por los Derechos Civiles

¿Quién revisa tu teléfono?

Situación de las herramientas de extracción forense de dispositivos móviles en sentencias judiciales y fuerzas de seguridad

PARTE 2

Septiembre 2022
adc.org.ar

Redacción: Luis García Balcarce
Diagramación y diseño: El Maizal - Cooperativa de Comunicación

Contenido

Resumen ejecutivo

Nuestros teléfonos celulares contienen información de todo tipo, desde fotos, videos y correos electrónicos, hasta información sobre salud, lugares visitados y ocio. Esos datos, ante determinados delitos, permiten a las autoridades investigar y probar determinados hechos. Para hacerlo se utilizan herramientas de extracción forense de dispositivos móviles. S e trata de softwares y hardwares proveídos por empresas privadas a fuerzas de seguridad y fiscalías para la extracción y análisis de la información contenida en nuestros celulares.

El presente informe es una continuación del trabajo de investigación que publicó la Asociación por los Derechos Civiles (ADC) en diciembre de 2021, "¿Quién revisa tu teléfono?"[1]. En esta oportunidad el enfoque está puesto en el uso de las herramientas de extracción forense de la Gendarmería Nacional Argentina (GNA) y la Policía de la Ciudad Autónoma de Buenos Aires, así como también ministerios públicos fiscales de ambas jurisdicciones. Además profundiza sobre la interpretación judicial en torno a las mismas y echa luz de manera incipiente sobre cuestiones de seguridad fronteriza y migrantes.

Para finalizar se brinda una serie de recomendaciones dirigidas al Poder Judicial, Legislativo y fuerzas de seguridad a tener en cuenta para la regulación y el uso de las herramientas de extracción forense de dispositivos móviles en un marco de respeto de las garantías procesales y el derecho a la privacidad.

Introducción

Las herramientas de extracción forense de dispositivos móviles permiten acceder a la información disponible en un teléfono celular. En el contexto de las investigaciones penales, estas prácticas son llevadas a cabo por peritos o laboratorios informáticos que dependen de fuerzas de seguridad nacionales y provinciales.

En el marco del intento de magnicidio de la vicepresidenta de la Nación Cristina Fernández ocurrido en septiembre de 2022, surgieron diferentes noticias e interpretaciones sobre las pericias realizadas al teléfono celular del atacante al intentar extraer los datos del mismo[2]. Al momento de redactar este informe, aún no está claro que sucedió ni cómo pero luego de un primer intento de pericia el celular secuestrado se habría reseteado a la configuración de fábrica.

Algunas de las versiones mencionan que habría ocurrido tras un fallido intento de la Policía Federal por desencriptarlo. Al no poder acceder a la información se lo habrían enviado a la Policía de Seguridad Aeroportuaria, pero cuando lo conectaron salió la leyenda "teléfono reseteado de fábrica", es decir que ya no había datos a extraer[3].

Este tipo de situaciones y desprolijidades en el manejo de la evidencia digital demuestra una necesidad urgente de una legislación específica sobre los protocolos claros y transparentes para el funcionamiento de las herramientas de extracción forense de información en teléfonos celulares, y capacitaciones para operadores judiciales y fuerzas de seguridad sobre su utilización.

En la actualidad la mayoría de las fiscalías cuenta con herramientas para llevar adelante estas prácticas. Para este informe se realizó un relevamiento del estado actual de situación de la Gendarmería Nacional Argentina (GNA) y la Policía de la Ciudad Autónoma de Buenos Aires, así como también ministerios públicos fiscales de ambas jurisdicciones.

El centro estará puesto en el caso de la Gendarmería Nacional Argentina ya que tiene funciones de seguridad fronteriza y de seguridad interior como Policía Judicial en el Fuero Federal e Investigación Criminal en materia de crimen organizado, delitos complejos, delitos tecnológicos, ciberseguridad y narcocriminalidad, en las que las herramientas de extracción forense de información son de suma importancia y muy utilizadas. También se hará foco en en el caso de la Policía de la Ciudad de Buenos Aires, ya que al ser la capital federal tiene una mayor concentración de actividades y población en comparación con el resto del país[4] y resulta importante reportar sobre este tipo de herramientas en dicha jurisdicción, dado que su uso es habitual para investigaciones criminales.

Sobre las herramientas la atención se centra en UFED (Universal Forensic Extraction Device) de Cellebrite, por ser la más usada para extraer y analizar información en dispositivos móviles en Argentina[5]. En algunos casos surge de los datos la utilización de insumos de otro proveedor por lo que se los explicará brevemente.

Cellebrite es una empresa isaraelí que, según su sitio web, ofrece tecnología y servicios líderes en la industria "en los que confían las fuerzas de seguridad pública y las empresas del todo el mundo para ayudar a proteger a las comunidades, preservar sus activos más valiosos, así como brindar justicia y paz a las víctimas y a las personas inocentes"[6]. UFED es un dispositivo de esta empresa que sirve para extraer y decodificar la información de la gran mayoría de teléfonos celulares.

En los últimos años ha surgido información respecto al uso de UFED Cellebrite para investigar y perseguir disidentes en algunos países como Venezuela, Bielorrusia, Rusia e Indonesia, conocidos por tomar medidas contra la disidencia política y la comunidad LGBTIQ+. Ante diferentes peticiones presentadas por organizaciones de derechos humanos al Ministerio de Defensa de Israel, la empresa anunció que dejaría de vender su tecnología a China y Hong Kong, y más recientemente a Rusia y Bielorrusia[7].

UFED Cellebrite contiene Software Comercial o Privativo, es decir que el código fuente de la herramienta se encuentra protegido por el derecho de propiedad intelectual[8]. En el informe publicado por la ADC en 2021 se advirtió que una etapa fundamental de los procesos, que constituye nada menos que la obtención de prueba que podrá determinar la culpabilidad o inocencia de una persona, es llevada a cabo mediante herramientas y programas cuyos códigos y algoritmos de funcionamiento se desconocen. Ello entra en tensión con el artículo 18 de la Constitución Nacional argentina que reconoce a la persona imputada de un delito la facultad de poder conocer y controlar la prueba que se utiliza en su contra. Más aún si se tienen en cuenta las supuestas vulnerabilidades en determinadas herramientas que podrían poner en duda la fiabilidad de la prueba obtenida[9].

La sensibilidad de la información que tienen en la actualidad nuestros teléfonos celulares requiere que las prácticas mediante las cuales se llevan adelante las tareas de extracción y análisis de datos, así como la normativa que permite incorporarlas en un proceso judicial, sean respetuosas de las garantías de la persona imputada. Tales prácticas deben adecuarse a principios tales como legalidad, limitación de la finalidad, exactitud y calidad, conservación limitada, seguridad de los datos y confidencialidad. Es importante que estas garantías se apliquen a las personas imputadas y a los terceros cuya información también se encuentra en sus celulares.

Las decisiones judiciales y las herramientas de extracción forense para celulares

En la actualidad los teléfonos móviles contienen todo tipo de información sobre sus propietarios y propietarias y también de terceros. Desde conversaciones, fotos y correos electrónicos, hasta información bancaria, de salud y ocio. Cuando un teléfono es peritado la extracción de la información implica, por un lado la puesta en jaque del derecho a la privacidad, y por el otro la posibilidad de que se comprometa la información extraída afectando el resultado de la pericia, y por ende el derecho de defensa[10].

No hay regulación específica sobre el momento y la forma de utilización de las herramientas de extracción forense para teléfonos celulares dentro del proceso judicial. Ante esta ausencia de regulación toma especial relevancia la interpretación judicial, es decir, lo que los jueces, las juezas y operadores judiciales deciden en los casos concretos que les toca resolver.

A los fines de considerar la utilización de las herramientas de extracción forense sobre teléfonos celulares en los procesos judiciales, y cómo se enmarca con el derecho de defensa y los derechos fundamentales de las partes y terceros, se realizó un relevamiento de sentencias que se han pronunciado sobre este tipo de tecnologías, y más particularmente sobre UFED Cellebrite.

En la investigación se encontraron referencias a estas herramientas y su utilización en sentencias y otras resoluciones judiciales[11]. Sin embargo no surgen de las mismas ni de entrevistas con distintos operadores judiciales cuestionamientos a la herramienta de extracción de información en sí, a la fidelidad de lo que se extrae, a la metodología de funcionamiento, ni al riesgo que implica que las herramientas puedan ser comprometidas[12].

A modo de ejemplo, en junio de 2022 el Tribunal Oral en lo Criminal Federal N° 1 resolvió en la causa "Shen, Yongchao s/Infracción Ley 23.73713[13]" que no se trata de una pericia cuando la policía descarga por segunda vez información de un teléfono celular a través de una herramienta UFED. El motivo es que se considera que esta ya se realizó con la primera descarga.

Algo importante para destacar de este fallo es que se alegó por parte de la defensa una violación de la intimidad como consecuencia de la reiteración de la extracción de datos. Como respuesta a dicho planteo, el tribunal estableció que la información que eventualmente se considerará en el debate oral y público será únicamente aquella que se ordenó obtener, esto es, la que estuviera relacionada con los hechos en debate. En ningún momento se especifica qué pasará con el resto de la información extraída que no vaya a debate.

En septiembre de 2019 la Sala IV de la Cámara Nacional de Apelaciones en lo Criminal y Correccional resolvió en "A.J.A. y otros s/ nulidad[14]" rechazar el planteo de nulidad contra la medida que dispuso la copia forense de dos teléfonos celulares secuestrados sin que se notificará a la defensa. Los jueces consideraron que la apertura de los dispositivos móviles es equivalente a la obtención de una copia de la información de los datos almacenados en el dispositivo. Esa copia, que realiza la Dirección de Inteligencia de la Policía de la Ciudad con UFED Cellebrite, para ellos no constituye un peritaje, sino que se trata de una medida ordenada para preservar la prueba. Con base en ese argumento el juez puede obtener copias o reproducciones de la información secuestrada a los efectos de preservar la cadena de custodia sin necesidad de notificar a la defensa.

Con respecto a la utilización de la herramienta UFED Cellebrite, en estas dos sentencias el cuestionamiento es sobre la notificación y reiteración del procedimiento procesal para la extracción de la información de los teléfonos celulares, no sobre las tecnologías que

se utilizan ni la fiabilidad de las mismas. Algo fundamental de estos dos fallos es que ninguno tiene en cuenta la importancia de la primera extracción de información digital de un teléfono celular, ya que en ese acceso se obtiene el hash, un algoritmo que crea un valor único que permite identificar que la información extraída sea exactamente la misma a la almacenada. Entonces, si esa información se modifica cambian los bits[15] de los archivos originales, cambia el cálculo del hash y, en consecuencia, la cadena o algoritmo no es la misma que arroja la primera extracción. Por eso es importante constatar el hash en la primera extracción y así asegurarse la correcta cadena de custodia de los datos[16].

También se observa en las sentencias citadas y en diversas entrevistas con profesionales especialistas en el tema que la judicatura aún no ha definido acabadamente aspectos básicos de la investigación digital, como por ejemplo una definición clara sobre si la evidencia es el hardware o aparato del que se extrae la información, o la información que se extrae propiamente dicha.

Tampoco se encuentra establecido el carácter judicial de la extracción de la información de teléfonos celulares, si son pericias o secuestros de información, si requieren una orden judicial expresa y si hay que notificar a la defensa. Estas definiciones que parecen meras categorías jurídicas son importantes porque de acuerdo a su clasificación se aplican determinados resguardos o medidas en pos del derecho de defensa y debido proceso de la persona afectada.

Por lo que se pudo determinar al momento la definición de estas calificaciones jurídicas es que dependen de la interpretación de la autoridad judicial para el caso concreto.

Resulta importante destacar que tampoco está determinada la confiabilidad de las herramientas de extracción forense, ni su margen de error, aspectos fundamentales para la valoración de los datos obtenidos.

La jurisprudencia analizada demuestra el desconocimiento de operadores judiciales sobre la evidencia digital en teléfonos celulares y el tímido acercamiento que los jueces han tenido en estos temas. Ello genera una incertidumbre jurídica que debe ser resuelta de manera urgente para lograr estándares protectorios acordes con el debido proceso y los derechos fundamentales de los y las involucradas, y actualizar la labor judicial en temas de extracción forense de información digital.

Fuerzas de seguridad, ministerios públicos y herramientas de extracción forense sobre teléfonos móviles

El relevamiento que se realizó sobre la utilización de herramientas de extracción forense sobre teléfonos móviles por parte de organismos públicos se centró en la Gendarmería Nacional Argentina, el Ministerio Público Fiscal Nacional, la Policía de la Ciudad de Buenos Aires y el Ministerio Público de la Ciudad de Buenos Aires.

Tal como se mencionó anteriormente, se consideró importante poner foco en Gendarmería Nacional Argentina por sus funciones de seguridad fronteriza y de seguridad interior en materia de crimen organizado, delitos complejos, delitos tecnológicos, ciberseguridad y narcocriminalidad, y en la Ciudad de Buenos Aires por la concentración de actividad y población y la habitualidad del uso de estas herramientas en investigaciones criminales.

Ese relevamiento incluyó pedidos de acceso a la información pública e investigación en sitios web oficiales. A continuación se presenta la información obtenida por dependencias:

Gendarmería Nacional Argentina:

La página web de Cellebrite hace mención a esta fuerza de seguridad y la utilización de sus herramientas en sus laboratorios[17]. Según este sitio, los oficiales de Gendarmería Nacional, a través de un Departamento de Forensia Digital con cinco sedes regionales en Campo de Mayo, Córdoba, Rosario, San Miguel de Tucumán y Bahía Blanca, entregan un flujo constante de dispositivos digitales al laboratorio. El objetivo es investigar produciendo inteligencia digital en temas relacionados con la seguridad fronteriza, el tráfico de drogas, el contrabando, entre otros asuntos. Además se detalla que investigadores y examinadores usan UFED

para extraer datos de dispositivos móviles, Cellebrite UFED Cloud para preservar y analizar datos de la nube, -como conversaciones de aplicaciones de mensajería e historial de navegación web-, Cellebrite Pathfinder para crear un entorno forense unificado en toda la red de laboratorios, y Cellebrite Physical Analyzer para generar informes.

A través de la respuesta a nuestra solicitud de acceso información pública[18] , la Gendarmería Nacional Argentina informó que en la actualidad se encuentran en distintas Unidades del Despliegue Institucional un total de 23 Equipos de Extracción Forense UFED en[19] Laboratorios Informáticos Forenses, que funcionan bajo la dependencia de la Dirección de Criminalística y Estudios Forenses emplazados de la siguiente manera:

Equipos de extracción forense

N°	UNIDAD	EQUIPOS	LOCALIDAD/ PROVINCIA
1	COMANDO DE REGIÓN I	UFED TOUCH II	Campo De Mayo (BS.AS)
2	JEFATURA DE AGRUPACIÓN VII "SALTA"	UFED TOUCH II	Salta - Salta
3	ESC 7 PASO DE LOS LIBRES " CBO MISAEL PEREYRA"	UFED TOUCH II	Paso de Los Libres -Corrientes
4	ESC 10 "EL DORADO"	UFED TOUCH II	El Dorado - Misiones
5	ESC 34 BARILOCHE "CABO PRIMERO MARCIANO VERON"	UFED TOUCH II	Bariloche – Rio Negro
6	DIV TELEFONÍA (DICRIEFOR) CELULAR	UFED TOUCH II	CABA
7	JEFATURA DE AGRUPACIÓN IV "MISIONES"	UFED TOUCH II	Posadas - Misiones
8	JEFATURA DE AGRUPACIÓN VI "FORMOSA"	UFED TOUCH II	Formosa - Formosa
9	JEFATURA DE AGRUPACIÓN XX "CÓRDOBA"	UFED TOUCH II	Córdoba - Córdoba
10	ESC NUCLEO 59 "SANTIAGO DEL ESTERO"	UFED TOUCH II	Sgo Del Estero – Sgo Del Estero
11	JEFATURA DE AGRUPACIÓN XV "ROSARIO"	UFED TOUCH II	Rosario

12	UNIPROJUVETUE	UFED TOUCH II	Venado Tuerto – Santa Fe
13	JEFATURA DE AGRUPACIÓN V "ENTRE RÍOS"	UFED TOUCH II	Paraná – Entre Ríos
14	JEFATURA DE AGRUPACIÓN XVI "SANTA CRUZ"	UFED 4 PC	Río Gallegos – Santa Cruz
15	JEFATURA DE AGRUPACIÓN II "CORRIENTES"	UFED TOUCH II	Corrientes - Corrientes
16	COMANDO DE REGIÓN V	UFED 4 PC	Bahia Blanca - BS.AS
17	JEFATURA DE AGRUPACIÓN XI "MENDOZA"	UFED 4 PC	Mendoza - Mendoza
18	DIV TELEFONÍA (DICRIEFOR) CELULAR	UFED 4 PC -	CABA
	DIV TELEFONÍA (DICRIEFOR) CELULAR	UFED 4 PC -	CABA
	DIV TELEFONÍA (DICRIEFOR) CELULAR	UFED PREMIUN	CABA
	DIV TELEFONÍA (DICRIEFOR) CELULAR	UFED 4 PC -	CABA
	DIV TELEFONÍA (DICRIEFOR) CELULAR	UFED 4 PC -	CABA
19	JEFATURA VII "CATAMARCA"	UFED 4 PC -	S.F Del Valle de Catamarca Catamarca

En el plan estratégico institucional de la Gendarmería Nacional 2020-2023, se señala como una debilidad la falta de recursos presupuestarios para mantener actualizadas las licencias del software correspondientes a UFED Touch19. Esta[20] es una herramienta forense móvil integral que permite a las fuerzas policiales, militares y de inteligencia, extraer datos de evidencia con solidez forense sin importar la ubicación.

Mediante el buscador avanzado de la página web del Boletín Oficial se encontró que para el 2022 las licitaciones abiertas convocan directamente para contratar el servicio de renovación de licencia UFED Premium para desbloqueo de celulares[21]. A través de la Licitación Pública 19/2022 se adjudicó a favor de la empresa IAFIS Argentina S.A. por la suma total de 39.631.782,00 pesos[22].

De la respuesta a la solicitud de acceso a información pública surge que Gendarmería mantiene contacto con los proveedores mediante

correo electrónico oficial, al solo fin de obtener la cotización y/o presupuesto para la iniciación de los actos administrativos que demanda la adquisición de los equipos forenses.

La Dirección de Criminalística y Estudios Forenses, en los casos de análisis de dispositivos móviles utiliza los siguientes protocolos y manuales:

- Pautas establecidas en diferentes publicaciones internacionales[23], de las que llama la atención el año del que datan (todas emitidas entre los años 2000 y el 2004), dado el avance de las tecnologías y el surgimiento de nuevos tipos de delitos.

- Resolución 528/2021 del Ministerio de Seguridad de la Nación: "Protocolo de Actuación para la Investigación Científica en el Lugar del Hecho"[24]. El mismo detalla la forma en que el o la especialista en informática forense debe actuar en el lugar del hecho, pero no hace referencia a la confiabilidad y seguridad de las herramientas que utiliza para extraer información de los teléfonos celulares.

- Resolución 234/2016 del Ministerio de Seguridad de la Nación: "Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Proceso de Recolección de Pruebas en Ciberdelitos"[25]. Aquí no se mencionan específicamente las herramientas de extracción forense de teléfonos móviles ni hay requerimientos sobre las características que deben tener para garantizar su compatibilidad con la garantía del debido proceso.

- Norma ISO/IRAM 27037[26] que establece las directrices para la identificación, recopilación, adquisición y preservación de evidencia digital.

Gendarmería declara en su respuesta al pedido de información pública que, en razón de tratarse de herramientas con licencias específicas de firmas reconocidas mundialmente, no se realizan auditorías relacionadas a la seguridad informática y que realiza reuniones de carácter técnico con los proveedores de las herramientas. Allí se exponen las novedades y actualizaciones al personal que opera dichos sistemas informáticos. Para ello se habilita para los operadores usuario y contraseña para acceder a la información técnica específica de cada equipo ofrecido, siendo los mismos de carácter reservado.

Respecto al funcionamiento resaltaron que a la información obtenida, al ser elevada a la autoridad judicial que la solicita, se le aplican dos Algoritmos HASH distintos, los cuales tienen como finalidad salvaguardar la integridad y autenticidad de las evidencias digitales relevadas. En esta misma línea, se detalló que los procesos y métodos de extracción varían según la marca, modelo y versiones del sistema operativo de cada dispositivo móvil. Entre los cuales existen:

- Extracción Lógica Avanzada
- Extracción Física
- Sistema de archivos: ADB
  - Android Backup
  - Android Backup APK Downgrade

A su vez, cada dispositivo forense posee su propio registro de extracciones, pero no discrimina los intentos exitosos de los fallidos. Asimismo, la Dirección de Criminalística y Estudios Forenses, precisamente la División Dispositivos Móviles, lleva un número de peritación único para cada requerimiento pericial, formando así parte del registro de los procesos de la herramienta forense. Por tratarse de Causas Judiciales en Trámite, las actuaciones son reservadas para las partes y secretas para terceros, y se trabaja bajo Acta de Confidencialidad.

Gendarmería afirma que no guardan copia de la información extraída una vez remitida a la autoridad judicial que la solicita.

Ministerio Público Fiscal de la Nación:

Dentro de la estructura del Ministerio Público existe la Dirección General de Investigaciones y Apoyo Tecnológico a la Investigación Penal (DATIP). Según la solicitud AIP Nº 379 del 22/08/2022 remitida a está organización, los laboratorios que desempeñan tareas periciales dentro del alcance de la disciplina que se conoce como informática forense son 2, a saber:

- Laboratorio de Informática de la DATIP
- Laboratorio de Análisis de Telecomunicaciones de la DATIP

Una de las funciones del Laboratorio de Análisis de Telecomunicaciones es gestionar la utilización y prestaciones a realizar a través del equipo de extracción de información de dispositivos móviles (UFED) con que cuenta DATIP y aquellos que puedan incorporarse en el futuro[27].La Dirección cuenta en su sitio web con un video de acceso público que se presenta como un instructivo para la descarga UFED[28].

Según lo que se pudo constatar a través del Boletín Oficial Nacional y de la página web de contrataciones del Ministerio Público Fiscal, el 20 de diciembre de 2021, a través de la Licitación Pública 38/2021, se aprobó la adquisición de tres licencias UFED 4PC Ultimate por el término de 24 meses y la renovación de una licencia UFED 4PC Ultimate por el término de 12 meses, a favor de la empresa VEC S.R.L. por 11.743.785 pesos[29]. En mayo de ese mismo año, por Licitación Pública 10/2021, se aprobó la adquisición de una licencia UFED 4PC Ultimate por 24 meses a favor de la firma IAFIS Argentina S.A. por 2.698.748,00 pesos[30].

Mediante la solicitud AIP Nº 379[31] del 22/08/2022 el Ministerio Público Fiscal informó que para la adquisición forense de dispositivos móviles y posterior análisis el Laboratorio de Análisis de Telecomunicaciones de la DATIP utiliza el software UFED 4PC versión Ultimate, contando en la actualidad con cuatro licencias activas.

A través del sitio web del Ministerio Público Fiscal de la Nación se puede constatar que entre junio y agosto de 2022 se realizó en dicha dependencia un taller técnico jurídico de análisis de extracciones UFED (teléfonos celulares), imágenes forenses (Autopsy – FTK-Encase), redes sociales y colaboración en la búsqueda de testigos[32]. El taller estuvo dirigido a empleadas/os, funcionarias/os y magistradas/os del Ministerio Público Fiscal, y su objetivo central fue adquirir las nociones fundamentales para realizar el análisis de evidencia extraída de un dispositivo electrónico. Además, a través de la solicitud AIP N° 379 se informó que los técnicos del Laboratorio de Análisis de Telecomunicaciones del Ministerio Público Fiscal Nacional han participado en demostraciones que realizan las empresas sobre las distintas tecnologías forenses, donde los proveedores locales participan activamente pero sin informar específicamente sobre qué tratan estos encuentros ni enviar la memoria de las mismas.

Respecto a los procedimientos de recolección de la prueba digital en dispositivos móviles, el Ministerio Público informó que se realizan respetando guías básicas y protocolos de actuación, entre las cuales se puede mencionar la resolución 528/2021 del Ministerio de Seguridad de la Nación, la resolución PGN 0756/2016 del Ministerio Público Fiscal de la Nación y la norma ISO/IRAM 27037, entre otras.

La resolución 528/2021 del Ministerio de Seguridad de la Nación es el Protocolo de Actuación para la Investigación Científica en el Lugar del Hecho[33] y no hace referencia a la confiabilidad y seguridad de las herramientas que utiliza para extraer información de los teléfonos celulares.

La resolución PGN 0756/2016 del Ministerio Público Fiscal de la Nación es una Guía de Obtención, Preservación y Tratamiento de Evidencia Digital del 2014 y parte de los principios que adopta son los de la norma ISO/IRAM 27037 antes citada. En dicha guía no hay referencia a las herramientas de extracción de información de teléfonos celulares. Lo único que se menciona es que el análisis en sí de los datos que se extraen de los dispositivos de almacenamiento informático se hace exclusivamente a través de cualquier herramienta de software avalada internacionalmente (Encase, por ejemplo) y que en ese momento las fuerzas de seguridad locales utilizan dichos programas por su óptimo y confiable rendimiento, y por contar con el aval del National Institute of Standards and Techonolgy (NIST)[34].

Además, cada licencia del software UFED 4PC Ultimate tiene un log[35] que informa cantidad de peritajes, tipo de extracción realizada, resultados, fechas de inicio y fin de actividad, entre otras variables. De la información brindada por el Ministerio Público Fiscal surge que entre el 15 septiembre del 2020 y el 3 de agosto de 2022 se realizaron en dicha dependencia 2.483 pericias. El resultado de las mismas se detalla en el informe que se genera por el log y puede ser exitoso, anulado, omitido o con error de lectura.

El Ministerio Público Fiscal Nacional no realiza auditorías internas, externas ni independientes para evaluar la seguridad informática de las herramientas.

Policía de la Ciudad Autónoma de Buenos Aires:

La Policía de la Ciudad de Buenos Aires depende del Ministerio de Justicia y Seguridad porteño. En el 2015 el gobierno nacional transfirió al Gobierno de la Ciudad de Buenos Aires los recursos para ejercer de manera plena las funciones policiales en su territorio. Dentro de la estructura de esta fuerza de seguridad se encuentra la División de Análisis de Inteligencia Informática y la Sección de Investigaciones Especiales[36].

No fue posible encontrar menciones institucionales en los sitios web de la Policía de la Ciudad de Buenos Aires o del Ministerio de Justicia y Seguridad porteño a herramientas forense de extracción de datos de teléfonos celulares. A través del buscador del Boletín Oficial no se obtuvieron resultados respecto a la adquisición, licitación u oferta de alguna de estas herramientas por parte del Gobierno de la Ciudad de Buenos Aires para la Policía y el Ministerio de Justicia y Seguridad. Las instituciones informaron que las mismas son adquiridas mediante los procesos de compras, ventas y contrataciones de bienes y servicios a través del sistema electrónico de adquisición y contrataciones del Gobierno por parte de la subsecretaría de la Gestión Administrativa del Ministerio de Seguridad, y que los contratos y las licitaciones son públicas.

Según lo informado por el Ministerio de Justicia y Seguridad de la Ciudad de Buenos Aires como respuesta al pedido de información pública NO-2022-30927160-GCABA-SLCC, la institución cuenta con la Superintendencia de Lucha contra el Cibercrimen de la Policía de la Ciudad, que a su vez tiene una Dirección de Investigación del Cibercrimen. De esta dirección se desprende el Departamento de Investigación de Delitos Informáticos, encontrándose subordinadas a éste la División Análisis Informático y la Sección Investigaciones Especiales. Estas dos últimas dependencias cuentan con laboratorios informáticos forenses que trabajan en conjunto con la extracción y análisis forense de teléfonos celulares, requeridos por las judicaturas.

En la misma respuesta se informa que se utiliza el hardware UFED Touch de la empresa Cellebrite y el software UFED 4PC (actualmente versión 7.57.0.13) para efectuar las extracciones forenses de los dispositivos móviles. En torno al análisis de las adquisiciones se utiliza el software Physical Analyzer (actualmente versión 7.56.0.20 de la empresa Cellebrite).

En lo referente a los protocolos para la utilización de estas herramientas, la única información brindada por parte del Ministerio

de Justicia y Seguridad del Gobierno de la Ciudad de Buenos Aires, en septiembre del 2022, establece que las diligencias se efectúan con estricto seguimiento a las “buenas prácticas forenses”[37], sin brindar copia ni detalle de esas prácticas.Por último informan que no tienen capacitaciones ni contacto con los proveedores de las UFED.

Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires:

Según la sección de contrataciones del Ministerio Público Fiscal de la Ciudad de Buenos Aires[38], se aprobó por Disposición OAF 30/2022 el procedimiento de Contratación Directa N° 4/2022 para la renovación de seis licencias EnCase™ Forensic SMS Servicio de Soporte y actualizaciones para el período entre junio de 2022 a junio de 2023, y la renovación de seis licencias Magnet Axiom Complete SMS con Servicio de Soporte y actualizaciones para el período comprendido entre agosto de 2022 y agosto de 2023 para el Cuerpo de Investigaciones Judiciales del Ministerio Público. Todo por la suma total de 34.635,00 dólares[39].

EnCase™ Forensic es una herramienta para encontrar, descifrar, recopilar y conservar datos forenses de una amplia variedad de dispositivos para investigaciones digitales[40].Según su sitio web, realiza una recopilación exhaustiva de pruebas, mejora la eficiencia de la investigación con flujos de trabajo optimizados con condiciones y filtros predefinidos o personalizados para localizar evidencia rápidamente, y proporciona los resultados de evidencia detallados para cerrar los casos más rápido.

Magnet Axiom es una herramienta que permite recuperar evidencia digital de diversos equipos informáticos, incluidos los smartphones, servicios en la nube y computadoras. En lo que respecta a celulares aseguran poder obtener información desde dispositivos con sistema operativo iOS y Android, y analiza la evidencia con herramientas analíticas integradas, tales como líneas de tiempo, conexiones, explorador de medios y mapas[41].

En noviembre del 2021 se aprobó el procedimiento efectuado en la Contratación Directa Nº 07/2021 por exclusividad, tendiente a lograr la contratación de la Certificación ENCE EnCase Certified Examiner y MCFE Axiom Magnet Certified Forensic Examiner, para uso del Cuerpo de Investigaciones Judiciales del Ministerio, por la suma total de 2.700.000,00 pesos[42]. Ambas certificaciones acreditan a los y las profesionales del sector público y privado en el uso de determinados softwares forenses[43].

También en octubre del 2021, por Disposición OAF 53/2021 se aprobó el procedimiento efectuado en la Contratación Directa Menor N° 10/2021 para renovar seis licencias EnCase Forensic (SMS) con servicio de soporte y actualizaciones, y adquirir dos Software Magnet Outrider Computer para uso del Cuerpo de Investigaciones Judiciales, por la suma total de 13.310,00 dólares[44].

En julio del 2021, por Resolución FGAG 178/2021, se aprobó el procedimiento efectuado en la Licitación Pública Nº 02/2021 tendiente a lograr la renovación de siete licencias UFED 4PC y dos licencias KIOSK Infield, para uso del Cuerpo de Investigaciones Judiciales del Ministerio Público Fiscal, que se adjudicó a IAFIS Argentina S.A. por la suma total de 117.410,26 dólares[45].

KIOSK Infield es una plataforma de hardware de Cellebrite diseñada para adaptarse al flujo de trabajo de investigación, que permite extraer y actuar rápidamente sobre datos móviles en ubicaciones específicas, como estaciones de policía y puestos de control fronterizo[46].

Migrantes y herramientas de extracción forense sobre teléfonos móviles

Con los teléfonos celulares la situación de migrantes y en pasos fronterizos se ha complejizado aún más que en épocas anteriores. Por ejemplo, hace unos meses se detectó que el gobierno de Estados Unidos entregaba a los migrantes que ingresaban desde México teléfonos móviles que tenían instalada solo una aplicación de rastreo y que no servían para hacer llamadas ni acceder a internet[47].

Cellebrite en su sitio web hace especial hincapié a la gran utilidad de sus tecnologías en pasos fronterizos y su seguridad[48]. En España, por ejemplo, en agosto del 2021 la Comisaría General de Extranjería y Fronteras de la Policía adquirió 15 dispositivos móviles Cellebrite UDEF Touch II Ultimate[49] para la realización de informes periciales judicializados en el ámbito de las fronteras terrestres, marítimas y aéreas.

En Argentina, Gendarmería Nacional es una fuerza de seguridad cuyas funciones de naturaleza militar con características de fuerza intermedia son cumplidas en el marco de la seguridad interior, defensa nacional y apoyo a la política exterior. Dentro de las funciones de defensa nacional se encuentra ejecutar el permanente control y vigilancia de las fronteras.

Cellebrite en su sitio web detalla que, a través de sus herramientas forenses, apoya las operaciones de Gendarmería en lo referente a la seguridad fronteriza y en garantizar que la inteligencia digital tome el centro del escenario en las investigaciones de dicha fuerza ahora y en el futuro. Una de las iniciativas que apoya la empresa es la creación de una nueva red de laboratorios mediante el estudio de dispositivos electrónicos conectados a posibles actividades delictivas, sin explicar exactamente de qué manera respalda esta iniciativa. Así, según declaraciones de expertos de la fuerza, la empresa se posiciona como

el proveedor de soluciones de inteligencia digital para las futuras generaciones de oficiales de Gendarmería Nacional[50].

Para conocer más sobre el tema, nos contactamos con con personas vinculadas a la defensa de los derechos de las personas migrantes en Argentina. En estas conversaciones no obtuvimos confirmación de la utilización de estas herramientas en las fronteras argentinas . De acuerdo a la experiencia de las personas contactadas, el procedimiento para el ingreso a Argentina consiste en la toma de huellas dactilares, la obtención de una foto, la pregunta por la razón de ingreso y la solicitud de un correo electrónico a dónde la Dirección Nacional de Migraciones envía un documento en formato PDF con la constancia de ingreso.

De todas maneras, sí surgió información sobre situaciones de abusos relacionados con teléfonos celulares.

Propuestas y recomendaciones

A partir de la investigación, se considera que cuando se utilizan estas herramientas de extracción forense en el marco de una investigación es necesario garantizar su confiabilidad y asegurar que lo que produzcan sea evidencia de calidad en el marco del debido proceso.

Con miras a dicha conclusión se realizaron una serie de recomendaciones:

Necesidad de información sobre el funcionamiento de hardwares y softwares

Aunque estas herramientas están protegidas por secreto comercial, es importante que exista información mínima sobre cómo funcionan. Debe existir un equilibrio entre ese secreto comercial y el conocimiento de su funcionamiento para garantizar el derecho de defensa y el derecho a la privacidad de las personas afectadas por la información extraída.

En nuestro informe del año 2021 se destacó que aunque el secreto comercial es un interés legítimo y protegido por el derecho, el mismo no puede ser invocado en situaciones que puedan afectar derechos fundamentales como el derecho de defensa.

La admisibilidad de estas herramientas en un proceso judicial debe estar condicionada a que se garantice una metodología confiable y que los resultados que se obtienen no hayan sido alterados. Para ello, promover la transparencia y control sobre cómo funcionan estas herramientas es indispensable y debe ser un valor más importante que la protección del secreto comercial.

Legislación sobre extracción de información

Las autoridades que utilizan estás herramientas deben contar con normativa de acceso público específica que garanticen el debido

proceso y el derecho de defensa sobre el uso de las herramientas de extracción de información.

Aunque el Ministerio Público Fiscal de la Nación informó los protocolos que utilizan para la extracción de pruebas en general y de pruebas digitales en particular, no sé detalla específicamente estándares de procedimiento y funcionamiento de las herramientas de extracción de información forense para teléfonos celulares.

Esto resulta fundamental para garantizar el debido control de la prueba por parte del afectado y la posibilidad de oponerse ante una manipulación errónea y/o ilegal durante la extracción de la información.

La elección de los proveedores de estas herramientas, para que se adapten a un estándar de confiabilidad comprobable en el proceso judicial, debe sujetarse a los criterios que se fijen en la normativa.

Legislación sobre el análisis de información

En la misma línea de la anterior recomendación, dada la cantidad de información propia y de terceros que se encuentra en nuestros teléfonos celulares, la extracción debe estar limitada al caso concreto y a fin específico que se busca, con un mínimo de perjuicio a terceros.

En la actualidad los teléfonos celulares cuentan con información sobre todos los aspectos de la vida de una persona, tanto del dueño o la dueña del aparato como de terceros que tienen relación con él o ella. Por esta razón es sumamente importante que la información que se analiza sea sólo la concreta para el caso y que involucre lo menos posible la privacidad de terceros.

La búsqueda de evidencia en un proceso penal no puede avanzar más de lo necesario sobre estos datos personales.

Legislación sobre el almacenamiento de la información extraída

Uno de los interrogantes que surgió al realizar este informe y para el que no se encuentra respuesta ni previsiones es la forma en que se almacena la información extraída por estas herramientas.

¿Dónde se almacena? ¿Es en un servidor de la institución que realiza la pericia o es de la empresa proveedora del software? ¿Cuáles son las medidas de seguridad sobre esa información?

Lo adecuado resultaría que la información obtenida no sea almacenada en servidores de terceros ajenos a la investigación, y que la institución que lo haga cuente con las medidas de seguridad necesarias para garantizar la inalterabilidad y robo de esa información, tanto para resguardo del derecho al debido proceso como al derecho a la privacidad de las personas involucradas.

Legislación sobre la eliminación de la información extraída y que no es relevante

Como principio aplicable a los datos personales en general, los mismos deben conservarse limitadamente.

La información extraída a través de las herramientas forenses sobre los teléfonos celulares no debe ser mantenida más tiempo del necesario para la investigación.
Debe existir una directiva clara sobre la eliminación permanente de la información extraída luego de un determinado período de tiempo.

Es muy importante resaltar que si la información que se extrae del propietario o la propietaria del teléfono no es relevante para el caso concreto debería ser eliminada inmediatamente, sobre todo cuando esta información es de y sobre terceros.

Información sobre el margen de error

En la práctica forense en general cuando se obtiene un resultado se hace de acuerdo con un enfoque técnico y metodológico específico, pero pueden existir disparidad de criterios y diversidad de resultados, es por eso que en las disciplinas técnicas es frecuente que no sea posible afirmar con certeza una conclusión, por lo que se admiten márgenes de error en los resultados[51].

Al usar las herramientas de extracción forense de dispositivos móviles, al igual que en otro tipo de pericias o testeos, los informes deben incluir un porcentaje sobre el margen de error en el que pueden incurrir estas tecnologías.

Es importante brindar esta información ya que garantiza posibles impugnaciones y cuestionamientos de la prueba por parte de la defensa, y una acorde valoración probatoria por parte de los jueces y las juezas.

Capacitación a operadores judiciales

La investigación que se realizó en base a la jurisprudencia y a la opinión de personas expertas demuestra no sólo desconocimiento por parte de operadores judiciales respecto al funcionamiento de estas tecnologías, sino también al carácter procesal que reviste su utilización dentro del proceso.

Esto incide directamente en el desarrollo del procedimiento judicial y en las garantías que rigen el mismo.

Es menester capacitar e informar a operadores judiciales sobre el funcionamiento, riesgos y eventualidades de estas herramientas de extracción forense, a los fines de generar una correcta valoración de la prueba obtenida a través de las mismas y garantizar que su utilización sea en el margen del debido proceso y derecho de defensa, con todas las garantías para la persona implicada.

Intervención humana significativa

El reemplazo de los técnicos y las técnicas forenses o peritos por diferentes tecnologías es una tendencia en crecimiento. Es por eso que se debe garantizar la intervención significativa de seres humanos en el proceso para proteger a las personas en la toma de decisiones arbitrarias que las tecnologías suelen adoptar.

Es muy importante que esta intervención humana sea efectivamente significativa y no simplemente una persona que conecta o manipula un software o hardware. Debe ser una intervención que implique una injerencia concreta en el uso y resultados de estas herramientas. Así se evitan decisiones arbitrarias por parte de las tecnologías.

Migración y derechos digitales

Los contactos mantenidos en el marco de migrantes y pasos fronterizos deja en evidencia la necesidad de un estudio más profundo sobre casos de abuso policial y explotación de datos personales. Si bien no se han detectado instancias específicas del uso de herramientas de extracción de teléfonos celulares, otros ejemplos de un accionar irregular llevan a pensar que se requiere más investigación antes de descartar dicha situación.

Resulta necesario una mayor visibilidad pública de la realidad migrante para lograr una reflexión que invite al cambio de determinadas situaciones de desprotección jurídica y humanitaria.

Es importante promover vínculos entre distintas organizaciones de derechos humanos en el ámbito digital y de migrantes para trabajar en una agenda en conjunto sobre el respeto de los derechos humanos en este tipo de situaciones.

Anexo

De acuerdo a lo informado por el Ministerio Público Fiscal de la Ciudad de Buenos Aires en respuesta al pedido de acceso a la información pública realizado, funciona bajo su órbita el Cuerpo de Investigaciones Judiciales (CIJ), organismo que cuenta con un Gabinete de Informática Forense perteneciente al Departamento Técnico Científico, en el que funciona un laboratorio de informática forense.

El CIJ fue creado mediante la Ley N°2.896, sancionada el 28/10/2008, y que a través de la Resolución FG N° 90/2020 se aprobó el reglamento interno y su organización funcional.

Para realizar las extracciones y análisis de teléfonos celulares y dispositivos móviles, el Gabinete de Informática Forense del CIJ cuenta con siete licencias del software UFED 4PC y dos licencias de UFED Kiosk, pertenecientes a la empresa Cellebrite; 12 licencias del software OpenText Encase Forensics; seis licencias del software forense Magnet AXIOM; dos licencias del software MAGNET Outrider pertenecientes a la empresa Magnet Forensics y una licencia del software DVR Examiner de la empresa DME Forensics.

En cuanto al hardware, el Gabinete de Informática Forense posee seis PC donde funciona el software UFED4PC, dos servidores DELL utilizados para los procesamientos requeridos por los softwares MAGNET Axiom y OpenText Encase Forensics. Asimismo, cuenta con dos duplicadores Tableau TX1, seis duplicadores Tableau TD3 y once bloqueadores de escritura Tableau (modelos varios según interfaz de conexión).

En cuanto a las licencias adquiridas por parte del Ministerio para su utilización en el Gabinete de Informática Forense del CIJ:

-LICENCIAS UFED 4PC (7) + KIOSK INFIELD (2): Licitación Pública N° 02/2021. Fecha de Finalización 30/04/2023.

-LICENCIAS ENCASE FORENSIC (12). Contratación Directa Menor N° 10/2021 (6). Fecha de Finalización 27/11/2022. Contratación Directa por Exclusividad N° 04/2022 (6). Fecha de Finalización 10/06/2023.

-LICENCIAS MAGNET OUTRIDER (2). Contratación Directa Menor N° 10/2021. Fecha de Finalización 30/11/2022.

-LICENCIA DVR EXAMINER (1). Contratación Directa por Exclusividad N° 6/2020. Fecha de Finalización 01/03/2023.

-LICENCIA AXIOM (6). Contratación Directa por Exclusividad N° 04/2022. Fecha de Finalización 31/07/2023.

En cuanto a los protocolos de actuación del CIJ para todas sus Unidades y/o Gabinetes se encuentra en etapa de desarrollo.
Sin embargo, el Gabinete de Informática Forense aplica, para la manipulación, recolección y análisis forenses de celulares y otros dispositivos electrónicos, las siguientes guías, directivas y buenas prácticas aplicadas por la comunidad forense internacional, en la normativa ISO/IEC 27037 y en las directrices para la recolección de evidencias y su almacenamiento publicadas por INCIBE-CERT (RFC3227). Por último, se incorporan como buenas prácticas aquellas descriptas en la Resolución 234/2016 del Ministerio de Seguridad de la Nación.

En cuanto a la existencia de procesos de auditoría formal, el Ministerio informó que no es una práctica que se utilice, sin embargo, la totalidad de licencias de software se encuentran actualizadas a octubre del año 2022. Además, informaron que el hardware utilizado se inspeccionó

los días 15, 16 y 17 de agosto del corriente por parte de personal técnico del Gabinete de Informática del Ministerio, y que el resultado fue satisfactorio para todas las unidades.

Por último, se informó que con el fin de llevar adelante las gestiones para la renovación y/o adquisición de las soluciones tecnológicas descriptas precedentemente se llevaron a adelante diversas reuniones con proveedores, tanto desde el CIJ como desde las áreas administrativas -Oficinas de Compras, Tecnología, entre otras-, pero no hay memorias de las reuniones.

* * *

Autoría

Luis García Balcarce

Abogado por la Universidad de Buenos Aires con experiencia y formación en la gestión de contenidos y herramientas digitales para el ámbito jurídico en Iberoamérica. Se desempeñó como director editorial y de contenidos en proyectos de difusión de información jurídica con universidades e instituciones públicas y privadas. Investiga sobre privacidad, protección de datos y libertad de expresión como oficial de proyecto en la ADC.

Notas

1 / https://adc.org.ar/wp-content/uploads/2022/01/ADC-Quien-revisa-tu-telefono.pdf

2 / https://www.infobae.com/politica/2022/09/04/ataque-a-cristina-kirchner-las-dudas-sobre-el-celular-reseteado-del-detenido-y-el-intento-para-recuperar-la-informacion/

3 / https://www.pagina12.com.ar/479088-ataque-a-cristina-kirchner-al-borde-de-perder-una-prueba-cla

4 / https://www.argentina.gob.ar/sites/default/files/poblacion_urbana_dnp.pptx_.pdf

5 / https://www.clarin.com/policiales/detectives-telefonos-secretos-sistema-abre-celulares-resuelve-causas-complejas_0_U-d0fZd2m.html

6 / https://cellebrite.com/es/pagina-principal#

7 / https://www.accessnow.org/cms/assets/uploads/2021/09/vigilancia-latam-espa.pdf

8 / El uso de software abierto para el análisis de la evidencia digital por Gustavo Presman y Pablo A. Palazzi, disponible en https://docplayer.es/90297795-El-uso-de-software-abierto-para-el-analisis-de-la-evidencia-digital.html

9 / Signal, "Exploiting vulnerabilities in Cellebrite UFED and Physical Analyzer from an app's perspective", 21.04.2021 https://signal.org/blog/cellebrite-vulnerabilities/

10 / Para más información sobre el equilibrio que debe existir entre el poder de policía del Estado y el derecho a la privacidad por la cantidad de información almacenada en los teléfonos celulares leer Riley v. California de la Suprema Corte de Justicia de los Estados Unidos, disponible en https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf

11 / A modo de ejemplo e ilustrativo: Vega, Diego Daniel y Otros s/Infracción Ley 23.737, Tribunal Oral Federal de Bahía Blanca, 03/06/2022. Disponible en **https://www.cij.gov.ar/sentencias.html**

12 / https://www.youtube.com/watch?v=6BjRuA5EvZ8

13 / Shen, Yongchao s/Infraccion Ley 23.737, Tribunal Oral en lo Criminal Federal N° 1, 27/05/2022. Disponible en **https://www.cij.gov.ar/sentencias.html**

14 / A.J.A. y otros s/nulidad, Cámara Nacional de Apelaciones en lo Criminal y Correccional - Sala IV, 20/09/2019. Disponible en **https://www.diariojudicial.com/public/documentos/000/087/223/000087223.pdf**

15 / El bit corresponde a un dígito del sistema de numeración binario y representa la unidad mínima de información

16 / Para más información de estos temas desde un enfoque más jurídico consultar "La extracción de prueba electrónica de teléfonos celulares y la garantía de defensa en juicio", de Carla Paola Delle Donne. Dsponible en: **https://www.thomsonreuters.com.ar/content/dam/openweb/documents/pdf/arg/white-paper/dossier-el-desafio-de-la-prueba-electronica.pdf**

17 / https://cellebrite.com/es/la-gendarmeria-nacional-de-argentina-esta-superando-las-barreras-de-tiempo-y-distancia-con-inteligencia-digital/

18 / La respuesta al pedido de información pública a Gendarmería Nacional Argentina se encuentra en nuestro poder.

19 / https://www.argentina.gob.ar/sites/default/files/plan-estrategico-20-23.pdf

20 / https://cellebrite.com/es/cellebrite-presenta-la-plataforma-ufed-touch2/

21 / https://www.boletinoficial.gob.ar/detalleAviso/tercera/2301589/20220311

22 / https://www.boletinoficial.gob.ar/detalleAviso/tercera/2311388/20220613

23 / Casey, E. 2004. "Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet". Baltimore, Maryland, USA. Editorial Elsevier.

24 / https://www.boletinoficial.gob.ar/detalleAviso/primera/253486/20211126

25 / https://www.argentina.gob.ar/normativa/nacional resoluci%C3%B3n-234-2016-262787/texto

26 / https://www.iso.org/standard/44381.html

27 / https://www.mpf.gob.ar/datip/laboratorio-de-analisis-de-telecomunicaciones/

28 / https://www.mpf.gob.ar/datip/#gallery

29 / https://www.boletinoficial.gob.ar/detalleAviso/tercera/2296402/20211220

30 / https://www.boletinoficial.gob.ar/detalleAviso/tercera/2276900/20210510

31 / La respuesta al pedido de información pública al Ministerio Público Fiscal de la Nación se encuentra en nuestro poder.

32 / https://www.mpf.gob.ar/capacitacion/actividad/taller-tecnico-juridico-de-analisis-de-extracciones-ufed-telefonos-celulares-imagenes-forense-autopsy-ftk-encase-redes-sociales-y-colaboracion-en-la-busqueda-de-testigos/

33 / https://www.boletinoficial.gob.ar/detalleAviso/primera/253486/20211126

34 / https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf

35 / Grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular. Es una evidencia del comportamiento del sistema.

36 / https://documentosboletinoficial.buenosaires.gob.ar/publico/PE-RES-MJYSGC-SECS-34-18-ANX.pdf

37 / La respuesta al pedido de información pública al Ministerio de Justicia y Seguridad de la Ciudad de Buenos Aires se encuentra en nuestro poder.

38 / https://mpfciudad.gob.ar/compras/search

39 / https://mpfciudad.gob.ar/storage/archivos/1fd6b060f907ca0884d4b7ecce511fc7.pdf

40 / https://security.opentext.com/encase-forensic

41 / https://www.magnetforensics.com/products/magnet-axiom/

42 / https://mpfciudad.gob.ar/storage/archivos/93ed13085179966abf4250920cf6ad01.pdf

43 / https://www.opentext.com/TrainingRegistry/course/details/2687

44 / https://mpfciudad.gob.ar/storage/archivos/564a6bfdf7f8c4743da673c6fd276c63.pdf

45 / https://mpfciudad.gob.ar/storage/archivos/0821ca2578b6ae2cdeab3482b4db74bd.pdf

46 / https://cellebrite.com/es/plataformas/

47 / https://cnnespanol.cnn.com/2022/06/05/telefonos-celulares-no-pueden-hacer-llamadas-ni-acceder-internet-ice-rastrear-migrantes-trax/

48 / https://cellebrite.com/es/cellebrite-responder-es/

49 / https://elcierredigital.com/tecnologia/122247883/interior-usara-tecnologia-israeli-hackear-telefonos-moviles-fronteras-espanolas.html

50 / https://cellebrite.com/es/la-gendarmeria-nacional-de-argentina-esta-superando-las-barreras-de-tiempo-y-distancia-con-inteligencia-digital/

51 / Para más información consultar "Certeza pericial y margen de error" de Apesteguy, Patricia Noemí disponible en https://www.lanacion.com.ar/politica/certeza-pericial-y-margen-de-error-nid1773887/

adc.org.ar