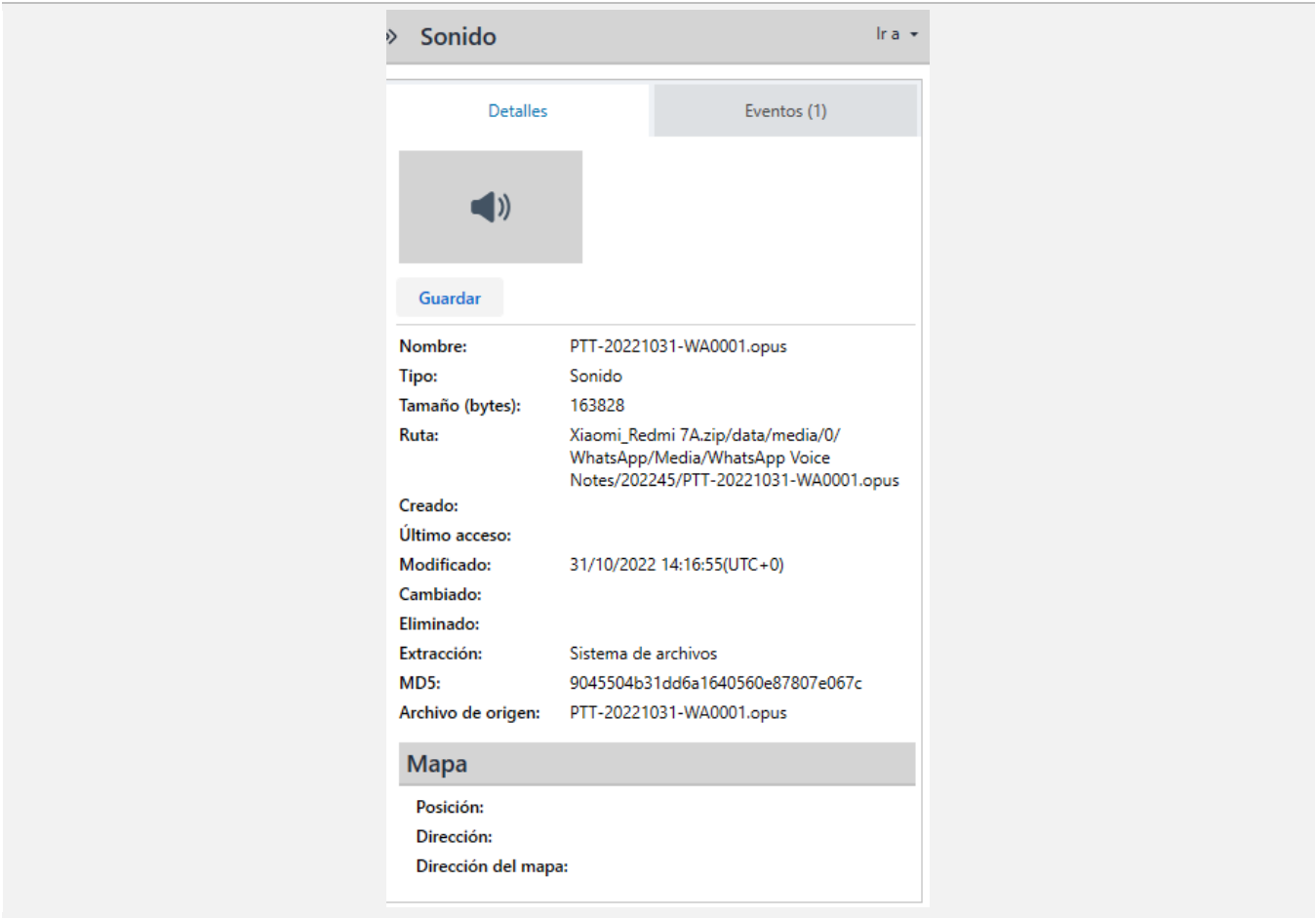


Imagen 14. -

Sonido

De haber ingresado por directorio del software forense, en la carpeta Sonido, se establece que cuenta con 1169 elementos, destacando el siguiente:

1	PTT-20221031-WA0001.opus	Xiaomi_Redmi 7A.zip/data/media/0/Whats...	163828		31/10/2022 14:16:55(UTC+0)
---	--------------------------	---	--------	--	----------------------------

Imagen 15. -

Transcripción:

Buen día Teteche, soy Magi, si José tuvo un accidente anoche a las diez de la noche, iba con dos personas más de Monteros, iban de Montero a Simoca y ahí, pasando la bandera esa grande, se le ha cruzao una moto, según él y yyy las choco a las personas y las mato a las dos chicas que iban, una de 19 años y la otra de 29 años, una de las chicas es sobrina de él, la de 19 años, hija de Mario Vitale, un primo de él, la otra chica es de León Rouge, no sé quién es, así que te pode imaginar cómo estamos, porque bueno, a José lo tuvieron que demorar anoche en la comisaria y ahora continúa en la comisaria hasta que le tomen las declaraciones en tribunale y vean cual va a continua siendo su proceso legal porque al haber dos muertes el está complicado y al haber venido alcoholizado lo complica a uno más, así que bue, esa es la novedad que tengo y cualquier cosa te estoy comunicando Teteche.

- Se observó también que sucedieron llamadas no recibidas utilizando la aplicación WhatsApp.

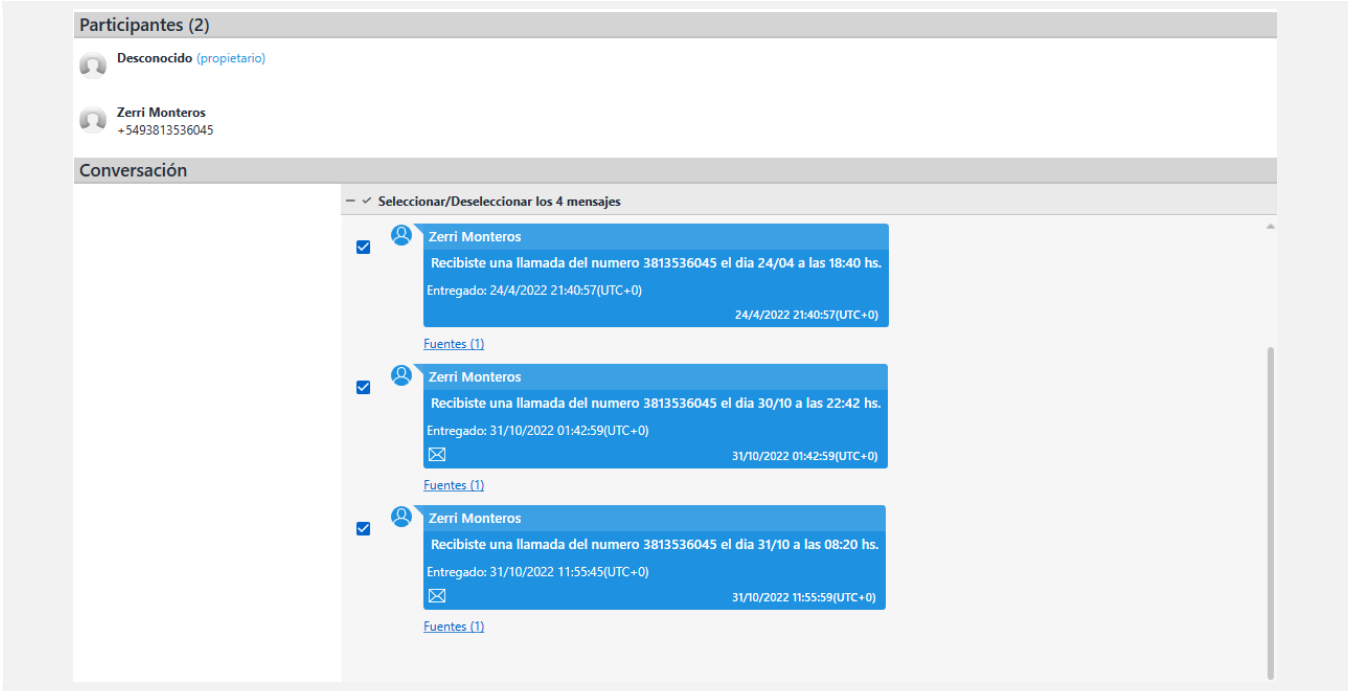


Imagen 16. -

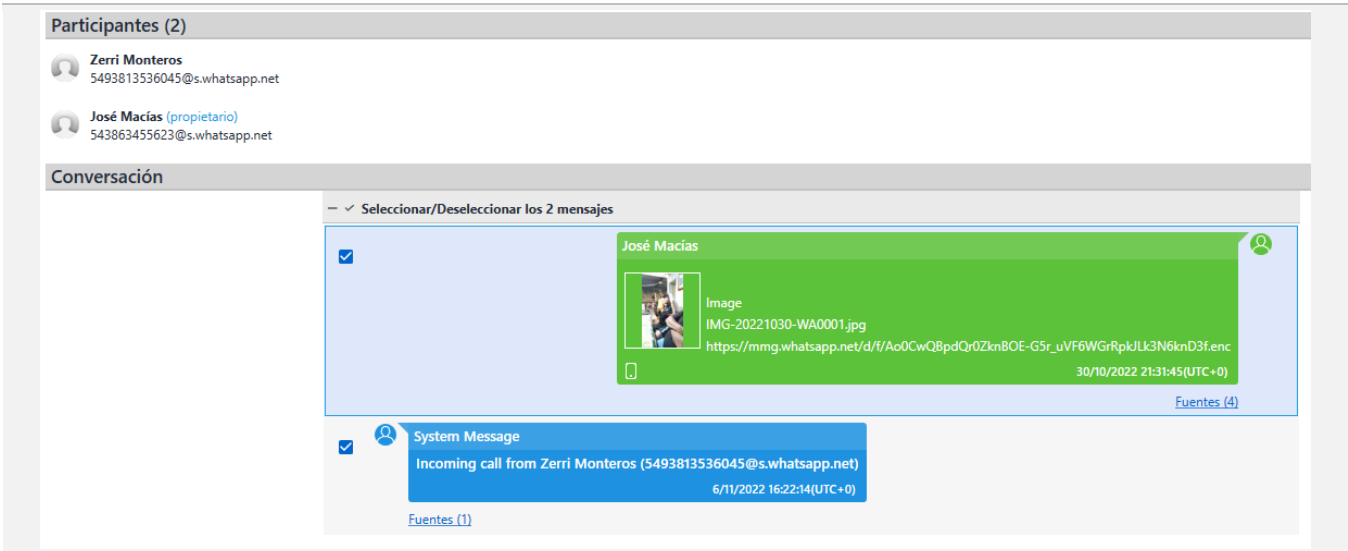


Imagen 17. -

3 FASE DE PRESENTACION

3.1. Responsabilidad y opinión del Director

3.1.1. Responsabilidad del Director

El **Director** es responsable de la preparación y correcta presentación del informe en conformidad con las políticas y controles internos del Departamento, realizando las correcciones necesarias para procurar evitar las declaraciones erróneas.

3.1.2. Opinión del Director

En opinión de la Dirección, el presente informe cumple con los principios básicos de relevancia, suficiencia, validez legal y confiabilidad. El examinador ha respetado los parámetros y modelo establecido para la confección del informe.

3.2 Resguardo de la evidencia digital

Habiendo finalizado las diferentes fases del presente informe el **10 de febrero de 2023 - 14:46**, se procede a resguardar las imágenes forense obtenidas de los dispositivos afectados, las que serán conservados por un plazo mínimo de 90 días y un plazo máximo de 6 meses. Es posible solicitar una extensión de dicho período de tiempo, mediante una nueva solicitud.

A continuación, se detallará los soportes ópticos que serán enviados en forma separada al informe.

Soporte óptico	Marca	Cantidad	Observaciones
DVD-R	TDK	01	-.

3.3 Conclusiones y recomendaciones

El examinador, en caso de considerarlo necesario, podrá realizar recomendaciones no vinculantes a la Unidad Fiscal para poder profundizar sobre la adquisición de ciertos dispositivos.

Teniendo en cuenta lo requerido por la UFI se establece que del análisis realizado al contenido del dispositivo **Teléfono celular, marca Xiaomi, modelo M1903C3EG (Redmi 7A), IMEI físico n° no visible, IMEI electrónico 1 n° 866679049934924, IMEI electrónico 2 n° 866679049934932**, se establece lo siguiente:

Cuentas de usuario:

01	José Macías	joo.ale333@gmail.com	
02	José Macías	joo.ale333@gmail.com	104875335561571961642
03	José Macías	joo.ale333@gmail.com	
04	José Macías	543863455623@s.whatsapp.net	Mobile 543863455623 Google Drive Account joo.ale333@gmail.com
05	REGINA EUGENIA MACIAS	macias.regina@colegioconsolacionconcepcion.edu.ar	
06	REGINA EUGENIA MACIAS	macias.regina@colegioconsolacionconcepcion.edu.ar	112828623144680718499
07	REGINA EUGENIA MACIAS	macias.regina@colegioconsolacionconcepcion.edu.ar	

01.- En lo referido a los abonados aportados por la UFI, según lista de contactos del dispositivo son utilizados por las siguientes personas:

01	3863455623	José Macías
02	3865564480	Carlos Aldonate
03	3865564480	Acosta Mario
04	3863408975	Campero Chueco
05	3813536045	Zerri Monteros

De las Conversaciones, se establece que cuenta con 535 elementos, destacando una conversación de la aplicación WhatsApp, donde Campero Chueco le saluda brindándole apoyo.

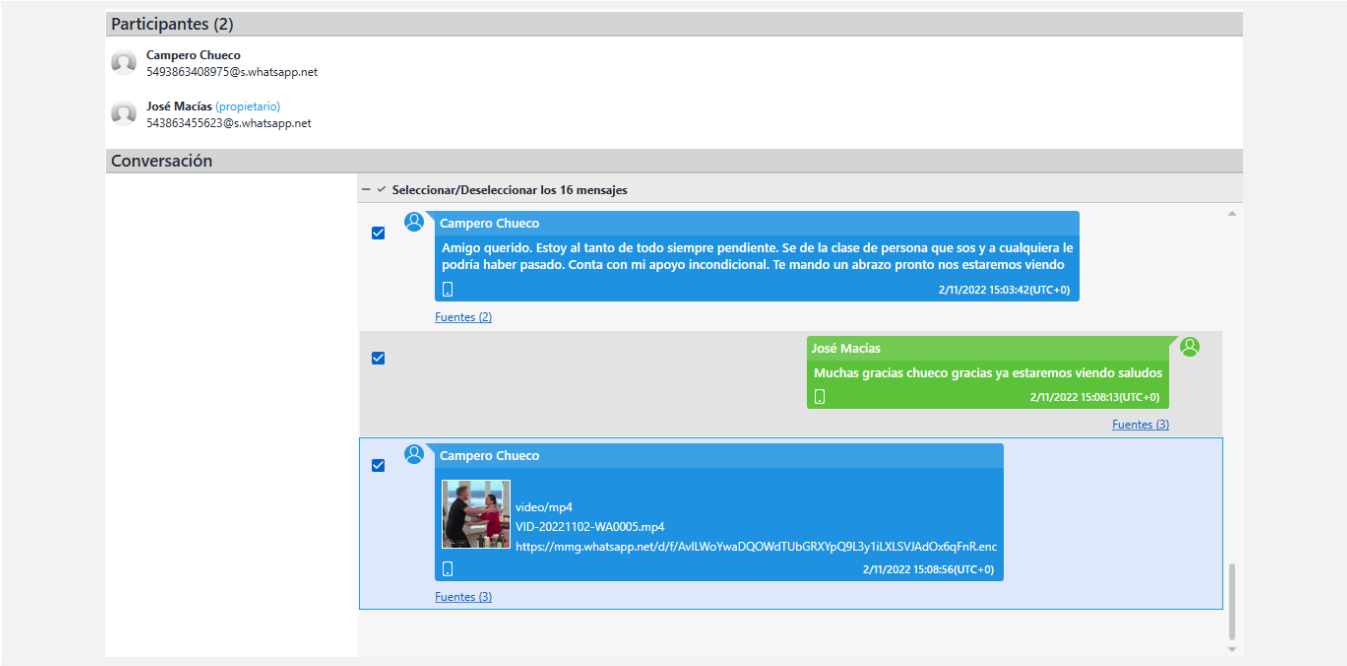


Imagen 18. -

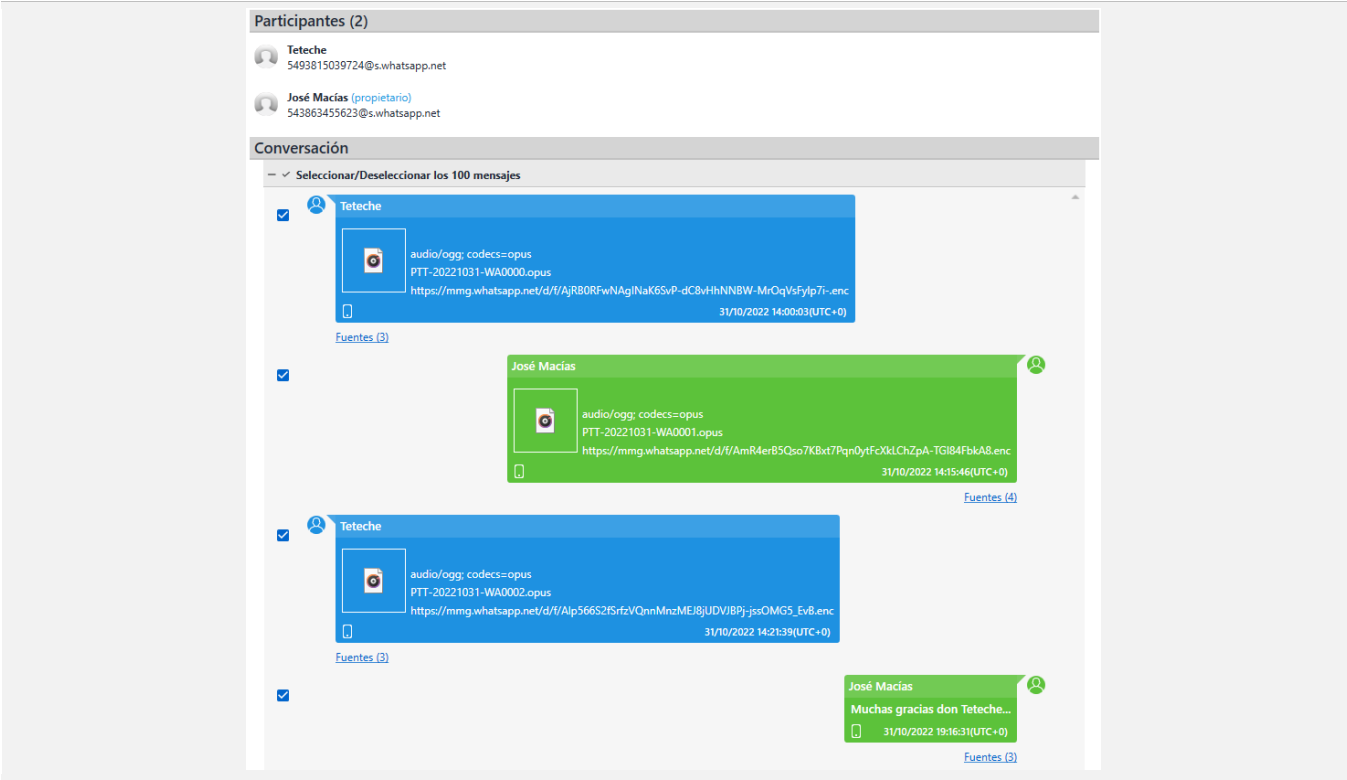


Imagen 19. -

Sonido

De haber ingresado por directorio del software forense, en la carpeta Sonido, se establece que cuenta con 1169 elementos, destacando el siguiente:

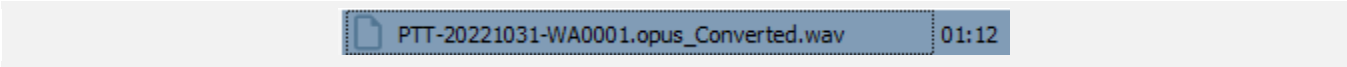
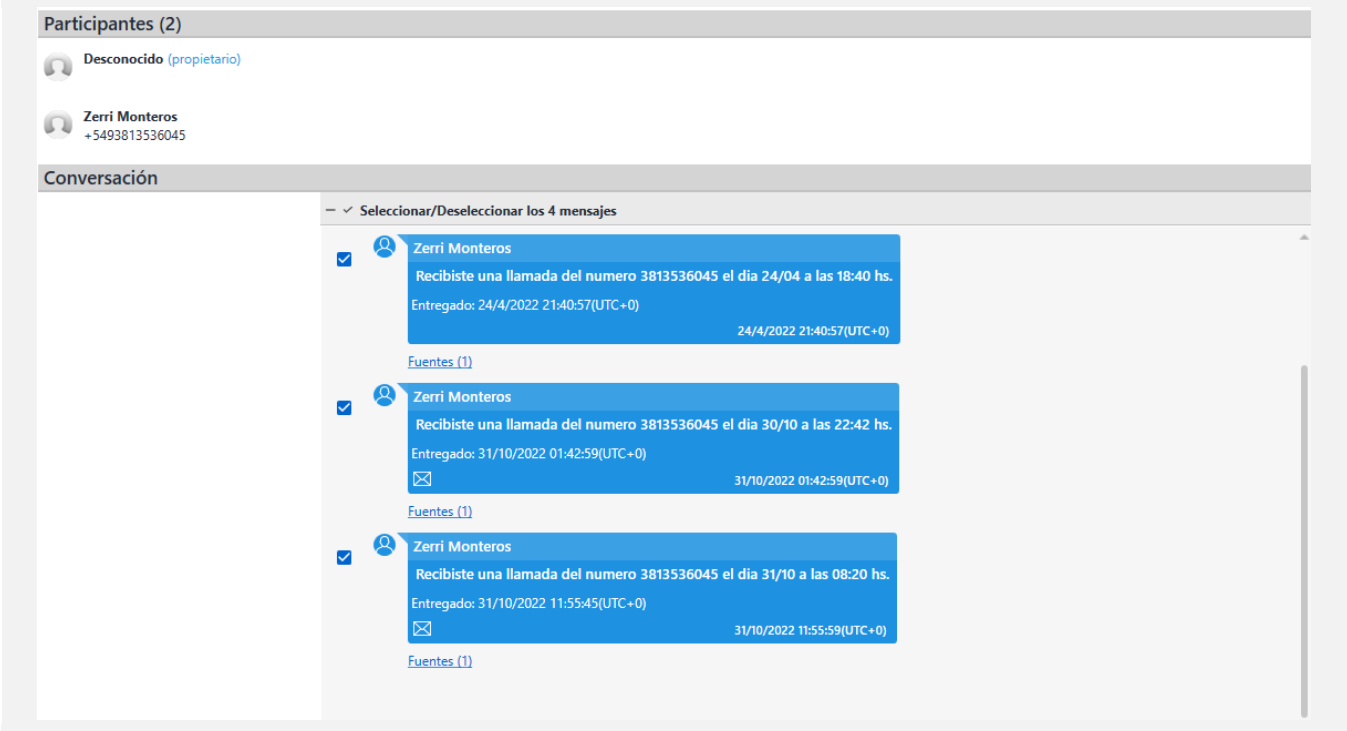


Imagen 20. -

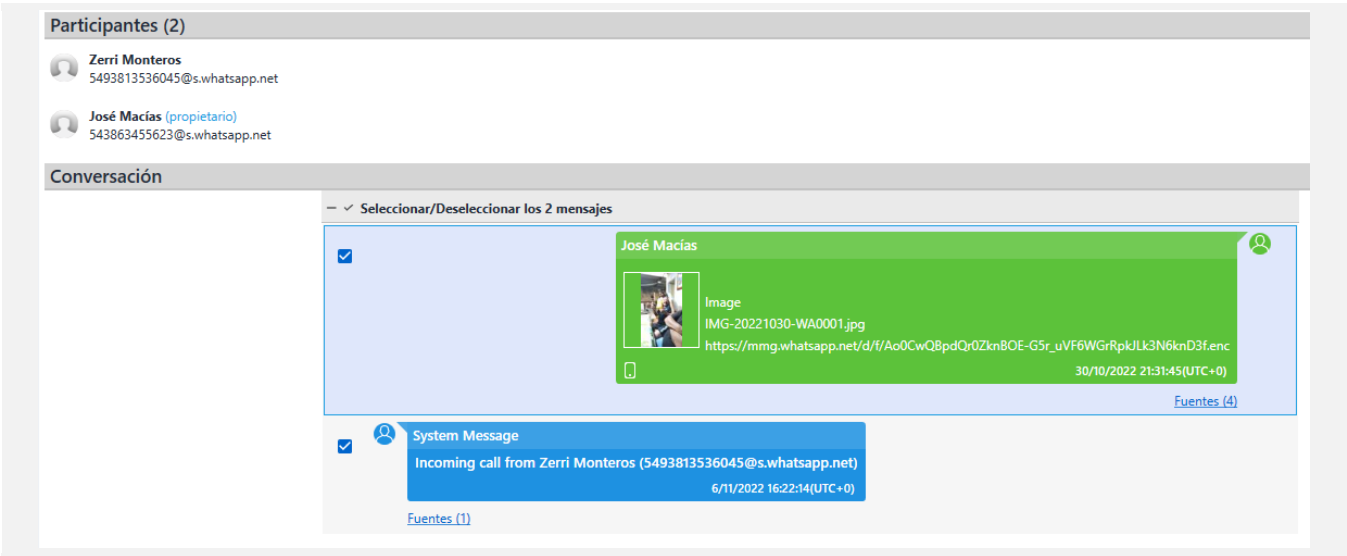
Transcripción:

Buen día Teteche, soy Magui, si José tuvo un accidente anoche a las diez de la noche, iba con dos personas más de Monteros, iban de Montero a Simoca y ahí, pasando la bandera esa grande, se le ha cruzao una moto, según él y yyy las choco a las personas y las mato a las dos chicas que iban, una de 19 años y la otra de 29 años, una de las chicas es sobrina de él, la de 19 años, hija de Mario Vitale, un primo de él, la otra chica es de León Rouge, no sé quién es, así que te pode imaginar cómo estamos, porque bueno, a José lo tuvieron que demorar anoche en la comisaria y ahora continúa en la comisaria hasta que le tomen las declaraciones en tribuna y vean cual va a continua siendo su proceso legal porque al haber dos muertes el está complicado y al haber venido alcoholizado lo complica a uno más, así que bueh, esa es la novedad que tengo y cualquier cosa te estoy comunicando Teteche.

- Zerri monteros, mediante la aplicación WhatsApp intenta llamar al usuario del dispositivo en dos ocasiones en fecha 31/10/2022.



- Zerri Monteros intenta llamar a José Macías en fecha 06/11/2022.



3.4 Firma electrónica

Las firmas electrónicas que a continuación son plasmadas se encuentran controladas en forma interna por este Departamento de Informática Forense. Poseen un cifrado con algoritmo clave RSA 1024-bits, la cual cumple con los requisitos de validez del artículo 1 y 9 de la Ley Nacional n° 25.506.-

Gustavo Fabian Luna

Firma del examinador (Control 1 de 2)

Firmado digitalmente porGustavo Fabian Luna
DN: cn=Gustavo Fabian Luna gn=Gustavo Fabian Luna c=AR Argentina l=AR Argentina e=300gustavoluna@gmail.com
Motivo: Examinador
Ubicaci- n:San Miguel de Tucum\$ñ
Fecha:2023-02-10 14:47-03:00

Edgar Jesus Aranda

Firma del director (Control 2 de 2)

Firmado digitalmente porEdgar Jesus Aranda
DN: cn=Edgar Jesus Aranda gn=Edgar Jesus Aranda c=AR Argentina l=AR Argentina o=ECIF MPF Tucuman ou=Departamento Inform\$ica Forense
e=arandapoltuc@gmail.com
Motivo:Soy el autor de este documento
Ubicaci- n:
Fecha:2023-02-10 14:47-03:00

FIN DE LA FASE DE PRESENTACIÓN

FIN DEL INFORME TÉCNICO