

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 Fabián 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
	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:
01.-	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 Motorola, modelo XT2159-1 Moto E40, en mal estado de conservación, IMEI físico n° 354434980920782, IMEI electrónico n° 354434980920782.**

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	19.814.845.342	70cf411fbdca64ed024d62c1f97f5a6a

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

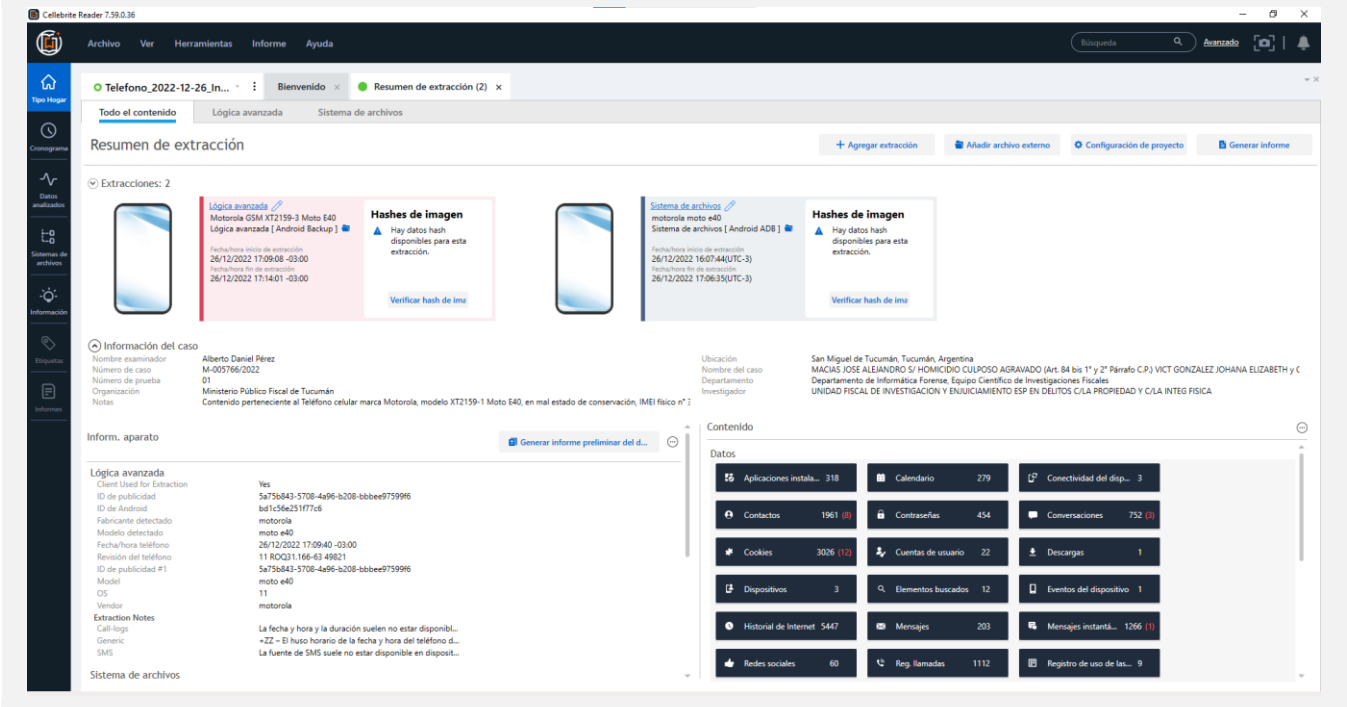


Imagen 1. -

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 22 elementos, destacando los siguientes:

01	Carlos Alberto Aldonate	carlosalbertoaldonat0@gmail.com	
02	Carlos Alberto Aldonate	carlosalberto.aldonate.7	Facebook Id 100010563462323
03	Carlos Alberto Aldonate		Facebook Id 100010563462323
04	Carlos Alberto Aldonate	carlosalbertoaldonat0@gmail.com	Google Drive 109318210102062205681
05	Carlos Alberto Aldonate	aldonatecarlosalberto	Instagram 54127914322
06	carlos Aldonate	543865564480@s.whatsapp.net	Mobile 543865564480

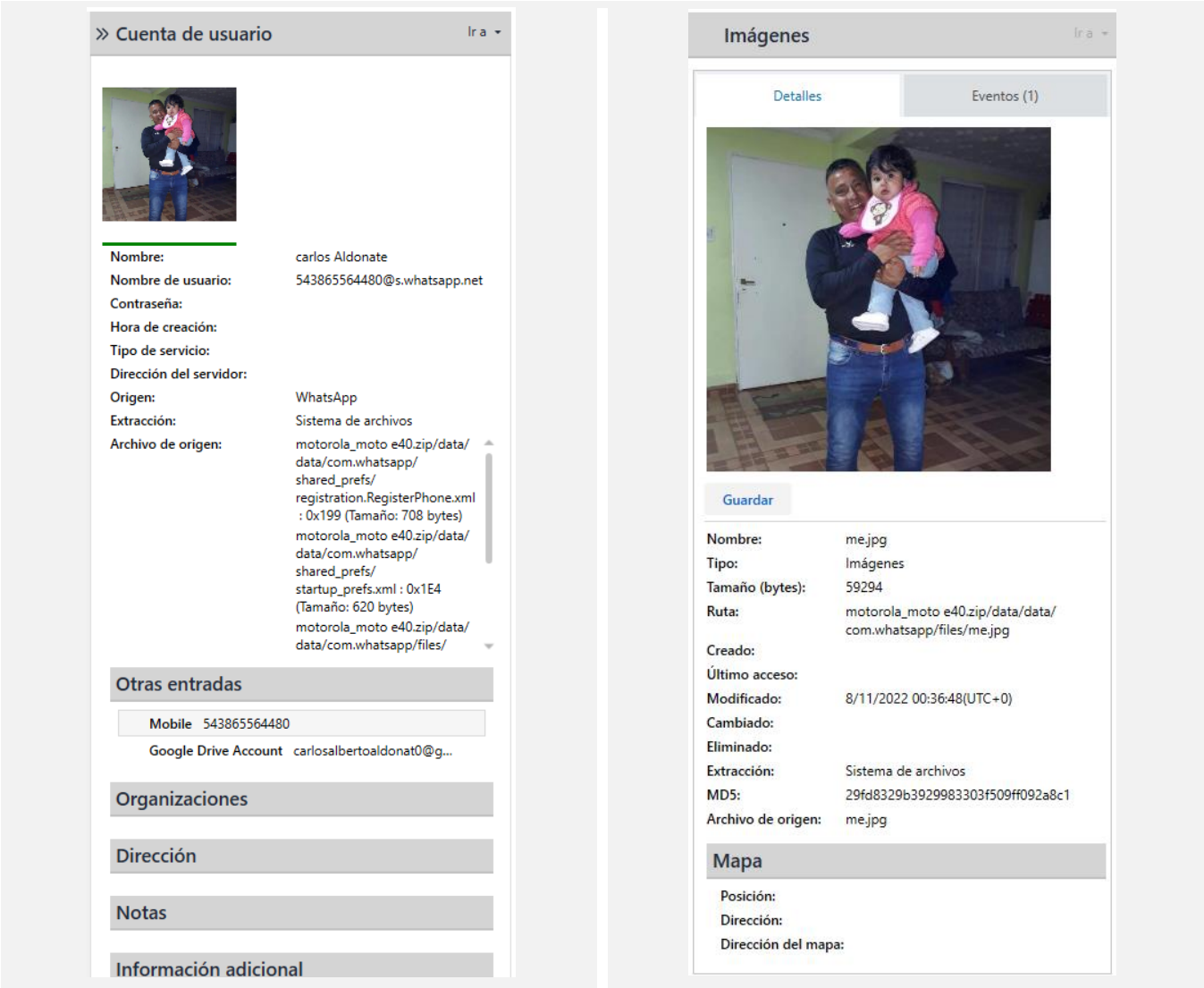


Imagen 2. -

Contactos

De haber ingresado por directorio del software forense, en la carpeta Contactos, se establece que cuenta con 1961 elementos. De haber filtrado el abonado 38633455623, se obtuvo lo siguiente:

#					↑ Nombre ▾	Estados de intera	Organizaciones ▾	Teléfonos ▾	Mensajes ▾	Otras entradas ▾
1					Macias Jose					+5493863455623
2					Macias Jose			Mobile 3863 45-5623 Enviar mensaje a +54 9 3863 45-5623 Mobile 3863455623		
3					Macias Jose			General 3863455623		WhatsApp User Id ..

Imagen 3. -

» Contacto



Nombre: Macias Jose

Descripción del dispositivo:

Origen: WhatsApp

Cuenta: 543865564480@s.whatsapp.net

Grupo:

Creado:

Modificado:

Fecha del último contacto:

Número de contactos:

Extracción: Sistema de archivos

Archivo de origen: motorola_moto e40.zip/data/data/com.whatsapp/databases/wa.db; 0x2A31D; Table: wa_contacts; Tamaño: 438272 bytes)

Estados de interacción

Información adicional

Detalles

General 3863455623

WhatsApp User Id 5493863455623@s.whatsapp...

Imagen 4. -

De haber filtrado el abonado 3863581588, se obtuvo lo siguiente:

	↑ Nombre ▾	Estados de intera	Organizaciones ▾	Teléfonos ▾	Mensajes ▾	Otras entradas ▾
	Acosta Marito			Mobile 386-358-1588 Mobile +5493863581588 Mobile +5493863581588		
	Marito Acosta					+5493863581588
	Marito Acosta			Mobile 3863 58-1588 Mobile +54 9 3863 58-1588 Enviar mensaje a +54 9 3863 58-1588 Mobile +5493863581588		
	Marito Acosta			General 3863581588 General +5493863581588		WhatsApp User Id ..

Imagen 5. -

» Contacto



Nombre: Marito Acosta

Descripción del dispositivo:

Origen: WhatsApp

Cuenta: 543865564480@s.whatsapp.net

Grupo:

Creado:

Modificado:

Fecha del último contacto:

Número de contactos:

Extracción: Sistema de archivos

Archivo de origen: motorola_moto e40.zip/data/data/com.whatsapp/databases/wa.db; 0x56CA3; Table: wa_contacts; Tamaño: 438272 bytes)
motorola_moto e40.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 3863581588

General +5493863581588

WhatsApp User Id 5493863581588@s.whatsapp...

Origen

Imágenes

Detalles

Eventos (2)



Guardar

Nombre: 5493863581588@s.whatsapp.net.j

Tipo: Imágenes

Tamaño (bytes): 3952

Ruta: motorola_moto e40.zip/data/data/com.whatsapp/files/Avatars/5493863581588@s.whatsapp.net.j

Creado:

Último acceso:

Modificado: 22/1/2022 01:43:44(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. -

De haber filtrado el abonado 3863408975 se obtuvo lo siguiente:

#					↑ Nombre ▾	Estados de intera	Organizaciones ▾	Teléfonos ▾	Mensajes ▾	Otras entradas ▾
1					Chueco Campe...					+5493863408975
2					Chueco Campe...			Mobile 3863 40-8975 Enviar mensaje a +54 9 3863 40-8975 Mobile 3863408975		
3					Chueco Campe...			General 3863408975		WhatsApp User Id ..

Imagen 7. -

» ContactoIr a ▾



Nombre: Chueco Campero

Descripción del dispositivo:

Origen: WhatsApp

Cuenta: 543865564480@s.whatsapp.net

Grupo:

Creado:

Modificado:

Fecha del último contacto:

Número de contactos:

Extracción: Sistema de archivos

Archivo de origen: motorola_moto e40.zip/data/data/com.whatsapp/databases/wa.db : 0x3ED6E (Tabla: wa_contacts; Tamaño: 438272 bytes)

motorola_moto e40.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 3863408975

WhatsApp User Id 5493863408975@s.whatsapp....

Organizaciones

Origen

ImágenesIr a ▾

Detalles

Eventos (2)



Guardar

Nombre: 5493863408975@s.whatsapp.net/j

Tipo: Imágenes

Tamaño (bytes): 4478

Ruta: motorola_moto e40.zip/data/data/com.whatsapp/files/Avatars/5493863408975@s.whatsapp.net/j

Creado:

Último acceso:

Modificado: 16/5/2022 00:22:16(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. -

- De haber filtrado el abonado 3813536045 se obtuvo lo siguiente:

#					↑ Nombre ▾	Estados de intera	Organizaciones ▾	Teléfonos ▾	Mensajes ▾	Otras entradas ▾
1					Serri					+5493813536045
2					Serri			Móvil +54 9 381 353-6045 Enviar mensaje a +54 9 381 353-6045 Móvil +5493813536045		
3					Serri			General +5493813536045		WhatsApp User Id ..
4					Serri			General +5493813536045 General +5493813536045		

Imagen 9. -

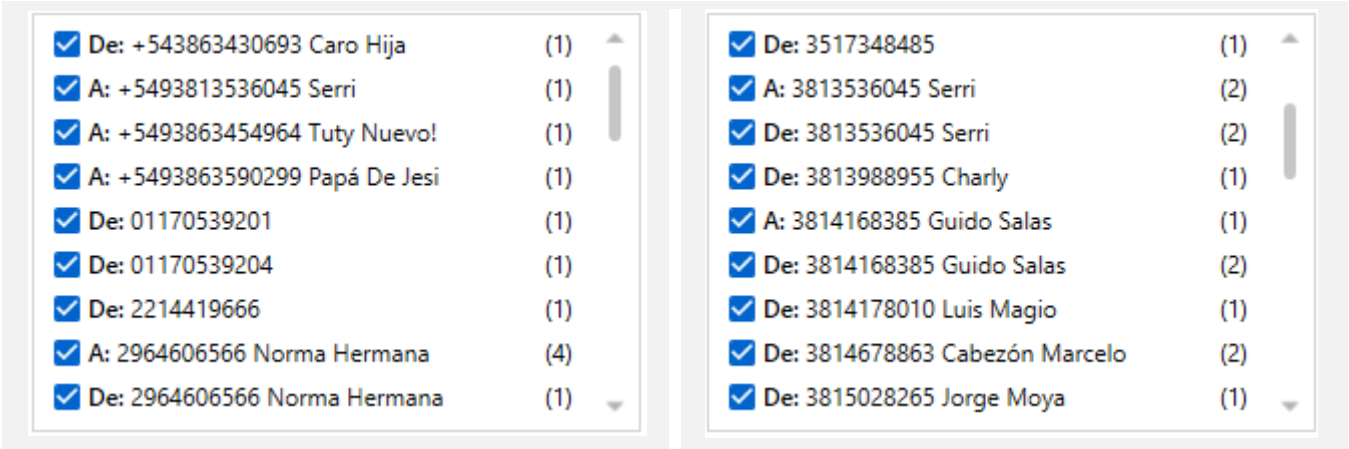


Imagen 12. -

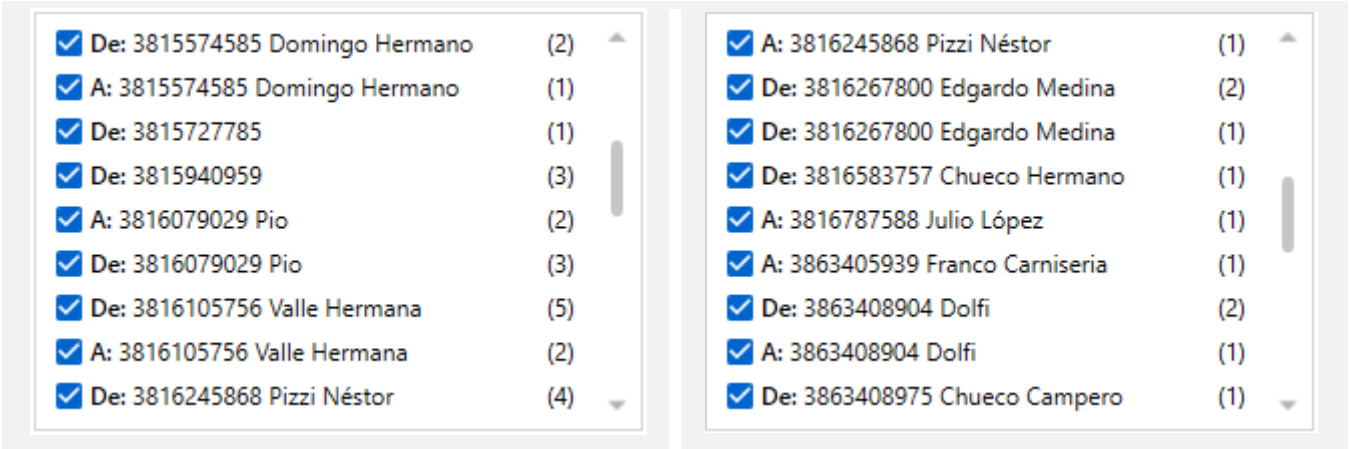


Imagen 13. -

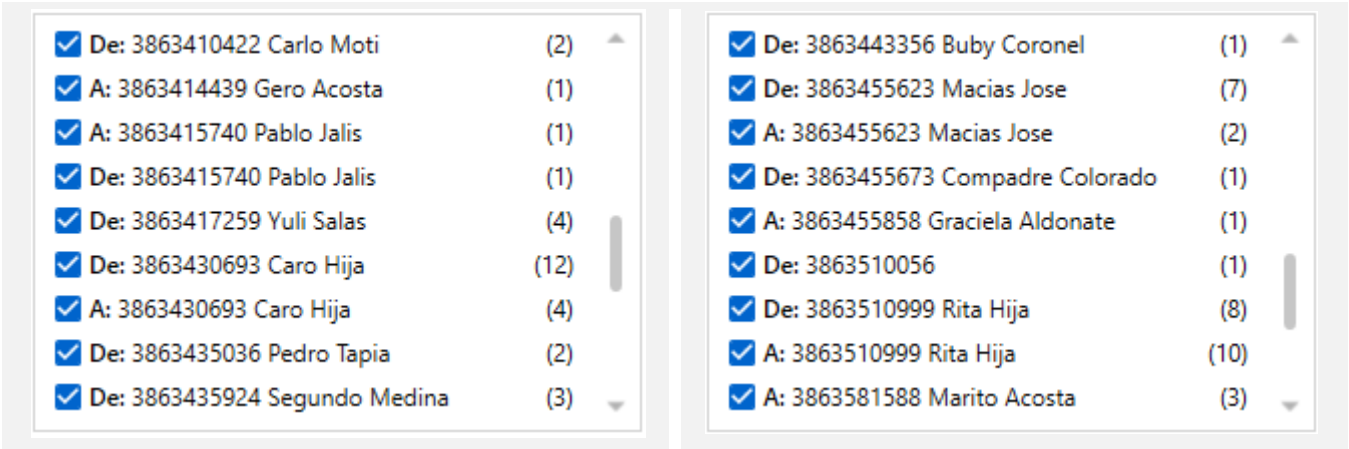


Imagen 14. -

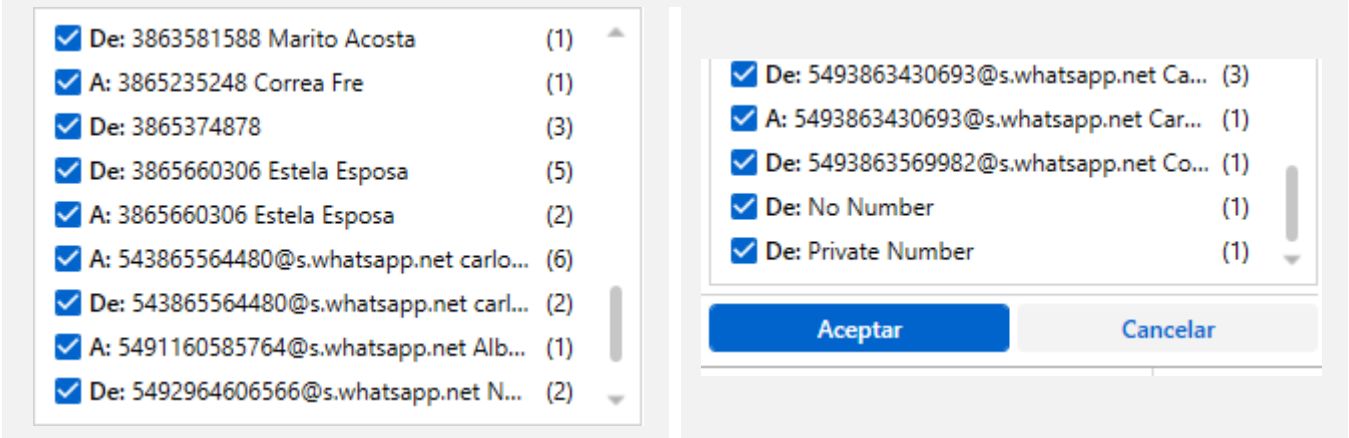


Imagen 15. -

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 - 14:30**, 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.

Los datos analizados correspondientes al dispositivo **Teléfono celular marca Motorola, modelo XT2159-1 Moto E40, en mal estado de conservación, IMEI físico n° 354434980920782, IMEI electrónico n° 354434980920782, SIM Card ICCID 8954310211056387374, Claro Ar,** con se obtuvo lo siguiente:

Cuentas de usuario

De haber ingresado por directorio del software forense, en la carpeta Cuentas de usuario, se establece que cuenta con 22 elementos, destacando los siguientes:

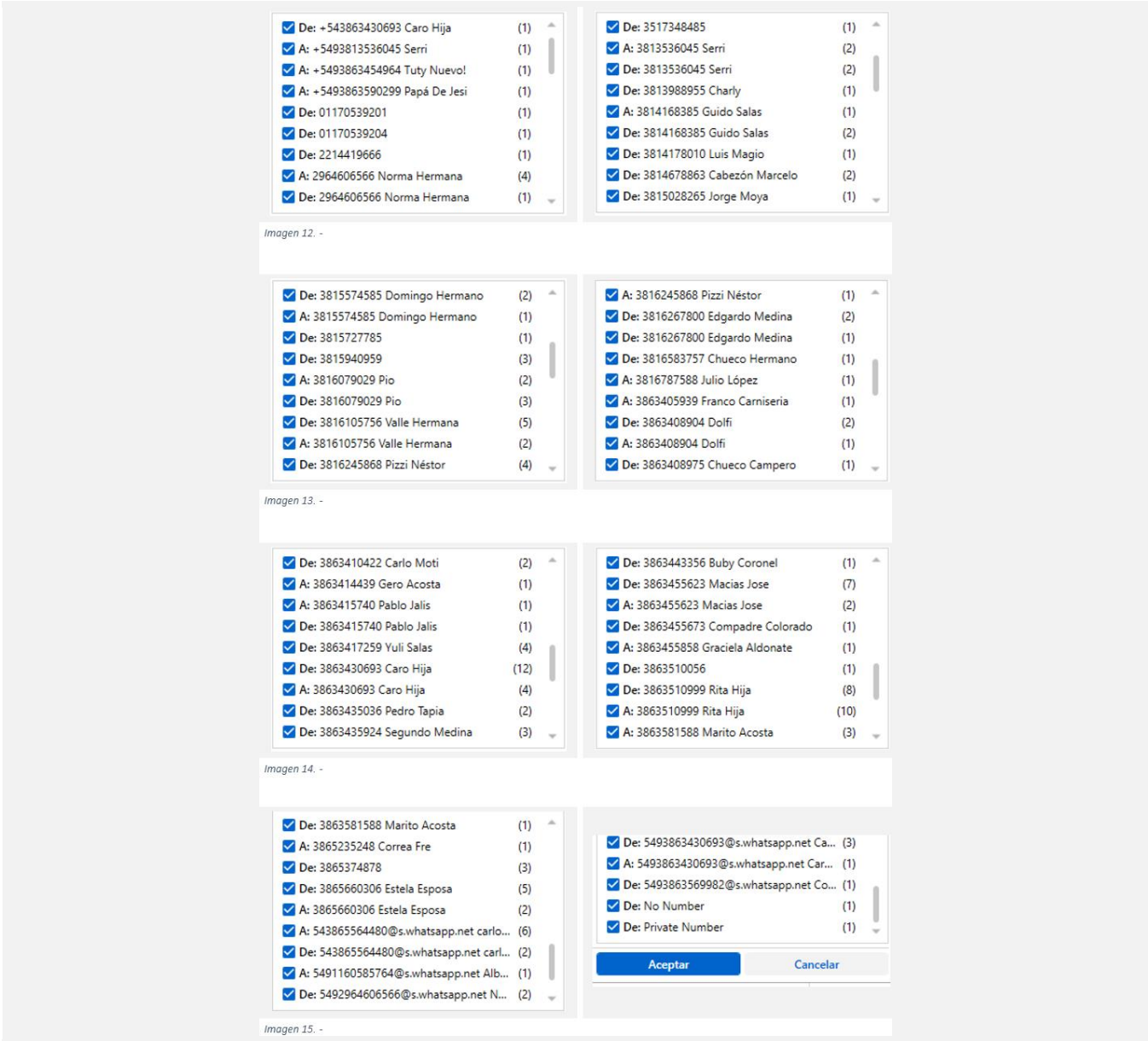
01	Carlos Alberto Aldonate	carlosalbertoaldonat0@gmail.com	
02	Carlos Alberto Aldonate	carlosalberto.aldonate.7	Facebook Id 100010563462323
03	Carlos Alberto Aldonate		Facebook Id 100010563462323
04	Carlos Alberto Aldonate	carlosalbertoaldonat0@gmail.com	Google Drive 109318210102062205681
05	Carlos Alberto Aldonate	aldonatecarlosalberto	Instagram 54127914322
06	carlos Aldonate	543865564480@s.whatsapp.net	Mobile 543865564480

Conversaciones

De haber ingresado por directorio del software forense, en la carpeta Conversaciones, se establece que cuenta con 752 elementos, no destacando ninguna de interés a la investigación.

Conversaciones

De haber ingresado por directorio del software forense, en la carpeta Conversaciones, se establece que cuenta con 1112 elementos, de lo que al filtrar las llamadas sucedidas desde fecha 31/10/2022 hasta el 09/11/2022, sucedieron 146 llamadas: 99 salientes y 47 entrantes.



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 por Gustavo Fabian Luna
DN: cn=Gustavo Fabian Luna, gn=Gustavo Fabian Luna, c=AR, Argentina, l=AR, Argentina, e=300gustavoluna@gmail.com
Motivo: Examinador
Ubicación: San Miguel de Tucumán
Fecha: 2023-02-10 14:30:03.00

Edgar Jesus Aranda

Firma del director (Control 2 de 2)

Firmado digitalmente por Edgar Jesus Aranda
DN: cn=Edgar Jesus Aranda, gn=Edgar Jesus Aranda, c=AR, Argentina, l=AR, Argentina, o=ECIF MPF Tucumán, ou=Departamento Informático Forense, e=arandajp@tucuman.gov.ar
Motivo: Soy el autor de este documento
Ubicación: Tucumán
Fecha: 2023-02-10 14:30:03.00

FIN DE LA FASE DE PRESENTACIÓN

FIN DEL INFORME TÉCNICO